WHITEPAPER

NIS 2 IN HUNGARY

Reflections and recommendations
from a year and a half of practice

PUBLISHED: NOVEMBER 18, 2025

VERSION 1.1

Impressum

Edited by: Dr. Váczi Dániel, Dr. Andrea Jeney, Ákos Orbók

Written by: William Z. Apró, György Arató, Gergő Barbul, Gabriella Biró, Zsuzsa Borbély, Péter Bódis, Gergő Csarnai, Patrik Cseh, Vencel Cserháti, Dr. Ágota Albert, Dr. Andrea Jeney, Dr. Judit Kiss, Dr. Anett Novák, Dr. Edit Szilvia Rubóczki, Dr. László Szabó, Dr. Emese Szilágyi, Dr. Balázs Gergely Tiszolczi, Dr. Dániel Váczi, Alexandra Enyedi, Krisztián Frey, János Gedra, Kinga Kálmán, György Attila Kovács, Tamás Lóth, Péter Maczkó, Róbert Major, Edina Mandrik, Márk Máté, Csaba Mészáros, Etele Mészáros, Imre Nagy, Norbert Pataki, Zoltán Sipos, Árpád Robotka, Ákos Solymos, Mária Etelka Szabó, Krisztina Szűcs, András Végh, Dr. Ádám Simon

Translated by Dr. Andrea Jeney based on the Hungarian version

Proofread by: György Arató, Dr. Dániel Berzsenyi, Dr. Tünde Bonnyai, Olivér Bor, Dr. Judit Kiss, Márton Miklós, Dr. Enikő Szilágyi

Project manager: Éden Forgács
Design: Zsófia Elek
Photos used: Ákos Solymos EFIAP/A-MAFOSZ/s

Participating organisations:

Table of contents

1. Introduction

Written by: Dr. Dániel Váczi

During professional discussions and the recording of the NIS2 podcast, the desire for clear guidelines was repeteadly emphasised to help the affected organisations navigate the disputable points of the legal implementation in Hungary. Several approaches can be taken. Some are widely accepted, while others are less supported by the professional community. However, one thing is certain: no single correct answer can be identified. Each approach must always be adapted with reference to the specific characteristics of the organisation.

Although this has long been a requirement, no practical or methodological documents – beyond the official guidelines – have been issued to provide further support, or assistance. Many organisations are struggling not only with the interpreting the legislation but also with its practical implementatio, and they must take into account as limited internal resource and ensure that the requirements are aligned with their day-to-day operations.

As the vision of the start-up I represent is to serve as a contact point between domestic and EU cybersecurity stakeholders in the context of NIS2, the idea arose to initiate the creation of such a document on a community-driven basis. Personally, I was motivated not only to talk about why compliance with NIS2 is fundamental, but also to provide a practical, step-by-step guidance on how it can be achieved.

In response to our call via professional social media forums, more than 50 experts and organisations with expertise in the field came forward. Some contributed by writing specific chapters, while others supported project management or editorial work. I am proud that so many dedicated professionals devoted their time and energy to this joint effort in addition to their daily responsibilities. This initiative demonstrated the power of community cooperation as well, with bringing together different perspectives, areas of expertise, and experiences to achieve a common goal.

This document is not intended to serve as a general training manual, nor does it claim to cover all topics required of Member States under NIS2. Our objective is to offer an available guidance to the affected organisations and the ecosystem that supports them, based on our practical experience. This document is rather intended for professionals in compliance and IT, subject-matter experts, and those in managerial or decision-making roles tasked with ensuring compliance at the organisational level.

We have therefore placed strong emphasis to maintain professional credibility while ensuring that the language remains clear and conceise. It is important to us that the material is not only understandable to those with in-depth subject matter expertise, but also to those who are new to the topic and yet have a vital role in NIS2 implementation.

We do not claim to have the best solution, if such a solution even exists. Due to the complexity of the NIS2 Directive there are undoubtedly topics that we have not covered in full, despite our efforts to present a variety of perspectives and approaches in parallel. Certain sub-topics (e.g., EISs, the risk management framework, or different implementations across Member States) would even merit separate documents. Nevertheless, our aim has been to provide a practical summary that helps organisations tailor their compliance measures to their specific operations, maturity level, and internal processes.

It is important to underline that this is not an official guide nor we do not guarantee that its application alone will ensure compliance or succesful audit. Nonetheless, we are confident that the document offers clear, practical

guidance on implementation and will serve as a valuable reference both now and moving forward.

Our goal is to periodically review and update the document and to incorporate new insights and legislative changes. If you feel that an important aspect or topic has been omitted, we encourage you to join our review process. In addition, we have created a repository where we have published materials that freely available for testing and practice purposes. We would be particularly pleased if these resources evolve over time with contributions from our readers and the professional community, allowing us to continue supporting each other in this way, even alongside the major preparation and audit activities.

The entry into force of NIS2 has initiated a new phase of development and learning for professionals across Europe, including Hungary. With this document, we seek to play an active role in that process. We encourage everyone to engage in this collaborative effort, either directly through this project or in other ways. The more knowledge and experience we share, the better we can adapt to emerging challenges. This is how we can contribute to the core objective of NIS2: a more cyber-resilient and secure future throughout Europe and, therefore, in Hungary.

02

Legal background

The ongoing development of European and national cybersecurity legislation aims to guarantee the security of digital infrastructures and services within a coherent and effective legal framework. The pivotal development in this process is the adoption of EU NIS 2 Directive , which significantly broadens the scope beyond its predecessor, with imposing stricter requirements, and directly influences how Member States implement into their domestic law. This chapter reviews the fundamental objectives of the NIS2 Directive and then presents the legal framework for its implementation in Hungary, with a particular focus on the obligations of the affected organisations and the process of embedding these into the domestic legal system.

2. Legal background

Written by: Dr. Edit Szilvia Rubóczki, Dr. László Szabó, Dr. Emese Szilágyi, Dr. Dániel Váczi

2.1. The purpose of the NIS2 Directive

The rapid growth of digitalisation and the need to safeguard the functioning of the single internal market made it inevitable for the EU to begin regulating cybersecurity as early as the early 2000s. EU Member States recognised that cyber threats jeopardise not only economic stability but also fundamental rights. Harmonised regulation therefore was introduced to establish a common basis for defense, in particular for the protection of critical infrastructure, whose resilience is vital to both society and the economy.

> The 2004 Madrid terrorist attacks, which prompted comprehensive regulation of critical infrastructure; followed by the cyberattacks on Estonia in 2007 in 2008, made it clear that the risk posed by acts carried out in cyberspace and not limited to economic damage or the unauthorised access to restricted data; a large-scale attack could even threaten the functioning of a state and its communities.

The formulation of the EU's cybersecurity strategy and the drafting process for the first NIS Directive commenced in 2013; the strategy's subtitle was ‚an open, secure and resilient cyberspace'.

As part of this process, the two pillars of European security expansion: the GDPR in the area of data protection[1], and the NIS 1 Directive in the area of network security[2], established fairly similar requirements from two different perspectives and for two different purposes (data and network protection), including security requirements and incident reporting obligations. While the NIS 1 Directive, seeking harmonisation on geopolitical grounds, laid down minimum rules and mandatory cooperation mechanisms for Member States, the GDPR remains directly applicable as a regulation.

It should be noted here that EU legislation aimed at developing the resilience of ICT products and making them more robust, such as the ex ante regulation represented by the above-mentioned Directive and the data security provisions of the GDPR, is not exclusive in nature. The EU also intends to protect the security of cyberspace from unexpected events that could undermine users' trust in technology, networks, and services by means of criminal law, which, due to its punitive and therefore an ex post approach seems to be of limited effectiveness, as the global nature of the acts committed makes detection difficult and the penalties imposed may not necessarily deter potential perpetrators. Nevertheless, according to the legislator, maintaining user confidence makes such regulation necessary, the roots of which can be traced back to the

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

2 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems across the Union (not in force)

1986 OECD report entitled[3]. The primary objective of the report was to identify offences committed in the digital environment and support their codification. The first document of this kind issued by the Union on this subject was Recommendation No. R[4] (89) 9 on computer-related crime, which contained a minimum list of acts that Member States were required to criminalise in the cyber domain. This regulatory process, which reached its international public law stage in the Council of Europe's 2001 Budapest Convention on Cybercrime, concluded in Directive 2013/40/EU, in which the legislator set the objective that the same criminal offenses relating to cyberspace should be punishable in all Member States.

This topic also includes the establishment of the European Union Agency for Cybersecurity (ENISA), as the relationship between the NIS2 Directive and ENISA is key to the EU's cybersecurity strategy. The NIS2 Directive, which entered into force in 2023, significantly expanded the role and tasks of ENISA, which was established by Decision 2004/97/EC of the European Council (EK) and is currently regulated by the Cybersecurity Act (EU) 2019/881[5] in order to strengthen cybersecurity at the EU level. NIS2 further expanded the agency's responsibilities under the act with regard to the implementation of the directive in question, such as providing technical support to Member States in transposing NIS2 into national law and assisting the work of the CSIRT (Computer Security Incident Response Team) network and the Coordination Group. As the NIS 1 Directive, adopted in 2016, sought to respond to increasing and worsening security incidents. Minimum harmonisation was justified by the impact of incidents on the continuity of economic activities and the financial losses they cause (e.g., downtime and recovery time and resource losses caused by a hacker attack), their transnational nature, and the varying levels of preparedness of individual Member States. NIS1 laid the foundations for cybersecurity cooperation and incident response capabilities (at the incident management and analysis level), set out tasks at Union level, and provided for the establishment of national strategies, dedicated organisations, and a network of Member State CSIRTs. The priority areas of NIS 1 are to mitigate system threats and ensure the continuity of services during incidents, with a strong emphasis on effectiveness.

The transposition of the NIS1 Directive into Member State law and the harmonisation of national legislation occurred between 2016 and 2018, with the national rules coming into effect on 10 May 2018.

As noted in the preamble to the NIS2 Directive, while the objectives and framework of NIS1 were forward-looking, its implemenation varied across Member States. These significant differences have led to fragmentation of the internal market, which has adversely negatively impacted its functioning, rendering a review of NIS1 compulsory. The review of the rules also became necessary due to digital transformation and the widespread use of network systems. The development and digitalisation of basic services such as transport, water supply, waste management, and lighting, as well as the emergence of innovative technologies (such as artificial intelligence), have further expanded the scope that needs to be protected to ensure safe operation. In addition, the COVID-19 pandemic[6] highlighted the

3 OECD (1986). Computer-related criminality: Analysis of legal policies in the OECD area. Paris: OECD.

4 Recommendation No. R (89) 9 of the Committee of Ministers to Member States on computer-related crime, 13 September 1989

5 Regulation (EU) 2019/881 of the European Parliament and of the Council (17 April 2019) on ENISA (the European Union Agency for Cybersecurity) and on cybersecurity certification of information and communication technology and repealing Regulation (EU) No 526/2013 (cybersecurity legislation) (text with EEA relevance)

6 Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs

economic importance of digital solutions and the vulnerability of supply chains.

The European Commission presented its proposal for the NIS2 Directive in December 2020, which was adopted by EU legislators in November 2022.

The purpose of NIS2 is to eliminate differences between Member States, improve cooperation among authorities and update the list of sectors to be protected. With NIS 2, the scope of application, which was previously sector-based, has been expanded to cover a larger part of the economy in order to achieve a high level of cybersecurity across the EU. To ensure legal certainty a uniform set of criteria and a size threshold rule have been applied thereby extending the Directive's scope to include medium-sized enterprises operating in the covered sectors and, in certain areas, actors of all size (e.g. trust service providers).

It should be noted that the NIS2 Preamble explicitly prioritises proactive cybersecurity measures over reactive responses, requiring the existence of appropriate tools for detection, as well as rapid and automatic sharing and understanding of alerts and response measures.

The development of technical and organisational capabilities, the prevention, detection, and response to incidents and risks has become more prominent. Compared to NIS1, the incident management tasks of CSIRTs have been given greater importance. In addition, addressing the specific cybersecurity needs of SMEs, raising and strengthening cyber awareness, including issues related to businesses acting as suppliers, has become a priority for Member States within the framework of their national strategies.

The main objectives of NIS 2 include:

- increasing the resilience of network and information systems
- effective defense against cyber threats,
- ensuring the seamless functioning of the internal market,
- and facilitating cooperation among Member States.

The objectives of NIS 2 were considered achievable by extending the scope of application - previously limiting to specific sectors - to a broader part of the economy. To ensure legal certainty a uniform set of criteria and a size threshold rule have been applied thereby extending the Directive's scope to include medium-sized enterprises operating in the covered sectors and, in certain areas, actors of all sizes (e.g. trust service providers).

The Directive lays down uniform EU-wide requirements to achieve a high level of cybersecurity protection for organisations that are essential to the functioning of the economy. This is attained through the adoption and implementation of state-of-the-art protective measures and technologies, as well as by strengthening the obligation to report incidents. The clear objective of the Directive is to prevent cyberattacks and other threats, mitigate the negative impacts of attacks that have already occurred and establish a unified „defense network" through coordinated cooperation among Member States.

The NIS 2 Directive should be interpreted in conjunction with the EU Data Strategy, the EU Cybersecurity Strategy and the EU Digital Act. The EU Data Strategy plays a key role in the development of the digital economy, as it aims to create a single European data market where data can flow securely and lawfully among Member States. In line with this, the Cybersecurity Strategy strengthens the EU's resilience to cyberattacks and sets out the defense frameworks that are essential for the

reliable functioning of digital services. The EU Digital Act[7] sets out the digital rights and expectations of citizens and businesses, ensuring that the digital transition is people-centered, secure, and sustainable. These initiatives are closely linked to the NIS2 Directive, as it aims to establish a high level of cybersecurity across the EU based on principles defined at EU level. They should also serve as a starting point for the everyday functioning of the economy and society, as well as for the development and deployment of new technologies.

The aim of the NIS 2 Directive is to limit the Member States' discretion in regulating cybersecurity within the covered sectors - compared to its predecessor - does not imply that it is intended to serve as an exclusive source of law. Nevertheless, while the Directive is not meant to be exclusive, independent national legislation is not permitted in areas where specific EU rules apply. Article 4 explicitly allows for the adoption of sector-specific EU legal acts. Moreover, the Directive acts as a reference point for other legal instruments — such as amendments to the eIDAS[8] Regulation — whether already in force or pending, when more detailed provisions are required than those set out in NIS2.

However, to determine whether sector-specific legal instruments apply to the organisation we manage or are responsible for, and to identify which sectors are covered by general versus specific regulations and the extent of their application, the following considerations should must be taken into account:

Article 4 of the Directive and the Commission Communication 2023/C 328/02 issued in connection with it also stipulate that specific rules may only apply to essential or important organisations as defined in the Directive. In other words, we can see a 'modular', complementary form of regulation in relation to NIS2 and a sector-specific EU legal act. This conclusion is not groundbreaking, since the existence of specific rules presupposes, in some extent, the existence of general rules. However, the clarity of the above observation is qualified by the fact that both the Directive and the aforementioned Commission Communication state that where sector-specific EU legal acts do not cover all entities operating in a given sector covered by the Directive, the relevant provisions of that directive (i.e. NIS2) continue to apply to organisations that are not covered by those sector-specific EU legal acts. In short, specific rules in a given sector (e.g. „manufacturing") do not cover all sub-sectors, but only the sub-sector „manufacture of electrical equipment," the provisions of NIS2 shall apply only to sub-sectors not already covered by the rules applicable to the „electrical equipment" sub-sector, within the „manufacturing" sector, unless additional rules are estabilshed.

The final element to consider regarding the scope of sectoral rules is that NIS2 allows for derogations from the general rule, i.e. the Directive, in cases where they are related to (a) cybersecurity risk management measures or (b) the notification of significant security incidents. According to Article 4, these alternative requirements must be at least equivalent in effect to the obligations laid down in the NIS2 Directive. In such cases, the relevant provisions of Directive (EU) 2022/2555, including the provisions on supervision and enforcement in Chapter VII shall not apply to the entities covered by the specific rules.

With regard to the typology of the sector-specific EU acts mentioned earlier, three examples will be presented that are positioned along a scale, with specific cybersecurity provisions and complementary regulations serving as the endpoints.

A typical example of the frequently referenced sector-specific EU acts is Regulation (EU) 2022/2554 on the digital operational resilience

7 EURLEX

8 Regulation (EU) No.910/2014 of the European Parliament andof the Council https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02014R0910-20241018

of the financial sector, which is currently being drafted as the banking services and financial market infrastructures sectors listed in Annex I to the NIS 2 Directive. Until now, this is the only sector-specific EU legal act to date that is included in the annex to the Commission's relevant Communication 2023/C 328/02. The Regulation on electronic identification for electronic transactions in the internal market (EU Regulation No. 910/2014) can also be interpreted in this context.

In this context, Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) is also relevant. It contains provisions applicable to trust service providers as essential entitites within the digital infrastructure sector, irrespective of their size.

Another example is Directive (EU) 2022/2557 on the resilience of critical organisations[9] which imposes obligations on organisations operating such infrastructure to develop their resilience, conduct risk assessments, and prepare crisis management plans with regard to certain critical infrastructures. A key difference between the two directive is that while NIS 2 focuses on the protection of network and information systems, the Cyber Resilience Directive focuses on physical and operational resilience, thereby complementing one another. This complementary relationship is further reinforced by the provision in the Critical Facilities Resilience Directive stipulating that the directive does not apply to matters covered by Directive (EU) 2022/2555, i.e. NIS 2.

Main innovations of NIS2 compared to NIS1:

- Broader scope: more sectors (digital infrastructure, public administration, ICT service providers, online marketplaces, social media, space, etc.) are covered by the directive
- Role categorisation: the distinction between essential service providers and digital service providers is abolished; instead, organisations (entities) are clearly classified as either essential or important.
- Risk-based requirements: stricter, detailed rules on risk analysis, incident management, supply chain security, cryptography, and multi-factor authentication.
- Supply chain responsibility: security compliance extends to suppliers, especially in the field of ICT systems.
- Stricter sanctions: significant fines can be applied – minimum of EUR 10 million or 2% of turnover for essential organisations, EUR 7 million or 1.4% of turnover for important organisations.
- Member State obligations: mandatory cybersecurity strategy, CSIRTs, crisis management framework, cooperation networks (e.g. EU-CyCLON e)
- ENISA role: ENISA is responsible for management of European vulnerability database, regular reports, registry of critical actors

9 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical organisations and repealing Council Directive 2008/114/EC (Text with EEA relevance)

2.2. The legal background of NIS2 in Hungary

Even before the transposition of the NIS1 Directive, Hungary already had a national cybersecurity strategy[10] and legislation, as well as an institutional framework for critical infrastructure. Based on this, instead of introducing completely new legal instruments it incorporated the EU requirements into the existing regulatory and institutional framework.

National rules complying with the NIS 1 Directive had to be adopted by May 9, 2018, and applied from May 10, 2018,. Meanwhile the identification by Member States of operators providing essential services (in all sub-sectors listed in Annex II within the territory of the affected Member State) had to be completed by November 9, 2018.

With the adoption of the 2013 cybersecurity strategy and sectoral strategies, Hungary ensured compliance with EU requirements. Operators providing essential services (energy, transport, finance, healthcare, drinking water, digital infrastructure sectors) were largely identified, allowing critical infrastructure to be covered by supplementing existing rules with the provisions of NIS1. On the other hand, digital service providers were included in the system through the introduction with new regulations.[11]. The Government Decree on the tasks of incident response centres was amended to incorporate the NIS1 rules on incident reporting (including the introduction of the concept of significant impact and the obligation to report without undue delay), while sector-specific Government Decrees[12] regulated the relevant sectors, while the rules applicable to digital service providers were aligned with the legislation on electronic commerce and information society services[13].

In December 2018, the government adopted Government Resolution 1838/2018 (XII. 28.) on the Strategy for the Security of Network and Information Systems in Hungary as a sectoral strategy. This document outlined „the new cybersecurity challenges and development objectives, the support by specialised institutions for activities promoting practical knowledge and awareness-raising aimed for the secure use of cyberspace, with a strong emphasis on research and development in the context of implementing the digital state."

In terms of the institutional framework, the supervision of the security of critical facilities and systems was carried out by the National Directorate General for Disaster Management of the Ministry of the Interior (BM OKF), while the National Security Service (NBSZ), within which the government incident management centre (GovCERT) operated, was responsible for responding cybersecurity incidents. As a result of the new regulations, the supervision and incident management of service providers subject to reporting obligations was transferred to NBSZ Special Service for National Security in 2019.

Hungary was among the first EU Member States to establish a national legal framework

10 Government Decision No. 1139/2013 (III.21.) on Hungary's National Cyber Security Strategy

11 Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities (Lrtv.), Act L of 2013 on the electronic information security of state and municipal authorities (Ibtv) and their implementing decrees

12 Energy: 374/2020 Government Decree; Health: 246/2015 Government Decree; Finance: 330/2015 Government Decree; Water management: 541/2013. Government Decree; Transport: 161/2019. Government Decree; Information and communication technologies: 249/2017. Government Decree; also regulated: Agricultural economy, Social security, Nat ional defense, Public safety and security (police).

13 Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Ekertv.)

in line with the NIS2 Directive[14] through the adoption of Act XXIII of 2023 (Kibertan.tv.), which entered into force in several stages up to October 18, 2024.

The new law classifies the affected organisations based on their level of criticality, distinguishing between high-risk sectors (essential entities) and risky sectors (important entities). It also extends the scope to sectors that have not previously been involved in information security allowing them to join the framework through self-identification. The definition of stakeholders was based on the size threshold set out in NIS2 (medium-sized enterprises - more than 50 employees or annual turnover exceeding EUR 10 million or EUR) and irrespective of these tresholds, also considered specific sectors covered by the Act. The goal of Kibertan.tv was to establish and operate a well-functioning, risk-proportionate information security management framework.

In accordance with the NIS Directive, the Supervisory Authority for Regulatory Affairs (SZTFH) has been designated as the national cybersecurity certification authority, while a separate authority is responsible for the defense industry's R&D and manufacturing. Under the provisions of the Cybersecurity Act, the SZTFH is also responsible for the cybersecurity supervision of the affected organisations and their EISs . The president of the SZTFH issues regulations the decree level the procedural rules for the activities of the certification authority, the registration and requirements of certified ICT products and auditors, the cybersecurity supervision fee, the audit process and other related matters.

In addition, Decree 7/2024 (VI. 24) of the Prime Minister's Office (hereinafter: MK Decree) on the classification of security levels and the specific protection measures applicable to each security level sets out the criteria for classification into security levels and specific protection measures to each level. The compliance framework was set out in Decree 1/2025 (I. 31) of the SZTFH (hereinafter: SZTFH Decree), which estatblishes the basic rules for cybersecurity audits and the applicable fee structure. Together, these two decrees form the basis for the practical implementation of the legal requirements. Further details are provided in the following chapters (see:8.1.1 and 8.1.2).

Act LXIX of 2024 on Cyber Security in Hungary (hereinafter referred to as the Cybersecurity Act) was enacted pursuant to Government Decree 1838/2018 on Hungary's National Cybersecurity Strategy. The Strategy consolidated, amended and redefined the provisions previously contained in the two fundational pieces of legislation in this field: Act L of 2013 on the electronic information security of state and local government bodies (hereinafter referred to as the Ibtv.) and Act XXIII of 2023 on cyber security certification and cyber security supervision (hereinafter referred to as the Kibertan. tv.). The primary objective of the legislation was to transpose the NIS2 Directive into national law, which establishes uniform and stricter cybersecurity requirements for EU Member States. The detailed implementing rules of this Act are set out in Government Decree 418/2024. (X. 30.) (hereinafter referred to as: the Government Decree), which specifiefs, among others, the framework for the identification of the affected organisations, their obligations, and the procedures for official supervision and control.

A more stringent set of national requirements is reflected in Hungary's new Cybersecurity Strategy adopted in 2025, under Government Resolution No. 1089/2025. (III. 31.)[15]. The Strategy acknowledges that the growing

14 The NIS 2 Directive had to be transposed into national law by October 17, 2024, and applied from October 18, 2024.

15 Government Decree No. 1089/2025. (III. 31.) on Hungary's Cybersecurity Strategy (1089/2025. (III. 31.) Korm. határozat)

number of online presence of both state and non-state actors increases the risks associated with that presence. In order to prevent, effectively counter and manage potential threats from cyberspace, the legislator aims to enhance the resilience of Hungarian ICT networks (including related products and services) as well as the sectors that perform essential and important functions for the economy and society, while simultaneously building operational capacity.

The legislation entered into force on January 1, 2025, alongside the repeal of both the Ibtv. and the Kibertan. tv., the latter having originally been adopted to implement the NIS2 Directive into Hungarian legislation. The new law not only consolidated the existing provisions, but also introduced wide range of new measures and obligations. A particularly notable innovation being the introduction of the categories of „essential" and „important" entities, categorised according to the critical importance of their services and the size of the organisation. The distinction between these two categories aligns with the framework established in the NIS2 Directive.

However, the introduction of a more uniform set of cybersecurity requirements under the Cybersecurity Act does not entail the abolition of individual sector-specific legislation due to their greater social, national economic or national defense or national security significance, call for tailored regulation. Thus, critical organisations and critical infrastructures (hereinafter collectively referred to as „critical organisations") designated under the Act on the Resilience of Critical Organisations (hereinafter referred to as „Kszetv."), as well as those identified under Act XCIII of 2021 on the Coordination of Defense and Security Activities (hereinafter referred to as „Vbö.") as significant for the protection and security of the country (hereinafter referred to as organisations significant for the protection and security of the country) fall outside from the scope of the Cybersecurity Act. The provisions of the law on cybersecurity supervision do not apply to critical organisations falling under the scope of the DORA Regulation[16] or to organisations significant for the protection and security of the country, while the rules on incident management apply, except as otherwise specified by law.

The multi-layered Hungarian regulatory framework is structured so that fundamental requirements are established at legislative level, while more detailed rules are set out in decrees. Compliance is further supported by other sources of law that are not legally enforceable, notably standards which, although not binding, carry significant and practical importance.

In its supervisory role, the SZTFH issues informational materials and the NKI publishes guidelines to help organisations in interpret and apply the legal requirements[17].

Notable examples should be as follows:

- The audit methodology was developed based on NIST Special Publication 800-53A Revision 5.
- The National Cyber Security Institute of the Special Service for National Security has published several guidelines[18]. On the one hand, it facilitates the implementation of individual security measures by organisations and, on the other hand,

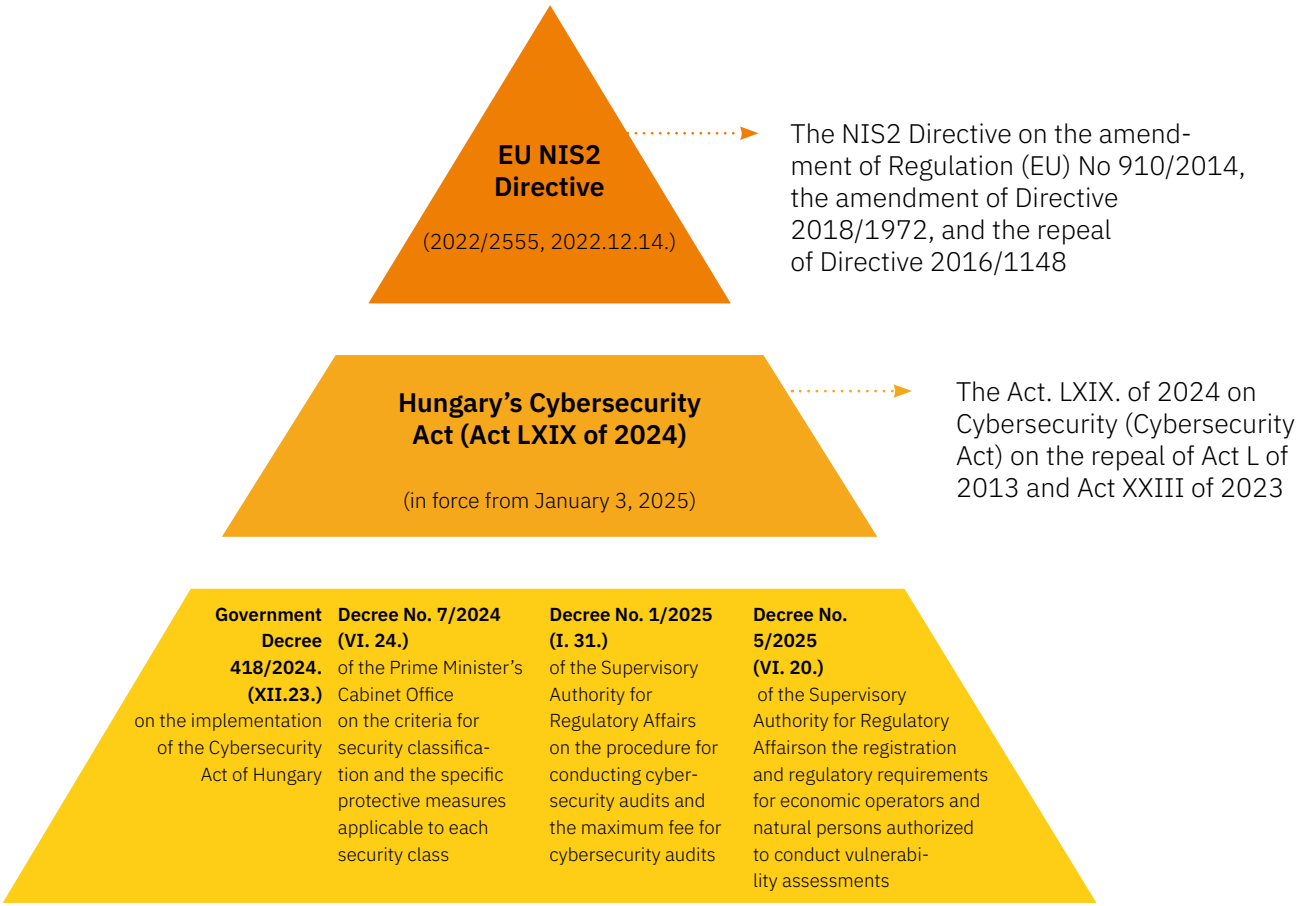
16 Regulation (EU) 2022/2554 of the European Parliamant and of the Council of 14, December 22 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/101 (DORA Regulation)

17 Justification of Act 69 of 2024 on Hungary's cybersecurity (Justification of Act LXIX of 2024)

18 Guidance on the application of the Catalogue of Cybersecurity Requirements for Electronic Information Systems and Organisations
Guidance on the practical application of the MK Regulation (EIR Guidance)
Preparations ((PDF)
Requirements catalog (XLSX)

assist organisations that have developed their information security management framework in accordance with the previously applicable Decree 41/2015. (VII. 15.) BM, or based on ISO/IEC 27001:2022 (or its predecessor, ISO/IEC 27001:2013), in aligning their controls with those prescribed in the new standard.

It should also be noted that several legislative instruments related to cybersecurity requirements have come into force which, while less directly applicable to all organisations concerned, are important for ensuring the completeness of the legal framework. Decree 2/2025. (I. 31.) of the SZTFH decree estatblishes the amount of the cybersecurity supervision fee and the rules for its payment, while Decree 3/2025. (IV. 17.) of the SZTFH regulates the details of the supervision and control procedures and the role of the information security supervisor, and Decree 5/2025. (VI. 20.) of the SZTFH regulates the registration of economic operators and natural persons authorized to conduct vulnerability assessments as well as the requirements applicable to them. Although these decrees do not directly affect all organisations subject to the legislation, they are nevertheless crucial for the uniform functioning of the cybersecurity ecosystem and for ensuring the proper authentication of market participants.



Figzre 1 (Source: MOORE Hungary - ACPM IT Consulting Ltd.)

2.3. Interpretation of NIS2 compliance in the Whitepaper

For the purposes of interpreting this document, it is fundamental to understand that organisations are not required to comply directly with the NIS2 Directive, but rather with the rules as transposed into Hungarian law. The NIS2 Directive is a European Union instrument that requires all Member States to transpose its principles and requirements into their national legislation. In Hungary, this has been achieved through the legislation outlined in the previous chapter, of which the following four are of particular relevant to the compliance of the organisations concerned and to this Whitepaper:

- • Act LXIX of 2024,
- • Government Decree 418/2024 (X. 30.),
- • Decree 7/2024 (XI. 15.) MK,
- • Decree 1/2025 (I. 31.) of the SZTFH

It is important to clarfify these terms such as „NIS 2 audit," „NIS 2 compliance," and similar expressions are commonly used in both everyday and professional communication, and the authors of this Whitepaper also use them frequently. In practice, they always refer to compliance with Hungarian laws and regulations. The only exception is when the context clearly indicates that the reference is to the Directive itself in its EU-wide sense.

It also should be noted that, in practice, EU-level requirements alone are not sufficient: during audits, Hungarian authorities examine compliance exclusively with domestic laws and regulations. To avoid misunderstandings, all subsequent references in this Whitepaper should be interpreted accordingly.

03

Identification of affected organisations

Determining which entities fall within the scope of the NIS2 Directive is a crucial step for compliance, since its requirements and obligations apply exclusively to those covered. However, accurate classification is not always straightforward. In many cases, expert support is required to assess the scope of activities, size category or geographical coverage of services. Particular challenges may arise from the precise interpretation of SME size thresholds, the distinction between domestic and EU-wide activities, and the complexity associated with the provision of international services. This chapter offers practical guidance on these matters to help organisations make informed decisions regarding their classification.

3. Identification of affected organisations

Written by: Gabriella Biró, Zsuzsa Borbély, Krisztián Frey, Dr. Kinga Kálmán, Etele Mészáros, Dr. Ádám Simon, Dr. Emese Szilágyi

3.1. Self-identification

The scope of NIS2 stakeholders is determined by the Cybersecurity Act. In essence, it establish whether an enterprise or organisation falls within NIS2 based on its activities, size, and revenue.

To comply, organisations must determine whether they qualify as affected parties and, where applicable, submit the information specified in the SZTFH decree (using form SZTFH 420, available at[19]) to the Authority via the company portal at for registration. Understandably, many organisations have raised questions about how to assess their legal status whether they fall within the scope.

Self-identification is not always evident, yet it remains a crucial step, and management is typically motivated to complete it. It should be emphasised that the top managment of the companies concerned is personally responsible for meeting the deadlines and submitting the registration application, and this responsibility cannot be delegated to anyone else.

According to estimates, 3,000-4,000 companies and organisations in Hungary may fall within the scope of the NIS2 Directive. As reported by the authorities, the SZTFH has received over 3,700 registrations to date. This number is expected to change over time, as some organisations and companies may eventually be removed from the scope of NIS2, while others may be added.

The estimates are derived from statistics and records, taking into account the scope of activities. It is therefore important to note that in Hungary it is common for companies to include activities in their records that they do not actually perform, without taking steps to remove them.

Size and revenue

NIS2 significantly expands the scope of organisations it covers. By default, organisations meeting at least the criteria for a medium-sized enterprise fall within the scocpe of the law. The size of an enterprise is determined under the Hungarian legal system based on the Kkvtv.[20] , in line with the EU definition[21].

Organisations that meet or exceed the thresholds for medium-sized enterprises (50 employees or EUR 10 million, i.e. annual turnover of approximately HUF 3.9 billion) including those, that qualify as medium-sized enterprises based on the combined number of employees or financial indicators with affiliated companies, are categorised under NIS2 according to their size and revenue.

For example, a company with 35 employees would qualify as a small enterprise on its own. However, when combined with a larger affiliated company, it would be considered a medium-sized enterprise and therefore fall within the scope of NIS2 Directive.

19 Application for registration of the affected organisation

20 Act XXXIV of 2004 on small and medium-sized enterprises,

21 Commission Recommendation 2003/361/EC concerning the definition of SMEs,

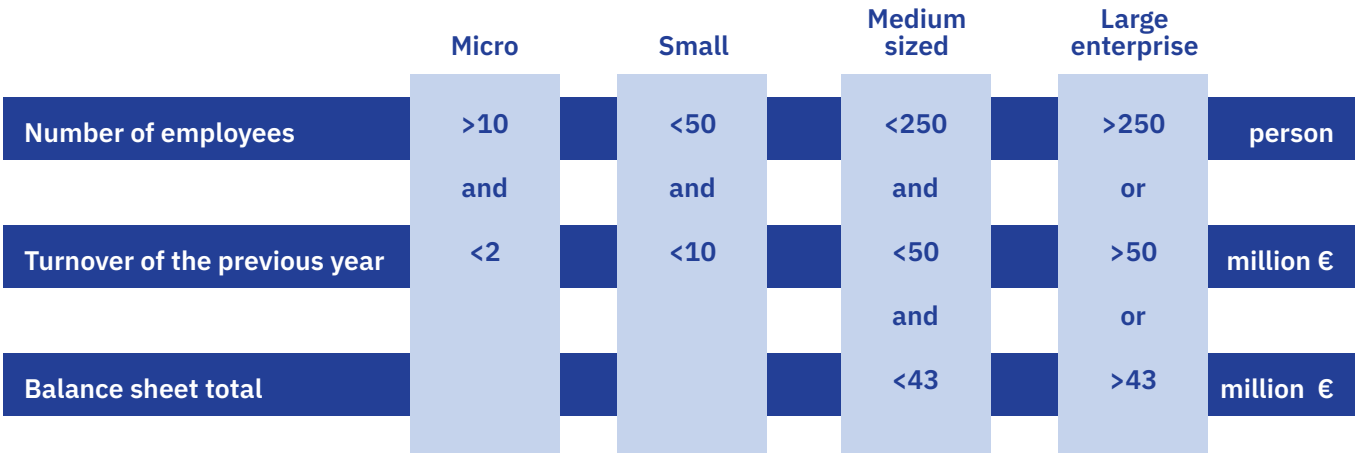


Figure 2 (Source: SZTFH) Downloaded: Februar 7, 2025

Nevertheless, it is important to stress that merely meeting these thresholds does not, by itself, determine whether a company falls within the scope of NIS2.

The scope of NIS2 primarily covers medium-sized enterprises, but small enterprises may also fall within the scope of the Directive if the other risk factors apply (e.g. if they provide critical services).[22] According to Article 2(2) of the Directive, the rule does not apply to small and micro-enterprises, unless they:

- operate in critical sectors as defined in NIS2 (e.g. energy, transport, health, digital infrastructure),
- carry out activities that are „of significant public interest".

Consequently, an enterprise cannot be excluded from the scope of NIS2 solely based on its size; the nature of its activities and services it provides are also a decisive factors.

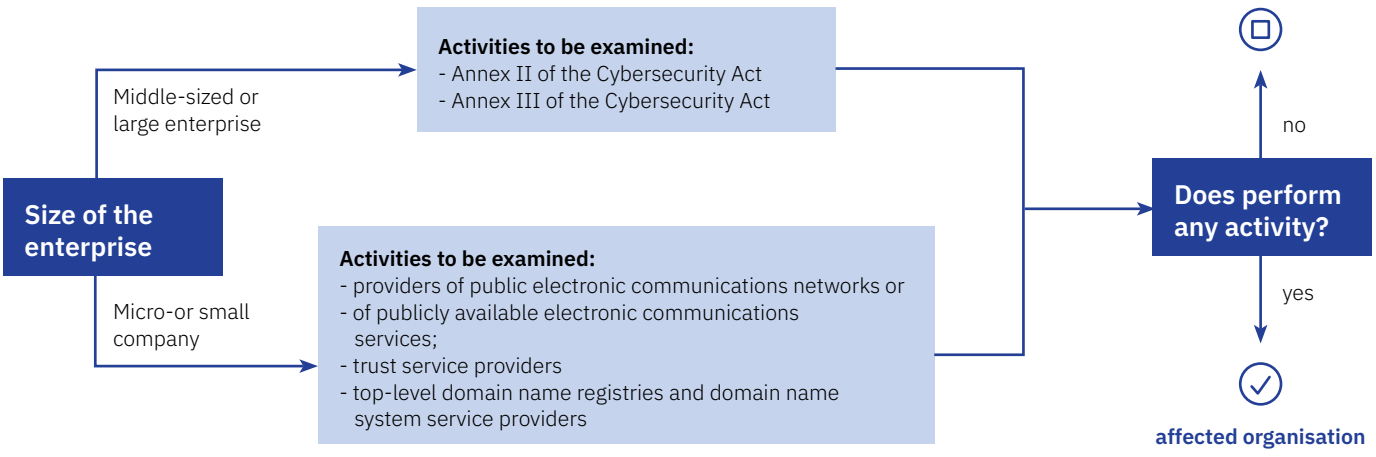


Figure 3 (Source: SZTFH) Downloaded: Februar 7, 2025

22 Directive (EU) 2022/2555 on ensuring a high level of network and information security across the Union (NIS 2).

Spheres of activity

Both NIS2 and the annexes to the domestic legislation[23] contain tables listing the sectors, subsectors and organisations relevant to each subsector. Regardless of the size thresholds, it is essential to assess whether a given organisation falls within the scope of NIS2 based on its scope of activities and the nature of its services, as well as to identify the authority responsible for its supervision.

If an organisation operates in one of the sectors listed in Annexes 2 or 3 of the Cybersecurity Act, it may be subject to NIS2, regardless of the number of employees or overall size.

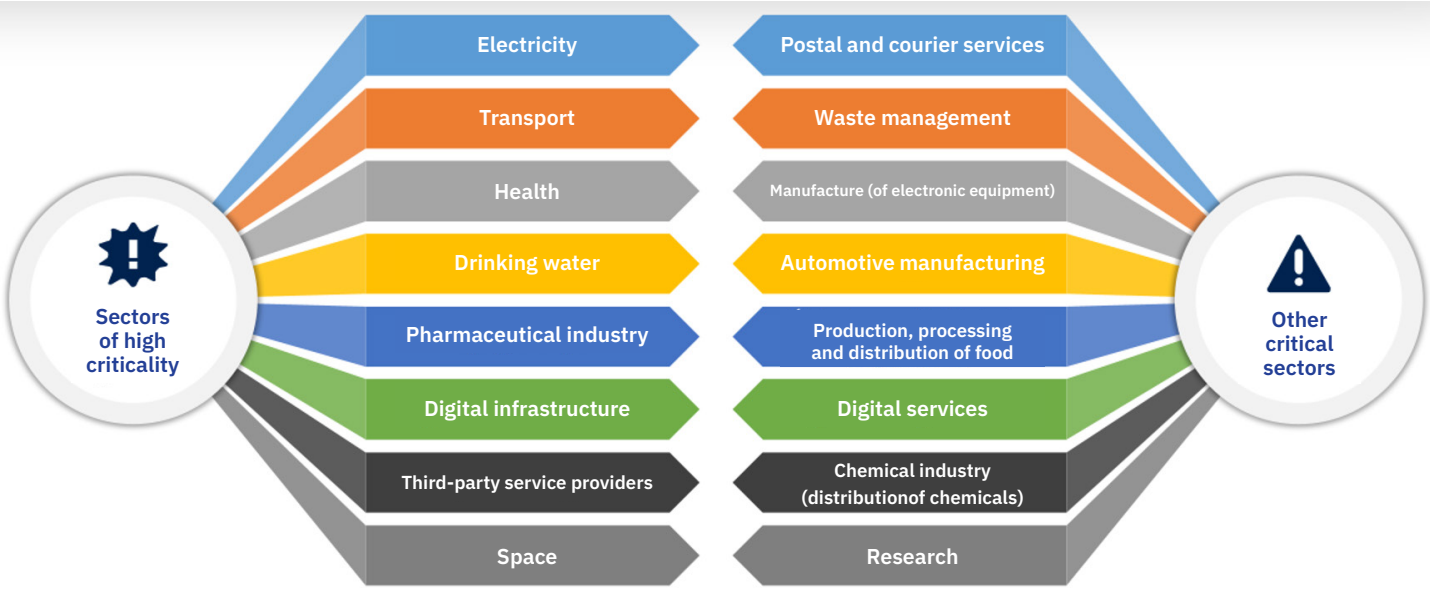


Figure 4 (Source: SZTFH) Downloaded: Februar 7, 2025

The following service providers, identifiable through the registers maintained by the authorities, are subject to NIS2 regardless of their size, including micro or small enterprises. (see brackets for the designation used by the Hungarian authorities)

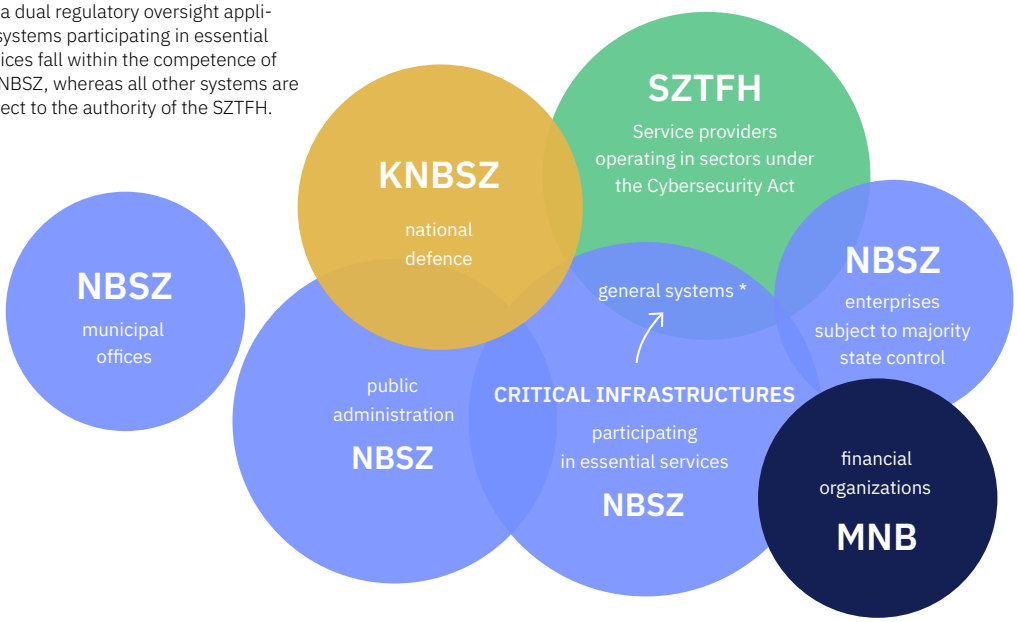
- electronic communications service providers (listed in the register of the National Media and Infocommunications Authority (NMHH))
- trust service providers (registered by the NMHH)
- DNS service providers
- top-level domain name registrars (the only organisation in Hungary: ISZT Nonprofit Kft.)
- domain name registration service providers (registrars listed on the domain.hu website operated by ISZT)

23 Cybersecurity Act, Annexes 2 and 3

Among the above, qualified trust service providers, DNS service providers and top-level domain name registrars are classified as essential organisations.

The competence of the cybersecurity authority depends on whether the organisation at issue belongs to the administrative sector, is an economic entity under majority state control, or has a defense-related connection. The following diagram from the NKI clearly illustrates the various realtionships of certain organisations.

* In the context of critical infrastructures, a dual regulatory oversight applies: systems participating in essential services fall within the competence of the NBSZ, whereas all other systems are subject to the authority of the SZTFH.



SZTFH: Energy, transport, health, drinking water, waste water, digital infrastructure, ICT service, space, postal and courier services, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing, digital services, research

Figure 5 (Source: NKI (2024)[24]

If the size threshold is met, i.e. the organisation qualifies as a medium-sized or large enterprise, the activities listed in the relevant annexes must be examined. As the registration form requires a detailed declaration of activities based on these annexes, it is strongly recommended that all activities be carefully reviewed.

Although banking services and financial market infrastructures are identified as high-risk categories in the NIS 2 Annex, these sectors are governed by sector-specific rules under Article 4 of NIS2. Accordingly, NIS2 does not apply to organisations already covered by the DORA Regulation, and the transposition of NIS2 does not impact the financial and banking sectors. The cybersecurity supervisory authority for financial organisations is the Hungarian National Bank (hereinafter reffered as to:MNB)

The public administration sector, defined in accordance with national law, including central government and regional public administration bodies, is also classified as high risk.

The sector or activity to be assessed during self-identification is based on the records kept by the relevant authorities for activities requiring authorisation. In other cases – typically in the manufacturing sector – it can be examined on the basis of the Hungarian Activity Classification (TEÁOR in Hungarian) code or other numbers, which may raise a number of questions. The interpretation of the classification may also raise practical problems at the sub-sector level.

24 https://www.eset.com/hu/mi-is-az-a-NIS 2-mi-lyen-uj-modositasok-leptek-eletbe/
Since the image was created, the relevant KNBSZ organisation has been renamed the National Cyber Security Authority.

For example, a software developer cannot be classified on the basis of its development activities, but it must be also be assessed whether it qualifies as an outsourced service provider, since in practice the development company often provides additional services related to development, which may render it relevant.

In Hungarian practice, companies sometimes include activities in their records that they do not actually perform, without taking steps to remove them. The raises the question of how many companies come to the attention of the authorities based on this activity classification system, as they are presumed, according to the records, to be engaged in activities in essential or important sectors. Although in many cases modifying the scope of activities is a simple administrative procedure, concerns may arise regarding the assessment of the actual activity performance and the enforcement of obligations in cases where companies fail to self-identify.

In other instances, a permit from the competent authority is generally required by law. The Hungarian authorities responsible for the various sectors are as follows:

- electricity, district heating, water utilities, natural gas: Hungarian Energy and Public Utility Regulatory Authority
- transport: Ministry of Construction and Transport (transport authority)
- food industry: National Food Chain Safety Office
- pharmaceutical industry, stockpiling, healthcare providers, chemical industry: National Public Health and Pharmaceutical Center
- electronic communications, trust and postal service providers: National Media and Infocommunications Authority
- Waste management: environmental protection authority.

Identification may vary due to differences in how Member States interpret their rules on sector classification.

An example is the food industry, where the scope of stakeholders was previously broader under Hungarian rules, as the Kibertantv referred to „food businesses as defined in the Act on the food chain and official supervision," while Annex 2 of NIS2 lists entities engaged in wholesale trade, industrial production and food processing." The current Cybersecurity Act already aligns with NIS2 and bases the identification of entities in this sector on data provided by food chain control authorities.

According to the above, in assessing whether an enterprise qualifies as an operator in a critical sector under NIS2 and national provisions, professionals from the legal, compliance, financial, and IT fields can jointly assist management in making informed decisions.

The amount of the cybersecurity fine that may be imposed on an organisation referred to in Section 1(1)(d) and (e) of the Cybersecurity Act in connection with registration may be determined as follows, based on Annex 3 to the Government Decree:

	A	B	C
1	Description of the irregularity	Minimum fine	Maximum fine
2	Failure to provide data for registration in accordance with Section 8(5) of the Cyber Security Act	the net turnover of the organisation referred to in Section 1(1)(d) and (e) of the Cyber Security Act in the previous financial year – in the absence of turnover, the pro rata share of the turnover for the current year – or 0.5% of the previous year's budget revenue estimate, but at least HUF 1,000,000	the net turnover of the organisation referred to in Section 1(1)(d) and (e) of the Cyber Security Act in the previous financial year – in the absence of turnover, the pro rata share of the turnover for the current year – or 2% of the budget revenue estimate for the previous year, but not exceeding HUF 150,000,000
3	Failure to provide data for registration pursuant to Section 8(5) of the Cyber Security Act after the deadline	50 000 HUF	0.1% of the net turnover of the organisation referred to in Section 1(1)(d) and (e) of the Cyber Security Act for the previous financial year – or, in the absence of turnover, the pro rata portion of the turnover for the current year – or up to 0.1% of the previous year's budget revenue estimate but not exceeding HUF 15,000,000

Source: National Legislation Database

3.2. Supporting actors

Although organisations are required to carry out the self-identification themselves, there are expertsboth within and outside the company who can provide support. If assistance is needed, it is advisable to seek guidance from the following actors:

Lawyers, legal advisors

A number of actors are defined in legal terms by the Cybersecurity Act, which under Hungarian legislation usually requires a license from a competent authority. The authorities responsible for the various sectors are as follows:

- Hungarian Energy and Public Utility Regulatory Authority: electricity, district heating, water utilities, natural gas
- Ministry of Construction and Transport (Transport Authority): transport sector,
- National Food Chain Safety Office: food industry,
- National Public Health and Pharmaceutical Center: pharmaceutical industry, stockpiling, healthcare providers, chemical industry,
- National Media and Communications Authority: electronic communications, trust and postal service providers,
- Pest County Government Office: waste management,
- Regulated Activities Supervisory Authority: petroleum.

If the company holds a license from a designated authority, it is advisable to consult the company's legal department or an external lawyer.

Financial experts

By default, organisations that meet the criteria for at least a medium-sized enterprise classification fall within the scope of the Cybersecurity Act, so it is recommended to verify their classification according to the SME Act.

The finance departments of organisations are generally familiar with the applicable rules and maintain up to date company classifications, e.g. for tendering purposes.

Cyber security and IT professionals

IT professionals, cybersecurity experts, and those working in quality management personnel typically have the grerateset expterise in information security compliance. It is reasonable to assume that individuals in these roles can assist in determining whether the organisation has information systems or services covered by NIS2.

Experts in technology, information security, and compliance also play a key role in completing the registration form.

Consultants, experts

In our time, cybersecurity stands out as a major challenge, and the NIS2 Directive is a key step in protecting digital infrastructure.It is therefore unsuprising that many consulting firms provide services in connection with NIS2, including consulting and training on the subject, as well as additional support such as information security officer services. Some firms have developed various NIS2 calculators, so as tools to help determine an organisation's level of involvement (e.g., RSM NIS 2 calculator[25], Datatronic NIS2 involvement assessment questionnaire[26]).

Several reputable consulting firms with cybersecurity expertise can assist in assessing an organisation's NIS2 relevance. However, caution is warranted, as the growing interest in this area has also attracted companies to this consulting market that lack the necessary professional expertise and experience.

Authorities

The SZTFH and the NKI provide informational materials to assist with self-identification. In addition, both organisations undertake a range of activities to provide guidance on the NIS 2 Directive and its implementation in Hungary. The SZTFH has launched a multi-station national event series, and has also delivered presentations at numerous conferences alongside NKI experts as guest speakers, and as well as providing information to interested parties through the podcast „Minden kiberül" (Everything is cyber)[27].

If difficulties arise during self-identification and support is unavailable, the SZTFH can be contacted or the registration form submitted, and the authority will provide guidance in determining whether your company falls within the scope of the NIS2 Directive.

3.3. Issues related to the provision of international services

Under the NIS2 Directive, the Member State, in which the organisation is established generally has jurisdiction. Consequently, in the most straightforward cases, Hungarian companies are supervised by the Hungarian authorities,

25 NIS2 Calculator 2025

26 NIS2 impact assessment questionnaire

27 Everything goes digital – SZTFH launches cybersecurity podcast

even when providing cross-border services (e.g. if a chemical company based in Hungary selling chemicals in Austria, is primarly subject to the Hungarian Cybersecurity Act for this activity).

However, issues of territorial and personal jurisdiction are often complex. There are numerous cases in which the previous example does not apply. This chapter presents two such instancecs, that are particularly relevant in business practice and may lead to different outcomes:

- Provision of cross-border digital services [e.g., cloud services, outsourced (directed) information and communication services, outsourced (directed) information and communication security services] in several Member States or as an organisation established outside the EU providing services within the EU,
- Regulation of electronic communications services..

In the cases described above, Article 26 of the NIS2 Directive sets out, at a fundamental level, which Member State's jurisdiction applies to a given organisation, that is, which Member State's implementation is most likely to be applicable. However, since the NIS2 Directive provides a minimum harmonisation framework from which Member States may deviate to a considerable extent, it is necessary in each case to examine the relevant Member State's legal environment when preparing for cybersecurity compliance in the context of cross-border services.

In the following, we provide a general overview of the relevant provisions of the NIS2 Directive and the Cybersecurity Act on the two topics outlined above, followed by a discussion of certain practical issues which are commonly encountered in the context of international service providers.

As international service provision is primarily concerns private-sector organisations, this chapter focuses on such entities. However, it is important to emphasise that the scope of the NIS2 Directive (and consequently the Cybersecurity Act) also extends to public and administrative bodies, although jurisdictional issues are less likely to arise in this context. In addition, Member States may retain the authtority to designate certain critical organisations within their territory or organisations that are important for national security and bring them under their own jurisdiction. While these issues are also an important aspect of NIS2 compliance, a more comprehensive analysis would falls beyond the scope of this chapter and the Whitepaper.

Cross-border digital services

When drafting the NIS2 Directive, the legislator sought to find a practical solution to ensure that operators of cross-border digital services, which are available simultaneously in all Member States do not have to comply with the local NIS2 implementation in each Member State, thereby avoiding the associated administrative burdens.

The NIS2 Directive covers DNS services, top-level domain name registration services, domain name registration services, cloud services, data center services, content delivery network services, managed services, and managed security services, as well as online marketplaces, online search engines, as well as and social media platform services (collectively referred to as „Digital Services").

To address the cross-border nature of Digital Services, the NIS2 Directive introduces a one-stop-shop compliance mechanism. Under this regime, jurisdiction over Digital Services is exercised by the Member State, where the organisation has its main place of business within the EU, thereby preventing other Member States from exercising jurisdiction over the service provider.

The NIS2 Directive sets out a three-step test to determine the main place of business. The main place of business shall be considered to be as:

- where the majority of decisions relating to cybersecurity risk management measures are made. In this context, the mere presence and use of electronic information systems is not, by itself, decisive, criteria in most cases, decision-making occurs at the location of central management;
- if no such Member State can be identidied, or if these decisions are made outside the EU, the main place of business is considered to be the Member State where the cybersecurity operations are conducted, and
- if no such Member State can be determined, the main place of business is deemed to be the Member State, in which the largest number of the organisation's staff are employed.

In the case of groups of companies, pursuant to recital 114 of the NIS2 Directive, the main place of business of the controlling undertaking is decisive. However, it should be noted that the NIS2 Directive contains significant inconsistency in this regard and it is currently unclear whether the main place of business must be determined separately for each entity within a group or whether it is possible to establish the main place of business within the EU for the entire group of companies.

Another significant issue is that, despite the transposition deadline of 18 October 2024, many Member States have not yet implemented the NIS2 Directive, so the main place of business may be located in a Member State where there no local legislation is currently in force. In practice, this implies there is no directly applicable legislation establishes the jurisdiction of the Member State over the digital services provided by the organisation, leaving the organisation uncertain as to which rules apply and effectively rendering it „stateless" under the NIS2 Directive.

Where an organisation is not established in the EU offers Digital Services within the EU, it must designate a representative within the EU. Based on our experience in the field of international service provision, it often occurs that a subsidiary of a multinational group outside the EU provides information and communication services, information and communication security services or cloud services to all entities established in the EU. In such cases, the subsidiary with its main place of business in the EU is typically designated as the representative.

Electronic communications services

The NIS2 Directive provides an additional exception to the general rule, stipulating that providers of public electronic communications networks or publicly available electronic communications services are subject to the jurisdiction of the Member State, in which they offer their services. Consequently, these providers must comply with the implementation measures of each Member State separately and simultaneously, where they operate such networks or services.

Regulation under the Cybersecurity Act

The Hungarian legislation is largely aligned with the framework of the NIS2 Directive, but it does not fully follow its logic.

The provisions of the Cybersecurity Act apply to organisations established or maintaining a representative office in Hungary, electronic communications service providers offering services in Hungary, and digital service providers whose main place of business is in Hungary. The determination of the main place of business also essentially follows the framework set out in the NIS2 Directive.

A key difference, however, is that the Cybersecurity Act requires all organisations not registered in Hungary to appoint a representative operating in Hungary if the organisation operates an electronic information system falls within the scope of the Cybersecurity Act. This provision considerably extends the scope of

the NIS2 Directive beyond digital service providers established outside the EU but also to all foreign entities subject to the Cybersecurity Act, including service providers based in other EU Member State. According to the interpretative provisions, the representative's role may appear to be merely that of a local contact person. However, under the Cybersecurity Act, the representative operating in Hungary bears the responsibility for ensuring compliance with the law, in accordance with the rules applicable to the head of the organisation. This single-tier responsibility regime, linking the head of the organisation and the representative, creates significant legal risk for the latter and makes the practical appointment of Hungarian representatives challenging.

Practical issues in the case of international service provision

If a Hungarian subsidiary provides digital services either within a group of companies or to third parties in another Member State, the one-stop shop mechanism must be taken into account when determining jurisdiction. In this context, the main establishment must be identified which is not necessarily Hungary despite the subsidiary's registered office being located there. This could be the case, for example, where the organisation's internal cybersecurity unit does not operate in Hungary. The situation becomes even more complex if elements of the internal cybersecurity unit are distributed across several countries, including jurisdictions outside the EU. Depending on the corporate structure, this assessment must be carried out either at the level of the specifiic organisation or at the group level.

Within a group of companies, a foreign parent company provides digital services to its Hungarian subsidiary, such services will, as a general rule, not fall within the scope of the Cybersecurity Act due to the the one-stop-shop mechanism. However, where the parent company is established outside the EU, in addition to the one-shop-stop designation, it may also be required to appoint a representative within the EU to act on its behalf.

In the case of non-digital services, as a general rule, services provided by an organisation established in Hungary fall within the scope of the Cybersecurity Act. Accordingly, it is highly unlikely that the implementation of the NIS2 Directive in other Member States would apply. However, for multinational companies, particularly where production and distribution are carried out across several countries and entities, it is advisable to consult with local lawyers in each juriscdiction concerned, as our practice shows interpretation of jurisdiction can differ across Member States.

Based on the Hungarian cybersecurity legislation and practical experience, the interpretation of key institutions and the fulfilment of obligations raises a number of practical issues even if the organisation concerned is not established in Hungary, These include cybersecurity audit and cybersecurity training requirements for foreign management members and a person responsible for the security of electronic information system, as well as the compliance of local registration requirements. It is also worth noting that foreign organisations did not have the possibility to register using the SZTFH 420 form until February 2025. In addition, auditing electronic information systems connected to Hungarian services provided by foreign service providers raises further practical questions requiring clarification. .

04

Roles and responsibilities

One of the fundamental pillars of the NIS2 Directive and the relevant national legislation is the explicit definition of cybersecurity roles and responsibilities. The allocation and documentation of cybersecurity tasks are essential to ensure oprational transparency, enable rapid response, and strenghten accountability within the organisation. The rules require all affected entities to clearly designate the individuals responsible for information security management, incident management, compliance monitoring, and supplier relationship management, and to document their tasks and responsibilities. A well-defined system of accountability not only facilitates legal compliance, but also enhances the organisation's cyber resilience by reducing security risks arising from negligence or misunderstandings.

4. Roles and responsibilities

Written by: Gabriella Biró, Dr. Andrea Jeney, Imre Nagy, Dr. Anett Novák

4.1. Information security roles

Performing information security tasks is a complex and multifaceted activity that requires close cooperation among various roles. To ensure an appropriate division of tasks and clear understanding of responsibilities, it is advisable to begin by reviewing the individual stakeholders. This approach provides clarity on how roles should be defined, executed and documented.

> It is particularly important for the organisation to clearly document these roles, along with the associated tasks, rights and responsibilities. This promotes transparency and provides a solid foundation for accountability in the event of security incident.

The NIS2 Directive strengthens and redefines the concept of management responsibility. It underscores that an organisation's top management - at the highest level of the hierarchy - remains ultimately accountable for strategic decisions related to information security. Senior executives are responsible for approving risk assessments, deciding on protective measures, and appointing a person in charge of information security, with whom they maintain continuous, day-to-day cooperation. Their responsibilities also extend to the assessment of technical aspects.

Personal oversight is exercised by the information security manager, appointed by the head of the organisation. This role encompasses the coordination of all professional issues related to information security, including the development of internal policies, the establishment of incident management procedures, internal and external communication with the stakeholders, and the organisation of awareness-raising training. The information security manager works in close cooperation with the IT manager and the IT team, who are responsible for operating the technical infrastructure and overseeing day-to-day IT operations. It is important to emphasise that the information security manager is not subordinate to the IT manager, but exercises independent professional authority.

Other key members of the organisation include application developers, who are responsible for developing and customising software solutions to meet business needs, and procurement managers, who oversee the acqusition of off-the-shelf software and other IT equipment. In addition, internal auditors may also play an important role by conducting audits of the organisations's information security systems and procedures, with a particular focus on safeguarding organsational interests.

Whether the organisation assigns the above roles to internal employees or outsources certain tasks is a business decision, taken by management and guided by internal procedures. Such decisions must cconsider not only legal requirements but also transparency and organisational clarity. Proper documentation is not only a compliance obligation, but also a prerequisite for effective operation and accountability.

If the organisation opts for an internal solution, information security tasks will be carried out by its own employees. The job descriptions of these employees will clearly define their responsibilities, their position within the organisational structure, and their reporting lines.

Several factors may influence this decision including financial considerations, the level of existing expertise, the organisational hierarchy, and management priorities. While choosing an internal solution offers many advantages, but it can also present challenges, such as resource limitations, dependency on in-house expertise, and the need for continuous training and development.

Advantages

One of the main advantages of internal solutions is that they offer greater control and transparency: the organisation directly manages information security activities without relying an external intermediary. This is especially beneficial during incidents, where a quick and direct response is crucial. Moreover, direct access to documents (such as log files, system logs) also enhances auditability, as these records are easier to review, maintain and keep up-to date.

Another advantage is that internal staff have in-depth knowledge of the organisation's operations and processes, enabling them to develop tailored protection strategies in line with the business objectives. This internal expertise is especially valuable, when advancing the organisation's information security maturity.

Communication within the organisation is generally simpler and more direct, allowing information security issues to become an integral part of IT, legal, or business discussions. This shared organisational culture supports the rapid identification and efficient resolution of issues, ensuring a level of responsiveness and effectiveness that is often difficult to achieve with external service providers.

Furthermore, organisational culture and commitment are often stronger when relying on internal solution. Employees ten to view the organisation's security as their own responsibilty, which increases their willingness to follow policies and actively cooperate in incident management. This contrasts with external experts, who usually work on a project basis and may not be as closely aligned with the long-term interests of the organisation.

Finally, it should be noted that budget considerations play a decisive role in organisational decision-making. Although internal solutions often require greater initital investment, they may become more cost-effective over time, especially if information security expertise is gradually developed and maintained in-house.

Disadvantages

Internal information security solutions offer numerous advantages, but they also present significant challenges and risks. These must be carefully evaluated to ensure the long-term, sustainable, and effective operation.

Recruiting, retaining, and continuously developing information security professionals requires significant financial investment. Given the rapid evolution of this field, employees must regularly update their knowledge, participate in training programs and conferences, and obtain professional certifications. These costs are considerable in themselves, and the design, implementation, and maintenance of a robust information security system - along with the necessary technologies - can further increase financial demands. Consequently, such expenditures should be carefully planned for and integrated into the organisation's long-term budgeting strategy.

Another significant challange is the specialised expertise required in the field of information security. As cyberattacks become increasingly sophisticated, the continuous professional development is essential to maintain effective protection and ensuring the organisation's secure operation.

To ensure uninterrupted protection, information security must offer round-the-clock

monitoring and rapid response. Achieving this requires an internal team to maintain 24/7 readiness—something particularly difficult, especially when resources are limited. As a result, responses to attacks or incidents may be delayed, potentially exacerbating damage. Furthermore, establishing on-call systems and rapid response protocols introduces further organisational complexity and financial burden.

If the information security manager reports to the IT manager or holds a strong operational role, there is a risk that security concerns will be downplayed in favour of business speed and continuity. Internal power dynamics and competing interests may therefore compromise professional judgment, leading to suboptimal risk management.

Another challange arises when critical information security tasks are concentrated in the hands of one or two key individuals. Their unexpected departure or extended absence can cause serious disruptions. Inadequate handover of knowledge, relationships, processes, and documentation can hinder operations or result in poor decision-making. Failing to prioritise knowledge sharing, establish substitution procedures, and maintain up-to-date documentation increases organisational vulnerability.

Finally, organisational growth, the introduction of new regulations, or the need for technological development may require a rapid expansion of information security capacity. However, quickly increasing the size and expertise of an internal team is both demanding and time-consuming.

In contrast, external service providers tend to offer greater flexibility and can adapt their services to specific organisational needs, for example through SOC (Security Operation Center), penetration testing or specialised consulting.

In addition, the acquisition, operation, licensing, and updating of information security tools (e.g., SIEM, IDS/IPS , authorization management systems) represent significant costs that the organisation must bear when relying internal solutions. These costs are often underestimated and extend beyond the initial purchase covering maintenance, expert support, integration, and training.

As mentioned earlier, continuous and accurate documentation is essential for maintaining the transparency in internal information security tasks including job descriptions, policies, incident logs, regular reports, traceable risk analyses, etc. However, the preparation, maintenance, and regular updating of these documents is time-consuming and labour-intensive processes, putting a significant burden on the organisation and potentially diverting attention from day-to-day operational defense.

In contrast, external service providers and consultants contribute up-to-date market insights and technological expertise gained through working with multiple organisations. Relying solely on internal resources risks fostering a narrow perspecitve, which may lead to an unrealistic assessment of the organistion's information securiy maturity and a failure to recognise emerging challanges and market trends.

Ultimately, the decision on which approach to adopt rests with the organisation's management, who must evaulate these factors the light of the organisation's specific needs. Strong management commitment and adequate budget allocation are crucial for the successful implementation and operation of the internal information security model.

Based on roles, the following may be taken into account (example)

Role	Responsibility / Tasks
Executive officer / senior management	- Overall management of the organisation's cybersecurity strategy and operations - Ensuring compliance with NIS2 and Kbtv. requirements - Accepting of risk levels, approving the allocation of necessary resources
Cyber security officer (e.g. CISO)	- Development and continuous improvement of information security management system - Risk management, policy development, awareness raising - Coordination of audits, preparation of reports, and incident management
IT manager/system administrator	- Operation and maintenance of technical security protection - Managing system updates, logging, access control - Technical analysis and coordinating response to incidents
Risk management officer	- Coordinating annual risk assessments - Monitoring risk mitigation measures
Incident management officer / CSIRT liaison	- Receiving, analysing, and reporting cybersecurity incidents - Liaising with the NBSZ NKI (National Cyber Security Institute) - Ensuring timely reporting (24-72 hours)
HR and training officer	- Cybersecurity awareness and training management - Managing security training related to access control and related policies - Familiarisation with relevant rules and regulations
Data Protection Officer (DPO) (if applicable)	- Ensuring the protection of personal data - Coordination between GDPR and NIS2 requirements
Business continuity manager	- Coordination the development and maintenance of business continuity plans (BCP) and emergency procedures - Integrating cybersecurity risks into business continuity and recovery scenarios

Role and responsibility matrix (short sample)

Activity	Management	CISO	IT	HR	DPO	CSIRT
Risk analysis approval	R	A	C	C	I	I
Update of the Rules	A	R	C	C	C	I
Start of training	C	C	I	R	I	-
Incident report to NKI	I	C	C	-	-	R
Backup and access management	-	C	R	-	-	I

R – Responsible
A – Accountable
C – Consulted
I – Informed

4.2. Required skills and certifications for the information security officer

Who needs an Information Security Officer (ISO) and why?

Given today's cybersecurity landscape, the presence of an Information Security Officer (ISO) is no longer optional but increasingly vital for organisations fofr all types and sizes. As reliance on IT systems continues to grow, so does the need for structured, and strategic cybersecurity leadership. The ISO serves as a central contact point between business needs and IT capabilities. Combining project management skills with both technical insight and business awareness, the ISO ensures that cybersecurity measures are effectively implemented and aligned with organisational goals and expectations.

Expected skills, common misconceptions

The common misconcenption among managers is that the information security officer must lready hold a leadership position, simply because the title includes the word „officer." At the other end of the spectrum, some assume that the system administrator or IT manager is the natural fit for the role. While either approach may be appropriate in specific cases, both are often flawed starting points.

The core issue lies in the potential conflict of interest between IT operations and information security. The primamry goal of IT is to ensure systems function run smoothly and continuously, whereas information security focuses on protecting data and reducing risk—even if that requires implementing controls that may restrict functionality. Balancing these priorities demands a certain degree of independence and strategic perspective.

Beyond technical expertise incybersecurity, an effective ISO must also have strong interpersonal skills – or so-called soft skills such as:

- being team-oriented and collaborative a team player,
- strong communication skills,
- effective conflict management,
- good mediation abilitites,
- the ability to handle stress,
- capacity to respond quickly to new situations.

The ENISA European Cybersecurity Skills Framework (ECSF) role descriptions along with its mapping to NIS 2-related tasks offers valuable guidance on competences and skills expected from an ISO.

Who is required to have an ISO, legal background

In some organisations, the appointment of an ISO is not optional, but a legal requirement. Organisations covered by the Cybersecurity Act are required to appoint an ISO. Guidance on eligibility is provided by the Government Decree and EM Decree No. 17/2025

Who is required to appoint an ISO – public sector

However, the Cybersecurity Act distinguishes which entities are required to appoint an ISO. Specifically, designated administrative and state bodies must meet certain criteria when makind such appointments, and these must be reported to the NKI. Anyone wishing to serve in this role must be listed on the NKI ISO register. Currently, the following requirements apply for registration:

- Have a higher education degree
  A diploma is required, classified at least as Level 6 under the Hungarian Qualifications Framework. The field of study is not restricted.

- Professional qualifications
  One of the following qualifications must be held:
  - Electronic Information Security Manager,
  - Certified Information Systems Auditor,
  - Certified Information Systems Manager,
  - Certified Information Systems Security Professional,
  - Certified in Risk and Information Systems Control.
- Or at least 5 years of proven professional experience in the following areas
  - Design, development or operation of information security management systems
  - Information security auditing or monitoring,
  - Information security risk analysis,
  - Information security certification,
  - Information security testing (ethical hacking).

Who is required to do this - economic sector

Unlike in the public sector, where the appointment of an information security officer (ISO) must be reported to the NKI or SZTFH (depending on specific regulatory requirement), economic organisations have greater felxibility in designating who fills this role. While the criteria outlined above serve as a useful starting point, the organisations should carefully consider their specific needs and circumstances when selecting an ISO. In general, an ISO has one of the three professional backgrounds:

- technical, mainly IT graduates with a strong IT background, who also familiar with business processes and have some knowledge of legal aspects;
- economic professionals, who are competent in organisational processes, and have solid IT konwledge, enabling effective communication with IT teams and handling legal issues;
- legal experts, who have a thorough understanding of applicable laws and regulations, as well as sufficient knowledge of business operations and IT, allowing them to communiate effectively across departments.

This illustrates that the ISO is a professional involved in multiple areas with a broad knowledge base, However, deep expertise in every field is not expected, as it is not a formal requirement.

Cybersecurity training

Cybersecurity and data protection traning courses are now widely available in the US. and provide solid foundation for those pursuing the role of an ISO. These courses often cover the key focus areas and specializations discussed above. If an organisation intends to appoint one of its own employees as an ISO, the following training programs serve as an excellent initial step for acquiring the essential knowledge. Currently, these courses include:

Basic training

- Óbuda University - Cyber Security Engineering,

Master's degree

- Óbuda University - Cyber Security Engineering,
- National University of Public Service - Master's degree in Cyber Security,
- Széchenyi István University - Law of Modern Technologies and Cyber Security,

Specialized continuing education program

- National University of Public Service - Electronic Information Security Manager,
- Óbuda University - Information Security Engineer/Specialist,
- Széchenyi István University - Certified Cyber Security Consultant,
- Gábor Dénes University - Data Protection and Information Security Manager.

05

Risk management framework development

The development of a risk management framework is fundamental requirement for compliance with the NIS2 Directive, ensuring the continuous protection of an organisation's operations and services. Its objective is to establish a comprehensive system that enables the identification and assessment of cybersecurity risks and mitigates their impact through appropriate and proportionate measures. Risk management is not a one-time activity, but a continuous, iterative process that adapts to the evolving technological landscape and threat environment. A well-structured framework supports informed decision-making, strenghtens organisational resilience, and provides the foundation for long-term information security maturity. The purpose of this chapter is to demonstrate that a risk assessment framework is not merely a compliance obligation, but a cornerstone of effective, sustainable cyber defence and organisational resilience.

5. Risk management framework development

Written by: György Arató, Bálint Ács, Péter Bódis, János Gedra, Dr. Andrea Jeney, Péter Maczkó, Róbert Major, Csaba Mészáros, Ferenc Molnár, Krisztina Szűcs

5.1. The risk management framework

The NIS2 Directive has fundamentally reshaped the approach to risk management. Risk assessment is no longer merely an administrative obligation, but a central pillar of organisational resilience. The risk-based approach extends beyond traditional IT systems, to encompass the entire IT ecosystem - including technologies, processes, and human factors - and becomes an integral component of corporate governance. At the same time, it establishes the foundation for security maturity and plays a critical role in ensuring regulatory compliance.

The purpose of the risk assessment framework is to systematically identify, evaluate and manage information and cybersecurity risks that may jeopardise the continuity of the organisation's operations or the reliability of its services. To achieve this, a comprehensive approach is required, that integrates risk assessment into the organisation's broader governance, control structures, and management systems. Only through such integration can security management operate not as standalone activity, but an essential and embedded element of organisational practice.

It is important to emphasise that risk assessment is not a one-off exercise, but an iterative, cyclical process that demands regular review and continuous monitoring. Only in this way can an organisation effectively adapt to technological developments, emerging threats, and an evolving regulatory landscape.

5.2. What should a risk management framework include?

The purpose of the risk management framework is to enable the organisation to identify, assess, and manage IT and business risks through appropriate measures before they escalate into actual problems. High-level guidelines alone are not sufficient; a practical and actionable framework must be established, one, that integrates day-to-day operations and provides tangible protection against cyber threats. This can only be achieved by clearly understanding of the framework and its core elements.

The framework rests on a comprehensive, structured, and continuously updated risk management process. This process follllows a logical workflow that guides the organisation step by step from the identification of threats to the implementation of targeted protective measures. For the framework to deliver real value, it must be underpinned by the following core elements.

1. Organisational governance: clearly defined roles, responsibilities, authorities, procedures, and decision-making mechanisms that establish who is authorised toact, at what stage, within which part of the risk managament proccess.

2. Risk assessment methodology: a well-documented, transparent procedure for identifying threats, assessing their likelihood and potential impact, and classifying risks according to severity. This methodology should also reflect the organisation's specific context and regulatory obligations (e.g., Cybersecurity Act, MK Decree, GDPR).
3. Threat and vulnerability catalogue: a tailored list of the most relevant threats and vulnerabilites that may affect the organisation's eletronic information systems, data assets, and operational processes[28]. This is not a generic inventory, but a risk map aligned with the organisation's specific technological, physical, and human environment.
4. Assessment and decision templates: Practical templates and forms that support the consistent documentation, classification, and monitoring the risks throughout the assessment process.
5. Action plan: a structured set of immediate and long-term protective measures, including milestones and responsitilites. Risks can only be managed effectively if countermeasures are clearly defined, assigned to responsible individuals and supported by deadlines.
6. Review and update process: the information security environment is dynamic and constantly evolving. Therefore, the framework must also include provisions for periodic reviews, regular audits and extraordinary updates. An outdated risk analysis can cause more harm than benefit.
7. Integration with other control systems: a risk management framework is most effective when integrated seamlessly with other regulatory and operational areas such as data protection (data protection impact assessment, DPIA), business continuity, incident management, change management, or IT operations.

A risk management framework is not merely a collection of documents. It becomes truly effective whan it serves a pratcical decisin-making tool for management, IT professionals and business units. A thoughtfully designed framework can identify when an electronic information system is at risk or when a business process involves data that needs stronger protection. This approach not only guarantees legal compliance but also mitigates financial losses, reputational damage, and operational disruptions.

In practice, the most important question is: „What will we lose if this system is damaged, failed, or data were lost?" If this question can be answered honestly and comprehensively at the system level, it demonstrates that a genuinely effective risk management framework is in place.

5.3. Should risk management be integrated into the existing framework or operate as a standalone system?

The aim of the NIS2 Directive is to ensure a high level of cybersecurity across the EU. Under the Cybersecurity Act, affected organisations must implement risk-based information security management. A key component of this requiremen is the development of a risk framework, which may either be integrated with existing systems or managed as a standalone framework.

To support decision-making, we have compiled the advantages of an integrated risk framework alongside potential concerns regarding intergation in the tables below.

28 Annex 3 to the MK decree

Arguments in favour of integration:

Argument	Explanation
Uniform management	Easier management support and transparency
Cost efficiency	Reuse of existing tools and processes
Audit synergies	ISO, GDPR and NIS 2 audits can be coordinated
More effective training	Uniform security culture
Better incident management	Faster response and reporting
Supplier compliance	Easier supply chain compliance
Management support	Less internal resistance
Focused operations	NIS2 becomes part of overall governance

Arguments against integration:

Argument	Explanation
Regulatory conflicts	Difficult to harmonise different structures
Increased complexity	More complicated compliance model
Slower implementation	Requires more coordination and validation
Auditability difficulties	NIS2-specific elements are more difficult to separate
Internal resistance	Organisational changes are more difficult to accept
Loss of focus	NIS2 may be overshadowed by other regulatory requirements

The decision to integrate the NIS2 risk framework within the organisation or manage it separately is a strategic one, to be made based on the specific characteristics of the organisation rather than a one-size-fits-all solution. The arguments and counterarguments clearly demonstrate that both approaches offer distinct advantages and face unique challenges.

The integrated model is beneficial for organisations with a mature information security framework, such as ISO/IEC 27001 certification, seeking long-term, sustainable, and cost-effective compliance. Factors such as the flexibility of the existing management structures, strong leadership support, and the ability to coordinate audits all contribute to making integration valuable from both a technical and a business perspectives.

However, there are situtations where managing NIS2 requirements separately may be more appropriate - such as when the organisation's current structure is rigid or overburdened, or there is internal resistance to modifying existing procedures.

Separate management of NIS2 requirements can facilitate expedited implementation, simplified audit procedures, and provide clear definition of responsibilities, making it more compatible with certain organisational cultures.

The ultitmate goal is not merely to achieve compliance, but to establish a risk management model that delivers real added value to the organisation through business stability, reputation protection, and operational security.

Regardless of the choosen option the organisation will be on the right path if it develops the framework with a strategic mindset, actively collaborates with stakeholders, and maintains clear focus on its uniqe characteristics and long-term security objectives.

5.4. Availability requirements

The aim of NIS2 Directive and the corresponding Hungarian legislation is to ensure that all organisations guarantee the continuous availability of their systems and data in a transparent, measurable and auditable manner, even in the event of unexpected incidents. Achieving this goal requires a comprehensive approach that includes risk identification, application of business impact analysis (BIA) (see:5.5.1 . chapter methodology, development of backup

and recovery processes, use of high-availability technical solutions, employee training, management accountability, supplier compliance, and ongoing testing.

In accordancce with legal requirements, all organisations must regularly assess the risks to their IT systems (e.g., cyberattacks, hardware failure, natural disasters). Appropriate technical and organisational protective measures must be implemented to mitigate these risks (such as firewalls, access management, up-to-date software, adequate physical protection, etc.). It is crucial that all emlpoyees must be aware of fundamental information security principles and understand the steps to be taken in the event of an incident.

Organisations are also required to perform regular data backups, ensuring that at least one copy is stored a physically or logically separate location. The success of backup restoration processes and the effectiveness of protective measures must be tested on a regular basis. Furthermore, system status and backup integrity must be continuously monitored and validated.

Continuous availability of services is maintained through the use of redundant (backup) servers, network devices, load balancing and automatic failover solutions. These measures ensure that in the event of a failure, the service is not completely disrupted, as the backup systems take over operations without delay. For components within the critical path, multi-layer redundancy and automatic failover must be implemented. In higher security classifications, alternative operating sites such as backup servers or cloud services must also be provided to further enhance resilience.

Based on the outcome of the BIA, a business continuity plan (BCP) should be developed to support prioritisation of recovery activities. In addition, a disaster recovery plan (DRP) must also be prepared, outlining the specific steps required to restore operations after an unexpected event.

Availability is determined not only by the independent operation of individual systems, but also the interdependencies among them. The failure of one service can trigger a cascading effect across systems. Therefore, it is necessary to identify all dependencies within the system architecture. Recovery plans must clearly define the order of dependencies and establish recovery priorities so that the fundamental components, the „bottom layer" (e.g., network, power supply) can be restored as early as possible.

Critical services are expected to maintain an annual availability of at least 99.9%, corresponding to a maximum allowable annual downtime of 8.76 hours. Availability can be calculated using the following formula:

Availability (%) = ((annual operating time – downtime) / annual operating time) × 100

> For example, if a service operates 24 hours a day, 365 days a year (365 days × 24 hours = 8760 hours), and downtime – e.g. planned maintenance, changeovers or outages due to faults – amounts to 8.76 hours per year (which is 0.1% of the total annual operating time, i.e. 8760 hours), then the availability is:
> ((8760 – 8,76) / 8760) × 100 = 99,9%

If IT operations are partially dependent on external partners (e.g., cloud service providers, hosting services, or IT operations), requirements related to availability, backup, and recovery must be cleearly defined in their agreement. These requirements should be regularly monitored (e.g., through an SLA, or service level agreement). In addition to SLAs, it may also necessary to conclude similar agreements within the organisation, between departments or operational units. These are referred to as Operational Level Agreements (OLAs). The purpose of OLAs is to precisely outline service levels, responsibilities, and mutual expectations between internal service providers and users,

thereby supporting the fulfilment of external obligations defined in the SLA.

Effective incident and maintenance notification rely on two key records:

- Stakeholder register: This contains the contact details of individuals and organisational units affected by incidents or maintenance activities, along with the required communication channels and specific notification requirements.
- Notification chain (escalation matrix): A documented process that defines who must be notified in the event of a fault or maintenance, in what order, through which channels and within what timeframes.

Both records can be maintatined in Excel or an IT Service Management system, ensuring that communication remains consistent, traceable, and aligned with orsanisational standards. When applied together, they ensure, that all affected parties are notified promptly, in the appropriate format and seqence, during system outages or urgent maintenance.

5.5. Data assets and the role of busienss impact analysis (BIA) in IT service management

An organisation achieves its objectives by delivering products and services to its customers. To maintain continuity, it must implement and sustain processes that systematicaly-ly analyse business impacts, assess the risks of disruptions, and support the development of effective business continuity strategies and solutions.

Business impact analysis (BIA) helps the organisation identify and prioritise interrupted whose interruption may require urgent recovery, as failure to resume them quickly could result in unacceptable damage. In some cases, dependent activities may also need to be prioritised due to their reliance on others. The analysis should cover all activities within the scope of the business continuity management system (BCMS).

The first step in the BIA process is to rank products and services based on ther criticality. This is followed by a series of optional BIA processes and activities. While individual business impact analyses may have limited scope, together they must comprehennsively cover the entire BCMS.

5.5.1. The BIA process

The BIA should be conducted following a predefined process, which consists of the following steps:

BIA Planning

The main steps in the BIA preparation phase are as follows:

- Identification of necessary resources,
- Grouping products and services,
- Identifying key stakeholders in the processes,
- Communicating expectations to participants,
- Developing a BIA plan.

BIA acceptance of the process approach

In order to successfully implement BIA, the organisation must develop a framework that constantly manages impact identification, criteria definition, and time frame setting. The following key considerations apply:

- Understanding impacts: The BIA process systematically identifies the organisational impact of disruptions affecting the delivery of products and services. These disruptions can originate internally, within the supply chain, or from other external sources, potentially causing interruptions

to one or more products or services delivered to customers and other stakeholders.

- Defining impact types and criteria: Impact types differ from consequence types or categories used in risk management. Impact refers specifically to the effect of a disruption on the organisation. The selection of impact types and criteria depends on the organisation's industry, context, and nature of activities, as well as its organisational culture. Choosing appropriate impact types and criteria, including whether to gather quantitative and qualitative data and what level, enables the organisation to effectively establish or validate its business continuity priorities and requirements.
- Time frame: Impacts typically worsen over time, but the rate of increase can vary. To measure the extent of these impacts as time progresses, the organisation may define specific assessment intervals (e.g., 1 hour, 6 hours, 24 hours, 3 days, 1 week), or use time ranges (e.g., 0 to 1 hour, 1 to 6 hours, 6 to 24 hours) and examine how the impact intensifies within those periods. These intervals should be tailored to the organisation's specific context and operational needs.
- Methodology definition: A consistent methodology should be developed to ensure that the same principles and criteria are applied when assessing all products, services, and activities, regardless of when the assessment is conducted or by which team.
- Additionally, the maximum tolerable period of disruption (MTPD), the point beyond which the disruption is unacceptable, must be defined. The recovery time objective (RTO) which specifies the time frame for restoring interrupted activities, should also be established. It is important that the RTO does not exceed the MTPD.

Definition of products and services with the involvement of senior management

The purpose of this process is to clearly define the priorities of the products and services provided by the organisation along with their associated continuity requirements, based on senior management's guidance:

- Overview: Senior management must establish the priorities of the products and services delivered by the organisation to its customers.
- Defining inputs: Service priorities are strongly influenced by customer needs, applicable legal requirements, and the consequences of non-compliance. These factors must be collected and analysed in advance to support informed decision-making.
- Defining product and service priorities: In line with the accepted methodology, senior management must determine, for each product and service group the maximum period for which a failure to deliver can be tolerated before it becomes unacceptable to the organisation. This determines the minimum acceptable capacity for initial recovery and the timeframe for restoring full capacity.
- Results: The results should be a ranked list of products and services with their corresponding continuity requirements, which then serve as the basis for prioritising related activites.

Identification of priority activities

The purpose of this process is to enable the organisation to clearly identify and prioritise the activities that are critical to maintaining the continuity of its products and services. To achieve this, the impacts, timing requirements, the interdependencies of activities should be

assessed using a consistent and structured methodology:

- Overview: The priority of products and services directly influences the priority of the activities that support them. When an activity forms part of a broader business process, it may need to be analysed in conjunction with related activities within that process.
- Defining inputs: The follwing inputs are required to assess and rank activities: (1) the defined scope of the BIA process; (2) agreed impact types and criteria; (3) product and service priorities defined by senior management; (4) known internal and external dependencies; (5) legal, regulatory, and contractual obligations.
- Identifying activities: For each product and service within the scope of the BIA process, the associated activities must be identified along with the individuals or roles responsible for them.
- Setting RTOs for activities: Based on the defined impact types and criteria, time frames, and the accepted methodology, those responsible must evaluate the consequences of potential disruptions. This includes determinig the MTPD, and setting the RTO, which defines the maximum acceptable time for restoring the activity.
- Identifying prioritised activities: Based on the RTO, a list of priority activities should be compiled. These activities require continuity strategies and solutions, which must be reviewed and approved by senior management.
- Results: The output of this process is an approved list of prioritised actvities: (1) Interdependencies and relationships between products, services, and activities; (2) assessed time-based impacts; (3) defined MTPDs; (4) defined RTOs; (5) minimum acceptable capacity levels.

Identification of resources and other dependencies

After identifying priority activities, the organisation should conduct a thorough assessment of the resources and related dependencies necessary for their operation, recovery, or ongoing maintenance. The purpose of this process is to provide a detailed understanding of daily resource requirements and conditions needed to support their continuity:

- Identifying resource and other dependency requirements: Once priority activities have been identified, the organisation should gather an in-depth overviev of the daily resource requirements necessary to support restoration or or continued operation of these activities.
- Resource requirements: For each identified resource, the following information should be collected: (1) quantity, the amount or number of resources required over time; (2) availability time frame(s), when and for how long the resource must be available; (3) characteristics of the resource; - specific attributes or features relevant to a resource (4) maximum tolerable loss of information resources; (5) dependencies: reliance on other resources; (6) applicable legal or regulatory requirements, that must be taken into account.

Analysis and consolidation of BIA results

The organisation should conduct a final analysis (or, where necessary, a consolidation of multiple analyses) that involves reviewing all validated and approved information collected throughout the BIA process.

The organisation should select an appropriate combination of quantitative and qualitative analysis methods, taking into account factors

such as the type and size of the organisation, its operational context, and the resources available.

Senior management approval of BIA results

The organisation should present the following key BIA outcomes available to senior management for review, possible modification, and formal approval before moving forward:

- prioritisation of products and services
- business process ranking (if conducted),
- ranking of activities
- confirmation of the original BIA scope or approval of the revised BIA scope.

Review of the BIA

Regular review of the BIA ensures that both the process and its outcomes are always remain current and aligned with the organisation's evolving operations, environment, and risk landscape:

- Review of the BIA process and methodology: The BIA process and methodology should be peridocally reviewed to support continuous improvement. Over time, adjustments will be needed to enhance the quality of results such as revising impacts types, time frames, data collection methods, or the individuals involved in the process.
- Review of BIA results: BIA results should be reviewed regularly (typically annualy) or whenever significant changes occur within the organisation or its operating environment that could influence business continuity priorities and requirements. In organisational areas that have remained mostly unchanged since the previous BIA, a full re-analysis may not be necessary; instead validation of existing results may be sufficient.

A well-prepared BIA delivers critical insights that enable the organisation to prepare for unexpected disruptions and maintain business continuity.

5.5.2. Expected results

The expected results are listed below:

Strategic results

- Identification of critical business processes: enables the organisation to determine which activities are essential for maintining operations.
- Setting priorities: supports the ranking processes based on their importance, helping to identify which ones must be restored first in the event of a disruption.
- Determination of response times and tolerable outages: defines values such as RTO (Recovery Time Objective) and RPO (Recovery Point Objective), to guide recovery planning and acceptable limits for downtime or data loss.

Operational results

- Mapping resource requirements: identifies the human, technological and financial resources needed to maintain critical business processes.
- Quantifying risks and impacts: enables the estimation of financial losses, customer attrition or reputational damage.
- Establishing a business continuity plan (BCP): develops a targeted emergency response plan based on the findings of the BIA, outlining how to maintain or quickly restore operations during a disruption.

Protection and recovery benefits

- Development of recovery strategies: involves palnning solutions, such as alternative work locations, backup systems or communication protocols to support rapid recovery.
- Faster emergency response: with a BIA in place, the organisation can respond more quickly to emergencies and also take proactive measures to prevent serious damage.
- Maintaining customer trust and reputation: ensuring operational continuity helps to prevent customer loss and preserves the organisation's reputation from negative perceptions.

5.6. Mapping business processes

Mapping business processes is a crucial step toward achieving efficient operations, digitalisation, risk management, and information security. It offers transparency into how an organisation functions, highlights bottlenecks, and identifies opportunities for process development. Additionally, it supports legal and regulatory compliance (such as NIS2, ISO 27001) and facilitates auditing and business continuity efforts.

Methodologies for mapping business processes

- Business Process Management (BPM): A structured approach encompassing process design, modeling, implementation, monitoring, and optimisation.
- Buisness Process Reengineering (BPR): Radical redesign of processes to achieve significant improvements in performance, efficiency or quality.
- Process map and sequence diagram: Visual tools that depict process steps, decision points, involved actors/resources, and data flow.
- Impact analysis and risk analysis: Assessment methods used to determine the importance/criticality and vulnerability of business processes.

The first step is to define and standardise the processes that deliver these services, followed by their optimisation and eventual automation. This approach ensures the professional delivery of business and support services, aligned with the Service Level Agreement (SLA,) and Operational Level Agreement (OLA). Mapping business processes not only supports business objectives, but also enhances process maturity and can drive the achievement of new business goals.

Business and support processes are documented and managed using various tools, including the service catalogue, process catalogue, data asset inventory, and system component inventory.

The maturity level of business processes reflects how effectively an organisation manages, develops, and optimises its processes. These maturity models are commonly used to assess organisational performance and identify areas for improvement.

The NIS2 requirements place particular emphasis on the control and transparent operation of processes, especially those supporting information security. The goal is to ensure that business operations are carried out securely and sustainably over the long term.

This includes, but is not limited to, the authorisation and procurement processes for EISs, development and deployment procedures that security by design and security by default; configuration management, testing and bug-fixing processes, as well as training and maintenance management. Equally important are change management, event and incident management, communication and onboarding processes, access management, logging and

Steps for mapping business and support processes

1. Define objectives: Which areas are we focusing on? (e.g., IT, HR , procurement, etc.)
2. Involving stakeholders: Who are the key players? (e.g., process owners, implementers, managers) + Workshops, interviews, understanding actual operations
3. Identifying processes: Documentation, regulations + Main and sub-processes, critical processes
4. Detailed mapping of process steps: Who does it? What do they do? What tools do they use? What is the output?
5. Process analysis: Bottlenecks, parallelism, redundant steps + Where can it be automated?
6. Development of optimisation proposals: Simplification, digitisation, standardisation + Definition of Key Performance Indicators (KPIs) for measurability
7. Documentation and communication
8. Continuous review: Regular audits, collection of feedback + Updating processes in line with changes.

control mechanisms, supervision of security measures, information security measurement and control activities, business continuity and risk analysis procedures, vulnerability management, management of the entire life cycle of EISs. This also involves ensuring encryption, anonymisation, and supplier relationship managament, and maintaining supply chain security.

5.7. Risk analysis, considering supply chain risks

So far, we have examined the general aspects of risk analysis at the system, processes, and resource levels within the organisation. However, for comprehensive risk management must also address risks inherent in the supply chain, whether involving suppliers, service providers, logistics partners, or external data processors. These factors can directly impact on the organisation's operations, making it essential to analyse them thoroughly and integrate them into the risk management system.

Risk management follows a three-step cycle that should be applied specifically to the unique characteristics of the supply chain as well.

Risk identification

Systematic mapping of potential sources of danger; the European Union Agency for Cybersecurity (ENISA) underscores the significance of supply chain attacks in several of its publications[29]. Idenfifying key risk areas, vulnerabilities, or exposure factors within the supply chain encompasses:

- Human and operational risks: Data leaks and data breaches, service outages (e.g. due to ransomware attacks), or intentional or accidental damage caused by supplier employees (insider threats) and incidents stemming from poor cybersecurity awareness or insufficient training.
- Software supply chain: Insertion of malicious code into the delivered software or its open source (OSS) components, as seen in the SolarWinds incident.

29 e.g.: ENISA THREAT LANDSCAPE 2024 September 2024. DOI: 10.2824/0710888.

- Hardware supply chain: Deployment of manipulated or counterfeit hardware devices or components within the infrastructure.

Risk assessment

Once identified, the risks should be prioritised accordidng to their severity.

Risk = Probability of occurrence x Impact

Risk is commonly assessed as the product of two key factors: the probability of occurrence and the impact. The probability of occurrence reflects the likelihood of an undesirable event happening within a given timeframe, while the impact measures the potential consequences of an event in financial, operational, or reputational terms.

For instance, a ransomware attack on an automotive supplier could cause a 5% drop in production at the customer ’s facility due to supply chain disruption. This highlights how risk can extend beyond the immediate target, resulting in significant downstream business impacts.

Risk management

For each identified risk, a decision must be made on how to address it. The four main risk response strategies are:

- Acceptance: The risk is considered low, and it is consciously accepted without additional action.
- Reduction: The risk is mitigated by implementing controls and safeguards. This is the most commonly used strategy.
- Transfer: The financial impact of the risk is shifted to a third party, typically through instruments, such as cyber insurance.
- Avoidance: The activity that gives rise to the risk is discontinued or modified to eliminate the risk entirely.

06

Identified EISs and system components

The implementation of the NIS2 Directive in Hungary aims to enhance the overall level of information and cybersecurity. It introduces new concepts and obligations for organisations and service providers. One of the most important of these concepts is the Electronic Information System (EIS). An EIS is not merely a collection of technical tools, it is a complex, functionanly integrated system that handles data, provides services, and directly influences az oganisation's operation.

This chapter aims to clearly define of what is meant by an EIS, how these components can be identified and grouped, and the criteria by which these systems should be classified into security categories. The objective is not only to ensure reegulatory compliance, but also to support the conscious and sustainable development of an organisation's cyber resilience.

6. Identified EISs and system components

Written by: Dr. Ágota Albert, Gergő Barbul, Péter Bódis, Tamás Lóth, Péter Maczkó, Róbert Major, Edina Mandrik, Márk Máté, Dr. Balázs Gergely Tiszolczi

6.1. What qualifies as an EIS?

EIS as a definition

Current legislation provides the following guidance for understanding the concept of an EIS. Based on the definition set out in the Cybersecurity Act, Interpretative provision, Section 4, Point 24, electronic information system - EIS is defined as follows:

„a) an electronic communications network as defined in the Electronic Communications Act,

[Act C of 2003 on electronic communications, Section 22 Definition of electronic communications network: systems based on a fixed infrastructure or centrally administered capacity allocation, enabling the transmission of signals by electronic means using electronic communications equipment, and, where applicable, switching or routing equipment and other resources, including non-active network elements. Electronic communications networks include, in particular, satellite networks, fixed networks (wired or wireless) and mobile radio telephone networks; energy supply cable systems to the extent that they are used for the transmission of signals; and broadcasting networks.

b) any device or group of interconnected or interrelated devices, one or more of which, pursuant to a program, performs automated processing of digital data, including cyber-physical systems; or

c) digital data stored, processed, retrieved or transmitted by the elements referred to in points (a) and (b) for the purposes of their operation, use, maintenance and repair;"

The above definition allows for multiple approaches to identification and interpretation. However, it is preferable to understand EIS as a legal category rather than purely an IT term, where it is typically viewed as a collection of IT systems or solutions from a particular organisational perspective. Conseqently, an EIS cannot generally be equated with a single specific IT system, but should be understood as a set of interrelated IT solutions.

The following chapters provide further guidance on identification and classification of EISs. However, before proceeding, it is worth reviewing what should not be identified or considered as an EIS.

Why is it important to identify EISs?

- Impact on audit fees: according to the SZTFH decree, the number of EISs directly affects the cost of cybersecurity audits and regulatory oversight fees.
- Basis for risk management: Proper identification of EIS-related risks is essential for ensuring NIS2 compliance
- Security classification: as stipulatd in the MK Decree, all EISs must be classified into security categories and assigned the appropriate protective measures.

What is not identified as an EIS?

The review and interpretation of the legislation reveals that organisations do not receive detailed guidance enabling them to clearly distinguish which elements should be identified as EISs and which IT solutions fall outside this scope.

The key to accurate EIS identification lies on considering critical dependencies, the significance of business processes, associated risks, while constantly treating IT systems as functional units.

Therefore, it is recommended to carefully review these factors, particularly business processes and risks, before proceeding with identification. Furthermore, individual IT solutions should be assessed and prioritised based on their criticality and overall importance.

Once this assessment is completed, it can be used to determine which solutions should not be classified as EISs, either because they are unrelated to core business activities or their risk level does not justify inlusion under the principle of risk-proportionate protection.

Primary and supporting system components

An EIS is a logical unit of interrelated IT components that serves a specific business or administrative purpose. When defining the EIS, the primary consideration should be delimiting the system based on business functionality rather than technical elements. The infrastructure components – including the networks, servers, operating systems, applications, data, operational processes and associated personnel – together form a unified system that ensures the operation of business or administrative processes.

As explained in the previous chapter, correct EIS identification relies on recognising critical dependencies, assessing the importance of business processes, and considering risk factors, while treating the system as a consistent, functional unit. This approach ensures that security, compliance, and business continuity genuinly support the organisation's operations.

Most of an organisation's EISs are under its own control, supervision, and operation. However, some systems may exist over which the organisation does not exercise direct control. This category covers information systems whose management, development, operation, supervision, or core infrastructure is provided not an external service provider or government agency. Examples include Software-as-a-Service (SaaS) applications operated by external cloud providers, as well as information and communication systems supporting electronic public services that are centrally managed by the government.

EISs comprise both the technical and human elements used to manage digital data and play a critical role in the operation and protection of business processes. What qualifies as a business-related system? Typical examples include:

- ERP systems (e.g., SAP, Navision)
- CRM systems (e.g., Salesforce, MiniCRM)
- HR systems (e.g., Nexon, Workday)
- Financial and accounting systems
- Production management systems (MES, SCADA)
- Document management systems (DMS)
- Web platforms, webshops, customer portals
- Mobile applications and APIs

These systems should not be listed in the EIS register as being under the organisation's direct control, since in such cases its responsibiltiy is limited. Nevertheless, the risks arising from their use must still be addressed and managed.

When defining EISs, components may be categorised into primary or supporting system elements depending on their role. Primary system elements are those components that

directly support the business or administrative process covered by the EIS and ensure its essential functioning. Without them, the process could not operate or interact effectively.

Supporting system elements are components that do not directly drive the business or administrative proces, but are nevertheless essential for operation. They often provide background processes or supplementary services and may be linked to multiple EISs rather being exclusive to a single EIS. While their role is supportive, they role is indispensible for ensuring the secure and operational functioning of the entire system.

Supporting system components, such as shared infrastructure, authentication services, backup, monitoring, or antivirus solutions, typically serve multiple primary EISs. For this reason, their risk profile and applicable controls may differ from those of individual business or public administration EISs. In such cases, it is advisable to treat these supporting components either as separate EISs or as a dedicated group of supporting EISs with their own responsibilities and risk assessment framework. This approach prevents the primary EISs from becoming unnecessarily complex. Supporting system elements should be defined separately whenever they effect the operation of several EISs. Their risk assessment must be carried out independently, taking into account the impact on the supported EISs, rather than simply transferring risks to the primary system.

Risk-based control selection eneables the adoption of measures that are proportionate to the primary EIS and tailored to the function of the supporting system component. During control selection, a business impact analysis (BIA) is used to assess the business damage caused by component failures and to choose risk-proportionate protective measures. Failures of supporting system components typically result in temporary functional disruption, and a separate recovery plan, such as alternative authentication path, restoration from backup, should be in place to restore their operation.

The foundation for transparent and auditable management of EISs is the maintenance of an up-to-date data asset inventory and system component inventory. These inventories ensure that the organisation has precise knowledge of the data, information assets, and system components it manages, and as well as the EISs to which they belong.

The two inventories complement each other and facilitate the accurate EIS identification, assignment of responsibilities, risk idenification, and the fulfilment of compliance requirements within a unified system.

Systems not owned by the organisation

A key issue in cybersecurity compliance is determining which systems an organisation is responsible for, the boundaries within which it must apply security controls, and the responsibility it assumes for the operation of the system and any incidents that occur within it. This distinction is addreessed in both the Cybersecurity Act and the MK Decree through the concept of „under control." The Cybersecurity Act interprets „under control" as a system belonging to the organisation, to which security classification and protective measures are mandatory. Although the law does not provide aMK precise definition, in practice, being under control means that the organisation governs the system's operation, access, data management, or configuration of the system, regardless of whether it physically owns the system.

Section 2(3) of the MK Decree states: *„Where the organisation's right of disposal extends only to certain elements or functions of the electronic information system, the [...] requirements shall be complied with in respect of those elements and functions."*

This provision expressly recognizes partial rights of disposal and allows for both vertical and horizontal interpretation of system boundaries. Accordingly, the legislation applies the concept of control not only to the entire systems but also to their individual components,

insofar as the organisation's responsibilities extend to them.

This interpretation is corresponds to the concept of „authorisation boundary" as defined in NIST SP 800-37, which refers to the set of components of an information system operated with the approval of an authorised person. This boundary excludes systems that have separate authorisation, even if they are connected to the system under consideration. The purpose of the concept is to establish a clear line for the scope of security controls and to identify who bears responsibility for the security of a particular system. Although NIST SP 800-37 and the Cybersecurity Act originate from different regulatory environments, but they share the common objective of clearly defining responsibilities and security boundaries. Accordingly, the concepts of „control" and „authorisation boundary" can be interpreted consistently to achieve this goal.

When interpreting system boundaries, two dimensions can be distinguished:

- Horizontal interpretation: Different components of a system may be subject to different organisational control.

  For instance, a server may be owned by a company, while the network infrastructure is supplied by the parent company. In this case, only the server falls within the systems at the disposal of the organisation.
- Vertical interpretation: The allocation of responsibilities across the technological layers of a service. In the context of cloud services, the organisation may exercise control even without physical ownership of the system, by controlling the operation of a specific layer, such as application-level access.

Nowadays, due to the outsourcing of digital services, the rise of cloud-based solutions, complex supply chains, and the globalisation of services, it is increasingly common for organisations to utilise IT systems or system components that are not directly under their control. Nevertheless, these systems often process business-critical data or deliver essential services. To ensure cybersecurity compliance and effective risk management, organisations are obliged implement appropriate controls in these cases as well.

The difference compared to systems owned by the organisation lies in the focus needed to meet security requirements. For non-owned systems, emphasis must be placed on establishing contractual safeguards, controlling the supply chain, and managing incidents. Contractual provisions should include precise definition of the service provider's ancillary obligations and, where necessary, mechanisms for their enforcement. It is particularly important to define SLAs in such a way that addresses security and business continuity, as well as expectations regarding the detection, reporting, incident mitigation and response. To ensure compliance, the organisation must have the right to audit - and actually conduct audits of - the service provider. Additionally, it is advisable to establish a well-defined exit strategy in advance to guarantee the safe and controlled termination of the service relationship.

6.2. Security classification guidelines

For organisations, information security is not merely a technical issue, it is a guarantee of reliable operations and the trust of end users and partners. To provide the strongest protection to the areas of greatest potential loss, all electronic information systems (EISs) must be managed according to their respective importance and risk level. This approach underpins security classification: the objective is not to apply uniform, general protection across all the systems, but to make security decisions proportionate to the actual exposure of each system.

In practice, this entails examining what information is processed by a particular EIS and considering the consequences if it were accessed without authorisation (confidentiality), if it were altered or damaged (integrity), or if the system itself were unavailable (availability). These aspects should be assessed not only from an IT perspective, but also from a business and legal perspective – for instance, in the terms of data protection liability, delay in obligations, or customer dissatisfaction.

When determining the security classification, potential threats to the EIS must also be taken into account. These may include physical events (e.g., fire, water damage, power failure), technological risks (software errors, network attacks), human factors (improper handling, unauthorised access), and intentional damage (data theft, sabotage).

In summary, prior to designating a classification, the impact assessment should evaluate the confidentiality, integrity, and availability requirements of the data processed within the EIS, assessing both the potential threats to the EIS and the functionality it provides.

The MK Decree gives a systematic overview of these requirements in Annex 1, Chapter 2, Classification into security classes, and Annex 3, Catalogue of threats.

Based on this framework, EISs can be classified into three security classes:

- Basic (low risk): Systems that do not prorcess sensitive or protected data and whose failure would have only a limited operational impact. Basic technical and organisational measures, such as password protection and periodic backups, are sufficient for these systems.
- Significant (medium-high risk): Systems that process sensitive data (e.g., customer information, financial data) or are important from a business perspective. Their failure could cause significant disruption. Required measures include detailed access control, logging, regular backups, and vulnerability testing.
- High (very high risk): Systems whose failure would immediately bring business oprations to a standstill or result in legal, financial, or serious data protection consequences. Required measures include multi-factor authentication, high availability, incident monitoring, and detailed audit requirements.

Classifying Electronic Information Systems (EISs) into security categories is a complex task, as the actual classification depends on a wide variety of organisational, technological, and risk factors. The examples below are illustrative and do not imply that these systems always fall into the same category, rather they can serve as a starting point for the classification process.

- Basic: asset management systems, internal administrative tools.
- Significant: customer relationship management systems, invoicing programs
- High: central enterprise management systems, partner or authority interfaces.

Classification is not a one-time task. Systems, processes, threats, and the business environment constantly evolve, so classifications should be reviewed at least annually, or immediately following any significant change. It is important to avoid both overestimating or underestimating a system's importance. Classifying all systems as „critical," resources will be spread too thin, whereas underestimating a genuinly sensitive system exposes the organisation to substantial risk.

The result of the security classification determines the required level of protective measures and informs the development of a risk management plan and information security policies. Each EIS should receive precisely the level of attention and protection that its actual risk level warrants -no more, no less.

This proportionate approach ensures that security measures supports, rather than hinder, the efficient and responsible operation of the business.

Operational Technology (OT) systems require special attention during security classification. These systems – such as industrial control systems (ICS, SCADA, DCS) – directly influence physical processes. Their failure can cause business disruption, environmental damage, lead to the shutdowns of critical infrastructure, and in extreme cases, endanger human life. Therefore, in OT environment, it is insufficient to consider IT aspects alone; ensure availability and secure physical operation is paramount.

When applying the MK Decree's catalog of threats, particular attention should be given to OT-specific threats, such as:

- process interruptions (e.g., manipulation of control signals),
- malfunctioning of sensors and actuators,
- exploitation of maintenance access (e.g., malware spread via USB),
- lack of network isolation (e.g., unsegmented OT/IT networks).

Security classification in an OT environment e often results in a critical level, even if the affected system processes low-volume data but has a direct impact on business continuity or human safety. As a result, appropriate physical and logical protections (e.g., dedicated firewalls, physical access restrictions, change tracking) are essential.

6.3. Specific features of OT systems

The NIS2 Directive establishes a uniform set of cybersecurity requirements at European level that applies to both traditional IT infrastructure and industrial control systems. While the overarching goal in both environments is to protect data and processes, the focus of protection, operating conditions, and technological characteristics differ significantly. Consequently, the practical interpretation of NIS2 in industrial environments requires special attention. The following OT-specific security issues are prioritised for achieving compliance.

The security of IT and ICS/OT systems is grounded on the three principles of confidentiality, integrity, and availability (CIA). Building on these pillars, NIS2 mandates the adoption of risk-based security measures, rapid incident reporting, senior management accountability, and supply chain risk management. Key security measures in both IT and OT contexts encompass network segmentation, multi-factor authentication, logging, and encryption of transmitted data.

Although the fundamental principles are the same, the primary area of focus differ. In corporate IT, data confidentiality is a top priority, while in ICS/OT environments, the continuous and secure operation of physical processes takes precedence, making availability and integrity the main concnerns. IT systems typically run in standardised hardware and software environments within controlled, air-conditioned data centres, where regular updates are standard practice. Industrial equipment, by contrast, often operates in harsh environments with lifecycles spanning several decades. Downtime in these settings can result in significant losses, which means updates must be carefulyly scheduled. Updating industrial systems is frequently a business decision, as even a few hours of downtime can have major financial consequences particularly in aging infrastructures. It is advisable to implement interim mitigating measure to address known vulnerabilities that would otherwise be resolved by the update, and all such measures should be properly documented.

At the technological level, IT networks primarily rely on TCP/IP and modern cloud services. Whereas, industrial networks employ specialised protocols such as Modbus, DNP3 or IEC 61850. These environments require real-time control, low, stable latency and ruggedised devices engineered to operate reliably under extreme conditions.

ICS architectures, integrate programmable logic controllers, distributed control systems, remote control units, and human-machine interfaces into cohesive system. Specific security solutions have also emerged, such as CIP Security associated with Ethernet/IP or the built-in authentication and encryption mechanisms of OPC UA.

The ongoing digital transformation is increasingly connecting, IT and industrial environments. IIoT solutions, cloud-based analytics, and artificial intelligence supporting predictive maintenance are creating new links between the two domains, while simultaneously expanding the attack surface. As a result, cyberattacks can now lead not only to data breaches but also to physical damage.

Close collaboration between IT and OT teams, a joint risk assessment process, and the implementation of integrated incident management are essential for compliance with the NIS2 Directive. Senior management must establish a unified strategy covering supplier assessment, 24-hour incident reporting, and comprehensive compliance audits. The use of converged security platforms, the integration of cloud and network security services, and the adoption of OT-specific detection and response mechanisms enable organisations to effectively protect both their information systems and their industrial operations. OT security is not merely an extension of IT policies, but a prerequisite for ensuring operational reliability. Compliance should not be regarded as a regulatory requirement, but as a critical element of maintaining uninterrupted business operations.

When ensuring compliance, it is particularly important to consider the specific operational characteristics of the industrial environment. In OT systems, manufacturing machines often do not support multi-user operation, resulting in operators sharing a technical account. While this practice does not align with traditional role-based access control requirements, it may be justified in certain operational contexts, particularly for quality assurance. In such cases, compensating measures, such as access logging, physical controls, and identification

based on shift schedules can provide adequate secure.

A similar adjustment may be required automatic screen locking, which can cause downtime, restarts, or errors on certain devices. Under these circumstances, alternative controls should be implemented to maintain business continuity, including camera-based surveillance, operator presence verification, or other methods of confirming access rights. All such measures must be properly documented, with consideration given to vulnerability management requirements.

Suppliers and technology partners often provide technical support via remote access. It is essential to regulate such access by making time-limited, logged, routed through a jump server, where possible, and secured with two-factor authentication. Temporary permissions must always be granted in a controlled manner and promptly revoked when no longer required.

Certain OT systems, such as HVAC controls, building automation, and access control systems, are not traditional IT systems. However, due to their business-critical roles, they are classified as electronic information systems (EIS). To comply with NIS2 and relevant domestic regulations, these systems must also be included within the scope of protective measures, with particular attention to availability, accessibility, and recovery requirements.

Integration of new OT devices presents not only a technical challenges but also information security concerns. IP address allocation, VLAN classification, access rights, backup and logging requirements, and firewall compatibility must be agreed upon prior to installation. New system components must undergo an ICS-specific risk assessment before installation and activation and be recorded in the EIS register. Consistent collaboration between IT and engineering teams plays a crucial role in achiving compliance.

.

6.4. EIS selection for SEVESO and critical infrastructure facilities

Regulatory background

The selection of EIS in SEVESO[30] and other critical infrastructure environments is a complex process that must satisfy strict regulatory requirements. Key considerations include achieving an appropriate level of safety, ensuring legal compliance, and guaranteeing long-term support.

Successful implementation depends on thorough risk analysis, adherence to relevant standards, and the application of proactive security measures. The selected system must be capable of adapting to the evolving cyber threat landscape while ensuring the continuos operation of critical business processes.

CER Directive and protection of critical entities

Based on the Critical Entities Resilience (CER) directive, the Act on the Resilience of Critical Entities (Kszetv.) was adopted in 2024, replacing previous regulations governing the protection of critical systems.

The objective of the Act is to enhance resilience: critical entities must be capable of preventing, withstanding, responding to, and recovering from all relevant risks, thereby ensuring the continuity of essential services even during crisis situations.

30 ECHA Understanding Seveso

6.4.1. Specific requirements for SEVESO environments

Safety Management System (SMS)

Hazardous establishments are required to maintain a Safety Management System (SMS) that encompasses technical, organisational, and personnel measures. The EIS must be an integral part of this safety framework and adhere to all applicable legal provisions.

Cyber security integration requirements

SEVESO establishments are required to implement cybersecurity plans and incident management procedures. As a part of the audit process, the following areas a typically examined:

- The functionality of firewalls and intrusion detection systems
- Implementation of network segmentation
- Access management and logging within control systems.

Recommended minimum security requirements for procurement:

- Support for VPN or encrypted protocols for remote communication,
- Capacity to operate in an isolated network without an Internet connectivity,
- Manufacturer's guarantee for updates during throughout the system's lifecycle.

6.4.2. EIS selection process and criteria

Identification of regulations and compliance requirements

At the beginning of the EIS selection process, it is essential to clarify the applicable legislation, including:

- SEVESO regulations,
- NIS 2/CER requirements,
- Sector-specific regulations.

Following this, specific technical and security requirements should be defined, such as:

- For NIS2: logging, incident management, encryption
- For SEVESO operations: SIS integration support,
- Standards assigned to metrics (e.g., „Support for SL2 level according to IEC 62443").

Data protection and access management

Ensuring GDPR compliance:

- Capability for appropriate data segmentation,
- Implementation of role-based authorisation levels,
- Logging of all data access activities.

Security requirements:

- Protection against zero-day vulnerabilities,
- Support for integration with intrusion detection systems,
- Compatibility with endpoint protection software,
- Support for two-factor authentication (MFA) – a basic requirement for critical systems,
- Secure authentication protocols (OAuth2, SAML).

Compliance with standards and technical requirements

Minimum technical requirements:

- Use of products with supported lifecycle,
- Ensuring regular security updates,
- Capability to manage vulnerabilities effectively.

Up-to-date status and support guarantee

Critical requirements:

- Manufacturer support throughout the product lifecycle,
- Regular provision of security patches,

- Scheduled version updates,
- Internal policies (standards) for updates („Critical patches must be installed within X days").

To be avoided:

- Use of outdated software,
- Systems lacking vendor support,
- Solutions without ongoing security updates.

6.4.3. Practical implementation

Risk analysis and protection levels

1. Cyber risk analysis prior to system implementation,
2. Determination of the appropriate Security Level (SL),
3. Implementation of protective measures according to the defined security level,
4. Regular review and update measures to manage evolving threats.

Audit and compliance

Elements checked during the SEVESO audit:

- Documentation of cyber risk analysis,
- Adequacy of protection levels,
- Configuration of security control network,
- Operation of firewalls and intrusion detection systems,
- Closed network operation and access management

Documentation requirements

Mandatory documents for EIR selection:

- Specification of security requirements,
- Compliance matrix for relevant legislation (CER),
- Risk analysis documentation,
- Security configuration plan,
- Incident management procedures,
- Update and maintenance plan.

07

International exposure and harmonisation

The NIS2 Directive aims to ensure a high level of cybersecurity across the European Union, with a particular focus on strengthening the protection of cross-border services. While the directive defines common requirements, its implementation varies significantly among Member States, espedially in terms of the technical and organisational controls, implementation timelines and compliance methods. This creates serious challenges for corporate groups operating across multiple jurisdictions, as they must comply with national legislation while also developing a coordinated, group-wide strategy. The challenges are further itentisified by differences in audit models, supply chain requirements, evolving sector specifications and the varying capabilities of national authorities and markets. This chapter provides a concise overview of the NIS2 implementation approaches and regulatory environments in selected Member States, highlighting key differences and practical implications for organisations.

7. International exposure and harmonisation

Written by: Norbert Pataki, Mária Etelka Szabó, Dr. Dániel Váczi

7.1. The approach of other EU Member States

In light of these differences, it is particularly important to identify the strategies, legal frameworks and practices that individual EU Member States are applying in the course of implementing the NIS2 Directive. While the directive seeks to promote harmonisation, Member States retain discretion in several areas, which has resulted in notable differences in implementation details. These variations have tangible implications for the predictability, cost and complexity of achieving compliance.

The pace of transposition also differs significantly, producing a diverse state of play across the EU. Accordingly, the information presented in this chapter reflects the situation as of 1 August 2025. Readers are encouraged to consult the accompanying overview maps, which provide country-specific links for further details. At the end of the chapter, a figure illustrates the current implementation status among Member States: countries marked in green already have enacted NIS2 legislation, while those marked in yellow only have published draft legislation.

The following section outlines a selection of countries where the relevant laws have either been finalised or have reached an advanced stage of implementation. These countries were chosen either because they serve as a key reference points for Hungarian regulatory development or because Hungarian organisations, particularly those within international corporate groups, commonly operate subsidiaries there. The examples highlight the diversity of audit models, compliance tools, reporting deadlines, and national interpretations (e.g., the concept of EIS) all of which pose challenges to coordinated, group-level compliance efforts.

Source: Brind interactive map[31]

31 https://www.brind.io/NIS 2acrosseu

The purpose of this chapter is not to provide an in-depth analysis of each country, but rather to offer context and comparative basis for evaluating the Hungarian compliance framework within the broader European landscape.

7.1.1. The EU requirements

The European Union has adopted a legally binding framework to support the implementation of the NIS2 Directive across all Member States. Commission Implementing Regulation (EU) 2024/2690 lays down technical and methodological requirements applicable to digital infrastructure service providers falling within the scope of NIS2 Directive. These include, among others, DNS providers, TLD domain registrars, cloud service providers, data centres, Content Delivery Networks (CDN), managed and security service providers, as well as online marketplaces, search engines, social media platforms, and trust service providers. The Regulation is direrctly applicable in all Member States and has binding effect on the organisations concerned.

7.1.2. Belgium

Belgium was among the first EU Member States to adopt the NIS2 Act, which passed on April 26, 2024, and entered into force on October 18, 2024. Its implementation is further supported by a Royal Decree (9 June 2024), which rmandates proof of compliance with recognised guidelines (e.g. CyFun or ISO 27001). Oversight is provided by the Centre for Cybersecurity Belgium (CCB), which defines reporting deadlines and registration obligations.

CyFun is nationally developed, risk-based, certifiable cybersecurity framework designed to support the effective implementation of NIS2 requirements. It combines elements of the NIST CSF, the structural clarity of ISO 27001, the actionable approach of CIS Controls, and the maturity assessment principles of CMMI. Recognition of CyFun is steadily growing across the EU, and an increasing number of countries are incorporating its principles into their own national compliance models.

7.1.3. France

In France, the transposition of the NIS2 Directive is currently progressing through the „Loi Résilince",(also known as the „Resilience Bill") which remains in draft form. Progress has been delayed due to the dissolution of Parliament in June 2024. The process is being coordinated by the National Cybersecurity Agency of France (ANSSI), which acts as a single point of contact for all matters related to implementation. The Resilience Bill is designed as an „omnibus law intended to transpose not only the NIS2 Directive, but also Directive 2022/2557 (CER) on the resilience of critical entities in the European Union and Regulation 2022/2554 (DORA) on digital operational resilience. Under the new framework, the scope of regulated entities has expanded dramatically, from around 500 entities under NIS1 to more than 10,000 entities, including local authorities and universities and sectors previously excluded from the regime.

7.1.4. Slovakia

Slovakia transposed the NIS2 Directive by amending its Cyber Security Act (Act No. 69/2018 Coll.). The amendment, published as Act No. 366/2024 Coll. was approved on November 28, 2024, and entered into force on January 1, 2025. The transposition is closely follows the provisions of the Directive, with no significant deviations. However, Slovakia took the opportunity to extend the scope to include local public administrations and introduced specific exemptions (e.g. national security, law enforcement agencies). The Slovak National Security Authority serves as a competent supervisory authority (also for Digital Service Providers and Operators of Essential Services) and also serves as the single point of contact (SPOC).

7.1.5. Austria

In Austria, cybersecurity is currently governed by the Austrian Netz- und Informationssystemsicherheitsgesetz (NISG) which transposed the original NIS1 Directive (EU 2016/1148), However, the amendment (NISG 2024 or 2025) intended to transpose NIS2 has not yet been adopted at national level. The previous draft was rejected by the Parliament (Nationalrat) on July 3, 2024, halting its progress. Although the new Austrian government reaffirmed its commitment to fully transposing the NIS2 Directive in its government program published in February 2025, final adoption and entry into force are are not expected before the second half of 2025. Responsibility for implementation lies with the Austrian Ministry of the Interior (Bundesministerium für Inneres, BMI), which also acts as a single point of contact and operates the official registration portal. Oversight of digital service providers (DSPs) and operators of essential services (OESs) - including their registration and reporting obligations -is exercised by the Federal Chancellery.Key elements of the draft include mandatory registration of entities within three months of the law's entry into force, incident reporting obligations, fines of up to 2% of global turnover for non-compliance, and reinforced responsibility at management level.

7.1.6. Germany

Following the entry into force of NIS2 Directive, the German government promptly initiated the legislative process for its national implementation. The first preliminary draft of the German NIS2 Implementation and Cybersecurity Strengthening Act (German: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) was published just four months after the EU Directive was adopted. However, the legislative process experienced delays, with five additional preliminary drafts released before the German government finally adopted the first official draft on July 24, 2024. This draft is still awaiting ratification by Parliament. Under the proposed legislation, the BSI (Bundesamt für Sicherheit in der Informationstechnik) will act as a competent authority and the natitonal single point of contact (SPOC). CERT-BUND, a cyber security incident response centre operating under the BSI, is designated as the national CSIRT, responsible for 24/7 incident response coordination. In parallel, Germany is also preparing to transpose the CER Directive (Critical Entities Resilience Directive, EU 2022/2557), thorugh the KRITIS-DachG, a comprehensive national framework for the protection of critical infrastructure.

7.1.7. Italy

Italy completed the transposition of the NIS2 Directive into national law in 2024 through Legislative Decree No. 138/2024, which entered into force on October 16, 2024. The legal basis for this decree is established by Law No. 90 of June 28, 2024, which establishes a broader regulatory framework aimed at strengthening national cybersecurity and also addresses procedures related to cybercrime. This implementation model differs from that of most other Member States. While other countries incorporate detailed NIS2 provisions directly into their national laws, Italy integrates NIS2 into a comprehensive national cybersecurity legislative strategy.

Affected organisations are required to comply with a set of compliance requirements aligned with the NIST Cybersecurity Framework (CSF), which emphasises risk-based management and a structured design of security controls. Compliance and enforcement fall under the responsibility of the Agenzia per la Cybersicurezza Nazionale (ACN), which is also operates as a national CSIRT, serves as a single point of contact and performs the EU-CyCLONE functions.

7.1.8. Latvia

On September 1, 2024, Latvia enacted the Nacionālās kiberdrošības likums OP 2024/128A.1, as the national implementation of the NIS2 Directive. The National Cyber Security Centre (NCSC/CERT.LV) serves as the primary authority and a single point of contact (SPOC), while the Satversmes aizsardzības birojs (SAB) oversees critical ICT infrastructure.

Organisations falling under the scope of the law are not required to undergo an external audit, but must submit an annual self-assessment report, structured as a standardised questionnaire. The report outlines the level of the organisation's compliance with cybersecurity requirements and explains any deviations. Reports are due by October 1 each year.

Overall, despite differing deadlines and occasional minor setbacks, Member States are making strong progress in advancing their information security frameworks, establishing robust legal foundations, and providing clear support to regulated entities.

7.2. Grouping principles: opportunities and pitfalls

In Hungary, many organisations are subject to NIS2 Directive operate in an international context either though affiliation with a foreign parent company or by relying on SaaS-type EIS hosted outside Hungary.

A common question in such situations is what obligations arising when an orgaisation uses an EIS that it does not fully control (e.g., the EIS is operated by the parent company, that is an international entity). In such cases, Section 6.1 shall apply, stipulating that an organisation is responsible for fulfiling the requirements set out in NIS2 Directive only to the extent that is control over the EIS.

Therefore, if an organisation uses an EIS operated by another entity and has no control or influence over it, i.e., it solely acts as a „user" of that EIS, the system may be excluded from the scope of the audit. However, if the organisation exercises any degree of control over the EIS relevant to NIS2 requirements (e.g., user management), then the EIS must be included in the audit. Under these circumstances, only those controls over which the organisation has influence will be subject to evaluation. For all other aspects, the organisation must provide justifcation for its lack of control over the relevant EIS.

08

Practical interpretation and application of domestic requirements

The Hungarian implementation of the NIS2 Directive comprises a set of interrelated and detailed legal provisions that not only establish the theoretical framework for compliance, but also pose practical challenges during implementation. This chapter provides an overview of the content and interrelationship between the two key legal acts relevant to affected organisations (the MK Decree and the SZTFH Decree), followed by a discussion of the typical difficulties that organisations may encounter in their day-to-day operations. In addition, it offers practical guidance on reconciling regulatory requirements with organisational realities, when and how to apply alternative measures or deviate from statutory provisions, and managing contractual compliance.

8. Practical interpretation and application of domestic requirements

Written by: Gergő Barbul, Gergő Csarnai, Alexandra Enyedi, Dr. Andrea Jeney, Tamás Lóth, Csaba Mészáros

8.1. Comparison of Decree No. 7/2024 (VI.24.) and Decree No.1/2025 (1.31.)

The two decrees serve distinct purposes: while Decree No. 7/2024 (VI. 24.) MK sets out requirements for organisations that manage EISs, Decree No. 1/2025 (I.31.) SZTFH primarly provides guidelines and methodology for auditors.

8.1.1. Decree No. 7/2024 (VI. 24.) MK

Public consultation on the MK decree began in late January 2024, and the related documents, such as the explanatory memorandum to the draft legislation[32] and the impact assessment[33]. are available on the www.kormany.hu website. These documents confirm that the decree was introduced to support the implementation of NIS2 Directive and it was indicated that no impact assessment on market participants had been conducted. Furthermore, based on the proposals received by February 8, 2024,[34] the legislator did not deem it necessary to amend the draft. The MK decree reached its current form on January 2, 2025, incorporating the amendments introduced by MK Decree No. 18/2024 (XII. 30.)[35]. The Decree applies to all organisations falling within the scope of the Cybersecurity Act.

Sources of the MK Decree

The MK Decree is based on NIST 800-53[36] and 800-53B[37] publikációkra épül. Ezek közül az előbbi egy kontroll katalógus, míg az 53B jelzésű az alacsony (low), mérsékelt (moderate) és magas (high) biztonsági szintekre alkalmazandó (továbbá az adatvédelemhez szükséges) kontrollokat határozza meg.

The former serves as a control catalogue, while the latter defines controls applicable to low, moderate, and high security levels including those required for data protection.

The purpose of NIST 800-53 is to *„provide a comprehensive framework for security and*

32 Draft ministerial decree on measures to ensure a high level of cybersecurity across the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, and laying down certain provisions for the implementation of Directive 2022/2555 of the European Parliament and of the Council (NIS 2 Directive).

33 https://cdn.kormany.hu/uploads/document/3/39/39b/39be5fd49840b90e1e74bbac495db23af33c6bbd.pdf

34 https://cdn.kormany.hu/uploads/document/a/aa/aa3/aa32c78bfe46d772318e0caee9d83fb25cc2f164.pdf

35 Hungarian Gazette (Hungarian Official Journal) • Issue137 of 2024

36 Security and Privacy Controls for Information Systems and Organizations

37 Control Baselines for Information Systems and Organizations

privacy controls for (federal) organisations and systems that handle information. The publication helps these organisations identify the controls necessary to manage risk and meet security requirements, offering a flexible catalog that adapts to changing threats and technologies. It also aims to establish a common vocabulary that facilitates communication between organisations on security, privacy, and risk management issues."

Publication 800-53B *„establishes baseline security and privacy controls for federal information systems and organisations and provides guidance for customising these controls. The publication is applicable to any organisation that handles information (federal, state, or private sector), but the minimum set of controls is mandatory for federal systems. The benchmarks serve as a starting point that organisations can customise based on their mission, stakeholder needs, and risk assessments to meet their security and privacy requirements."*

Consequently, the legislator has adopted this set of requirements originally designed for US federal information systems and the corresponding measures for each security classification, applying them not only to public sector, but also to commercial organisations

.

Structure of the MK Decree

The first three sections provide substantive information. The legislator did not specify a compliance deadline, so organisations are expected to adhere to the requirements outlined in legislation upon its entry into force. Section 2(3) is particularly important, as it stipulates that the measures listed in Annex 2 apply only for those EISs and EIS components over which the organisation has control. This control is closely tied to the organisation's decision-making authority.

Annexes to the MK Decree

The MK Decree contains three annexes, outlined as follows:

- Annex 1:
  (1) The risk management framework (see 5 . chapter), (2.) Safety classification (see 6.2 . chapter), (3.) Deviations (see 8.7 . chapter), (4.) Substitute protective measures (see 8.6 . chapter), (5.) Risk analysis and risk management.
- Annex 2 – Catalogue of protective measures:
  The catalogue consists of 20 sub-sections. It may be helpful to start with Section 20, as it provides a detailed guide to using the catalogue. While NIST 800-53 contains 20 control families, the MK Decree contains only 19. The difference arises from the group „Personally Identifiable Information Processing and Transparency (PT)", which is excluded, becasue this area is regulated by the GDPR and Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Infotv.)
- Annex 3 - Catalogue of threats:
  The source of the catalogue is not a NIST publication, but the BSI IT-Grundschutz Compendium[38]. A more detailed description of the 47 threats listed in this appendix can be found in the Compendium, which may help perform tasks under the risk management framework. Note that the information security principles of confidentiality [C], integrity [I], and availability [A] in column B of the table are also defined in the Cybersecurity Act.

38 IT-Grundschutz Compendium Edition 2022

8.1.2. Decree No.1/2025 (I.31.) SZTFH

Although this requirement is gradually being phased out, under the Cybersecurity Act, organisations falling within its scope were originally obliged to conclude a contract with an auditor registered with the SZTFH by the end of 2024. However, no methodology had been established for calculating the audit fee, which meant that auditors were unable to provide organisations with quotations. In a statement issued after Christmas 2024, the Authority announced that it would not impose sanctions in the absence of relevant legal instruments.[39] At the end of January 2025, the SZTFH issued a Decree, which, among other things, set out the method for determining the the maximum fee for cybersecurity audits, thereby removing obstacles to the conclusion of contracts between auditors and organisations.

The purpose of the SZTFH Decree is to *„lay down the basic rules for cybersecurity audits intended to verify compliance with cybersecurity requirements and to determine the limited fees applicable for such cybersecurity audits."*

The decree applies to organisations required to undergo a cybersecurity audit pursuant to Section 16(1) of the Cybersecurity Act.

Regulatory sources of the SZTFH

NIST 800-53A rev.5[40] (Annex 5, point 1.1.1 of the Regulation also clearly refers to this), which aims to *„provide guidance for developing effective security and privacy assessment plans and provide comprehensive procedures for assessing the effectiveness of controls implemented in systems and organisations. The publication enables more consistent and effective assessments, promotes a better understanding of organisational risks, facilitates cost-effective evaluations, and provides reliable information for risk management decisions. Organisations can tailor assessment procedures based on factors such as security classification and risk assessments. The assessment process is an information gathering activity that helps identify security weaknesses, prioritise responses to risks, support monitoring activities, and inform authorisation and budget decisions."*

Structure of the SZTFH Decree

The sections of the Decree provide for the use of the annexes, which are described in a greater detail in this chapter. The Decree also specifies which security classes may be audited by the auditors listed in the SZTFH register[41]. In addition, Section 6(3) obliges the audited organisation to retain evidence for five years from the date of closure.

- Annexes 1-2: „Register of electronic information systems" and „Questionnaire on the organisation":
  Pursuant to Section 3(3) of the Decree, these annexes must be made available to auditors by the organisations, enabling auditors to submit their quotations. Under the same provision, the Authority is required to publish a completion guide on its website. However, at the time of writing this Whitepaper, the guide had not been yet made available. The MK Decree must also be used when completing Annex 1. Column C of the table refers to the security classes described in the MK Decree, while columns D to F refer to the three categories of confidentiality, integrity and availability. Annex 3 of the MK Decree (Catalogue of Threats) may also be taken into account when completing the table, serving as a risk identification tool.

39 NIS 2 – An important SZTFH regulation will be promulgated in 2025 – Authority for the Supervision of Regulated Activities

40 Assessing Security and Privacy Controls in Information Systems and Organizations

41 Auditors –Supervisory Authority for Regulatory Affairs

- Annex 3: Maximum fee for a cybersecurity audit:
  Revenue is essentially a given: it is difficult to imagine that any economic operator attempting to reduce its net revenue to lower the maximum fee for an audit. More significant factors are the highest security class and the number of EISs, which are discussed in a greater detail in Chapter 6 of this Whitepaper.
  According to preliminary data from the Hungarian Central Statistical Office (KSH)[42], in 2023 the average „net sales revenue" of medium-sized enterprises was approximately HUF 4,051,936,155, while for organisations not classified as SMEs, the same figure was HUF 16,022,697,871. Annex 3, Section 1.1 specifies the multiplier to be used when calculating the organisation's net sales revenue for the previous financial year.

In addition to turnover, the number and security class of the organisation's EISs must also be considered when calculating the audit fee, with multipliers provided in Annex 3. The table below illustrates how the audit fee would have been calculated in 2023, based on the average revenue data reported by the Hungarian Central Statistical Office, taking into account the number of EISs, their security class and the multipliers specified in Annex 3. Legally required multipliers are indicated in square brackets.

- Annex 4: Register of derogations and alternative safeguards: For more detailed information, please refer to Section of 8.7 of the Whitepaper
- Annex 5: Audit methodology. This topic is addreessed in Chapter 10 of the Whitepaper. However, it is worth highlighting an example to illustrate the relationship between the two statutory provisions.

42 9.1.1.17. Performance indicators for enterprises by small and medium-sized enterprise category

		Security class		
	Number of EIRs	Basic [1x]	Significant [3x]	High [5x]
Medium-sized enterprise	1–5 [1x]	1,925,000	5,775,000	9,625,000
Organisation not classified as an SME		4.812.500	14.437.500	24.062.500
Medium-sized enterprise	6–15 [2.5x]			
Organisation not classified as an SME		12.031.250	36.093.750	60.156.250
Medium-sized enterprise	16 or more [4x]	7.700.000	23.100.000	38.500.000
Organisations not classified as SMEs		19,250,000	57.750.000	96.250.000
		HUF		

- The „critical deviation" described in Section 2.2.4.1.3.4 of the SZTFH Decree shows significant overlap with the damage events listed in section 2.2.4 of the MK Decree, such as personal injury and damage to national data assets. However, there is one key distinction: while the MK Decree refers to damage events involving special categories of personal data in Section 2.2.4.1 for the high security class, the SZTFH Decree refers to damage affecting the confidentiality of all personal data without the special data-qualifier. Considering that a significant portion of EISs involves the processing of personal data, such as unique user ID, strict adherence to this methodological requirement as written inthe legislation is likely to create a critical deviation, which would immediately result in a „non-compliant" assessment.
- Annex 6: It defines the assessment methods to be used in the cybersecurity audit, as well as the characteristics of the requirement groups relevant to the audit procedure. These characteristics include whether a particular group of measures should be assessed at the organisational or EIS level (Column B), the test methods employed (Columns C-E), the type of measure (assuring/supporting), which is an important factor in calculating the Vulnerability Management Index (VMI). The Decree also specifies whether a given set of requirements may be excluded from the assessment; excluded requirement groups are classified as „not applicable" during the audit.
- A review of the tables in the Annex reveals that some serial numbers are missing (e.g. 1.8. (Organisational Architecture – Offloading), 1.13. (Internal Threat Program), etc. These controls are supplementary protective measures in accordance with the MK Decree („protective measures for which both Columns „C" contain a „-" sign") and unlike to NIST 800-53A, the SZTFH Decree does not specify the audit-relevant characteristics or provide evaluation instructions for them in Annex 7.
- Annex 7: Assessment of the groups of requirements under the MK Decree. The table breaks down the requirements of the MK Decree into basic requirements in a considerable detail – see the tables below. However, it does not indicate the security classes for which the implementation of the respective measures is required. Organisations classified under the basic or significant security classes are advised to compare the two Decrees from this perspective, so that they have at their disposal both the requirements and the corresponding assessment points needed to verify compliance.
- Annex 8: Contents of the audit report. The annex is intended for auditors and specifies the requirements for the audit report set out in Section 5 of the SZTFH Decree. The report must be provided to the audited organisation in a printable format, as well as in a format that allows for machine processing by the SZTFH

.

Relationship between regulations (and their sources)

MK Decree	NIST 800-53
2.1. The organisation 2.1.1. Develops, documents, issues, and communicates to the persons designated by the organisation according to their roles	AC-1 POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
2.1.1.1. an access control policy containing organisational, process, and system-level requirements that:	1. [Selection (one or more): Organization-level; Mission/business process-level; System level] access control policy that:
2.1.1.1.1. defines objectives, scope, roles, responsibilities, management commitment, framework for cooperation within the organisation, and compliance criteria, and	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2.1.1.1.2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines applicable to the organisation.	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

SZTFH Decree	NIST 800-53A
2.1. Policies and procedures K02.001_P[1 List of persons or roles who must be made aware of the access control policy	AC-01 POLICY AND PROCEDURES ASSESSMENT OBJECTIVE: Determine if: AC-01_ODP[01] personnel or roles to whom the access control policy is to be disseminated is/are defined;
K02.001_P[2] It is specified that the access control policy is defined at the organisational, process or system level.	AC-01_ODP[02] personnel or roles to whom the access control procedures are to be disseminated is/are defined;
K02.001_O.2.1.1.(a) The access control policy at the K02.001_P[2] level has been developed and documented by the organisation.	AC-01a.[01] an access control policy is developed and documented;
K02.001_O.2.1.1.(b) the access control policy has been issued by the organisation K02.001_O.2.1.1.(c) the access control policy has been disseminated to the persons or roles specified in K02.001_P[1]	AC-01a.[02] the access control policy is disseminated to <AC-01_ODP[01] personnel or roles>;
the access control policy defines the objectives	AC-01a.01(a)[01] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy addresses purpose;
the scope of the access conrol policy has been defined	AC-01a.01(a)[02] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy addresses scope;

SZTFH rendelet	NIST 800-53A
the access control policy defines roles	AC-01a.01(a)[03] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy addresses roles;
... and here, based on point 2.1.1.1.1 of the MK decree, the „responsibilities, management commitment, framework for cooperation within the organisation, and compliance criteria" should follow, i.e. K02.001_O.2.1.1.1.1.(a) to (g)	
K02.001_O.2.1.1.1.2 the access control policy is consistent with the laws, directives, regulations, standards and recommendations applicable to the organisation	AC-01a.01(b) the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines

"P" and "O" type basic requirements

These variables, which depend on organisational decisions, are referred to as "organisation-defined parameters (ODPs)" in NIST 800-53. In the SZTFH Decree, the reference code for such parameters contains the letter "P".

Typically, the requirement element of the MK Decree containing the terms „determines" and „determined" appears in the SZTFH Decree as a parameter, for which both the definition of the specific parameter and the implmentation of the corresponding activity must be audited. Based on the wording of the MK Decree Sections 2.1.1.1. and the other x.1.1.1. requirements, it may seem that the rules mandate *„organisational, process and system level requirements"*, whereas the NIST 800-53, 800-53A and SZTFH Decree present this as an optional or discretionaly approach.

As stated in the requirement in 2.1.1.1.1. (*„defines the objectives, scope, roles, responsibilities, management commitment, framework for cooperation within the organisation and compliance criteria"*) and the related SZTFH K02.001_O.2.1.1.1.1.(a) - (g) - each element listed in the MK Decree constitutes an auditable measure with a separate serial number.

Minor differences between the Decrees

As the Decrees are based on NIST publications, which are quite extensive, minor differences between them may occur. An example of this is the parameters K05.001 P[1] and K05.001_P[2], which refer to the policy and procedures for logging and accountability, even though the fifth group of measures is „Evaluation, authorisation, and monitoring."

Useful resources

National Cyber Security Institute Application Guide for the Catalogue of Cyber Security Requirements for Electronic Information Systems and Organisations[43], as well as other recources available on this page[44], which provide explanations, implementation steps, and additional useful information.

43 Application Guide for the Catalog of Cybersecurity Requirements for Electronic Information Systems and Organisations – National Cyber Security Institute

44 Download the table of security measures (ver. 1.0)

8.2. Practical tips for implementing high resource requirements

The practical implementation of the NIS2 Directive is not merely a matter of compliance, it also represents a complex organisational and project management challenge. This is particularly critical for institutions with limited IT security, compliance, and legal capacities. The following measures and methods are designed to help organisations achieve compliance gradually and efficiently in line with their strategic priorities.

Priority-based implementation

Organisations should create a simple, business risk-based priority matrix that considers:

- the impact on business processes (risk)
- the severity of the compliance gap,
- the estimated cost and time required for implementation,
- available organisational resources.

A well-structured matrix enables organisations to focus first on areas that pose the greatest risk while requiring the fewest resources. A phased, iterative approach helps reduce concurrent workloads and enhances transparency throughout the implementation process.

Small, focused project team

Form a project team with representatives from IT, information security, legal, HR, and business areas. To ensure productive collaboration, employ:

- a RACI matrix for task allocation,
- a project charter to document goals and expectations,
- regular short status meetings for progress follow-up.

A well-organized, compact team can make swift decisions and respond to evolving circumstances with minimal administrative overhead.

Automation wherever possible

Routine processes should be automated to reduce human resource requirements. Recommended areas as follows:

- Logging and event management: SIEM systems, automatic collection and analysis of log files.
- Access management: use of IAM or PAM tools to manage permissions.
- Training and awareness: integration of an e-learning platform with auditable participation.

Additional options include automating version tracking, generating compliance reports, and integrating update reminders.

Agile project management approach

Unlike the traditional waterfall model, agile, sprint-based operations are recommended for implementing NIS2 compliance, particularly in environments changing requirements and limited capacities:

- Short, 1-2 week iterations (sprints)
- User stories to describe tasks,
- Regular retrospective discussions to capture lessons learned,
- Demo phases for validating partial implementations.

This methodology enhances responsiveness and supports gradual maturation of organisational capabilities.

Targeted involvement of external resources

If internal competencies are insufficient, it is advisable to engage external consultants or service providers in the following areas:

- Risk analysis and classification,
- Policy development and internal procedures,
- Technical security assessments (e.g., penetration tests, internal audits),
- Business continuity and incident management.

When drafting contractual terms and conditions, ensure they incorporate NIS2-compliant requirements, such as SLAs, data security measures, quality assurance mechanisms.

+1. Conscious communication and management support

NIS2 compliance is an organisational challenge, making active support and commitment from senior management essential. This includes:

- communicating strategic objectives
- regular updates on project status,
- offering decision-making support to resolve bottlenecks.

8.3. Proposed amendments to contracts

The fundamental objective of the NIS2 Directive is to enhance cyber resilience, mitigate threats and strengthen cybersecurity capabilities in key sectors. This introduces new legal obligations on the organisations concerned, requiring a review of existing contracts and, where necessary, their amendment.

Accordingly, it is advisable to subject current contracts to a comprehensive legal review, taking into account the NIS2 Directive, the Cybersecurity Act, the Government Decree on its implementation, and the relevant provisions of the MK Decree regarding security classification requirements and the specific protective measures applicable to each security class.

Existing contracts between the parties may take various forms (SLA agreement, SaaS, IT operating agreement), with provisions that can differ significantly depending on the industry and the specific service provided. The following suggestions for amending contractual provisions are offered as guidance. They shoud be adapted to the nature of the contract, but can serve as a useful reference when reconsidering contractual content.

Subcontractors

To ensure the supply chain security, legal entities in a subcontracting relationship with the organisation must comply with the NIS2 requirements as follows:

„New Subcontractors may only be engaged with the prior written consent of the Customer. The Subcontractor undertakes to comply with the provisions of the NIS2 Directive, to assess its EISs and classify them according to security classes, and to implement the protective measures corresponding to the security class. The Subcontractor shall provide the Custotmer with documentary evidence of compliance no later than one month prior to the date of the first scheduled cybersecurity audit."

Incident management

NIS2 establishes strict deadlines for cybersecurity incident management, including notification and reporting obligations.

„The Contracting Party shall continuously monitor its information security systems, review system logs and ensure their secure storage. It shall also report detected information security incidents related to EIS to Customer without undue delay, and in any event no later than X hours after detection. Such notification shall include all available information necessary to enable the Customer to notify the the competent authorities. Furthermore, the Contracting Party shall also forward the relevant system logs to the Customer for further investigation and shall fully cooperate in all subsequent response and remediation activities."

Harmonisation of documents

NIS2 impacts a number of existing documents, making their harmnoisation essential. [Information Security Policy, Incident Management Policy, Data Management and Data Security Policy (if necessary), Access Management Policy, Information Security Strategy, etc.]

„The Contracting Party undertakes to subject all documents affected by NIS2 to a legal

compliance review and, and based on the results of that review, to amend the affected documents no later than (date)..... The updated versions shall be made available to the Customer without delay."

Liability issues

It is advisable to obtain insurance to cover any cybersecurity incidents, which may also be a legal requirement. The contract should clearly specify the scope of liability for damages, its allocation, the coverage limit and the obligation to maintain the insurance policy.

„The Contracting Party undertakes to obtain liability insurance covering any damages arising from cybersecurity incidents. The insurance policy shall be submitted to the Customer no later than one month prior to the Customer's first cybersecurity audit. When determinig the insured amount, the nature of the delegated activities and the potential risks shall be taken into account, based on a risk assessment conducted by the Contracting Party. The Contracting Party shall maintain valid insurance coverage beyond the Customer's cybersecurity audit. Any changes to the terms of the insurance policy, must be communicated to the Customer without undue delay."

Security awareness, training

Increasing security awareness is an important objective of NIS2. This can only be achieved if all employees of the contracting parties are aware of and comply with the information security rules relevant to their specific position. Therefore, mandatory training and testing must be required in all cases.

„The Contracting Party shall provide regular security awareness training to its employees of the organisation it manages, tailored to their roles and responsibilities. Each training session shall be followed by an assessment. The Contracting Party shall make the relevant documentation (training reports, test results) available to the Customer no later than one month prior to the Customer's first cybersecurity audit."

Obligation to cooperate

Cooperation between the parties is essential, as without it the NIS2-obliged party cannot fulfil the audit compliance criteria. Therefore, the obligation to cooperate must be expressly stated.

„The parties shall fully cooperate with each other to ensure the successful completion of the Customer's cybersecurity audit. Such cooperation shall in particular, require compliance with information security and audit requirements. Failure by either party to comply with this, shall constitute a material breach of contract and shall constitute grounds for termination. The exercise of the right of termination shall not be conditional upon the imposition of penalties or official measures agains the Customer."

Changes in legislation

The parties shall consult with each other in the event of any legislative changes, and if necessary, jointly amend their existing contract accordingly. Keeping the contract up-to date is a prerequisite for a successful audit, as auditors also perform document-level checks.

„The parties undertake to consult with each other in the event of any legislative changes, and, if necessary, to jointly amend their existing contract to reflect such changes."

Designation of an Information Security Officer

It is essential that the information security officers of the parties maintain regular contact, and where necessary, consult on the measures to be taken.

„The parties shall designate information security contact persons, namely..... for Company X and ..... for Company Y. This contact persons shall maintain regular consulations, inform each other of the adopted information security measures, and coordinate their actions based on the information exchanged."

Regular risk assessment

The parties shall update the information asset inventory related to their EISs and the associated risk assessment at regular intervals. This is essential, as changes in circumstances may require adjustments or different protective measures, which can only be ensured through periodic review and monitoring.

„The parties shall review the information asset inventory and related risk assessment to their EISs at least annually and update them as necessary. Following such updates, the parties shall modify or reassess the protective measures in place to ensure that the level of protection of EIS remain appropriate."

The above contractual amendments serve not only to ensure legal compliance, but also to maintain trust between the parties and minimise operational risks. It is the joint responsibility of the contractual partners to ensure the continuity of services and the protection of critical systems in a digital environment, as well as to ensure that the related legal safeguards are transparent and accountable.

8.4. Do all points have to be met?

To achieve compliance, a number of security requirements based on the NIST 800-53 Rev.5 international standard must be met. The security classification of EISs determines the number of applicable requirements.

Oganisations have varying levels of maturity and therefore start from different baselines when prepairing for compliance. Taking this into account, the Cybersecurity Act allows organisations to apply a risk-based approach. This means that each company must assess the security maturity of its EISs, classify them into appropriate security categories, perform a GAP analysis, and conduct a risk assessment. Once risks have been identified, the organisation can determine which measures can mitigate them and whether these measures exist in the catalogue of protective controls. If the catalogue does not contain measures that can be effectively applied and in proportion to the risk, alternative protective measures may be defined to replace missing or insufficienet controls. A record of the chosen measures must be maintained and approved by management. Annex 4 of the SZTFH Decree provides a template for this record. Audit companies request this report either when the audit contract is concluded or within 15 days of signing the contract.

The substitute measures must be documented and evidence of their implementation must be presented during the audit.

8.5. Risks of over- or under-compliance

One of the main requirements of NIS2 is to ensure compliance. While this process is mandatory, it is important to recognise that both under-compliance and over-compliance carry significant risks. The objective is to adopt a proportionate and reasonable approach.

Risks of under-compliance: the cost of non-compliance

Failure to comply with NIS2 requirements can have immediate and serious consequences. These may include significant fines (up to 2% of annual turnover), restrictions on certain activities, or even a ban on operations. From an operational perspective, non-compliance increases the risk of cybersecurity incidents such as data breaches or service outages, which may damage reputation and disrupt business continuity. Such incidents can also result in substantial financial burdens due to recovery costs and lost revenue.

Risks of over-compliance: the „gilded cage”

Surprisingly, over-compliance also carries risks, primarily in the form of wasted resources. Organisations may incur unnecessary costs from excessive technological investments and the purchase of superfluos software and hardware. While „boxed” products that claim to ensure NIS2 compliance can assist in establishing and demonstrating compliance, no single software product solution can guarantee full compliance on its own. Moreover, human resources may become overburdened if excessive working hours and specialists are tied up in non-essential tasks, diverting them from strategically important activities or even from day-to-day, revenue-generating operations. Additional bureaucratic burdens, such as redundant documentation and overly complex processes, further exacerbate the problem.

Operational efficiency may also be undermined, as excessive control points and administrative tasks can slow down business processes, hinder innovation, and obstruct agile operations. Excessive control and unnecessary tasks can even reduce employee satisfaction. Over-compliance can create a competitive disadvantage, as additional costs reduce competitiveness while overly restrictive security processes impair the customer experience. Finally, attention may shift away from critical areas if focus is directed to less relevant but „easy to tick off” tasks.

The optimal solution: a reasonable and proportionate approach

A risk-based approach is essential to minimise risks. This involves identifying the most critical areas and processes, taking into account the results of business impact analysis (BIA) and the organisation’s key data assets. It is crucial to interpret the NIS2 requirements and implement tailored solutions appropriate to the organisation’s size and complexity. Continuous review and adaptation ensure that measures remain effective in an ever-changing environment. Strong management commitment and targeted employee training are also key to achieving successful compliance.

8.6. Possible substitute protective measures

The purpose of the security measures required by security classification is to ensure that all registered EISs maintain an identifiable and measurable level of protection. However, in practice, organisations may not always be able to comply with every required control, whether due to technological constraints or specific business needs. In such cases, well-documented substitute protective measures may be applied but provided they demonstrably achieve the objective of the original control.

This is particularly important in environments where information technology (IT) and operational technology (OT) coexist but operate under different logics. In a traditional IT system, for instance, a security function can often be implemented via software, whereas in OT systems, the same function may only be ensured through physical access controls or the reorganisation of operating protocols. The key point is that any alternative solution should not only satisfy formal compliance requirements, but also effectively reduce the risk that the original control was intended to mitigate.

The use of substitute measures is not only a right but also a responsibility. In all cases, it must be based on a risk-based assessment, thorough documentation, and senior management approval. Compliance is not demonstrated by the method used, but the results achieved. Auditors does not examine whether a control has been followed to the letter, but whether the audited organisation has demonstrably reduced the relevant risk. This is supported by the record-keeping template prescribed in Annex 4 of the SZTFH Decree, which provides transparency for both the organisation and the auditor regarding decisions and their rationale.

8.7. Management of deviations

In the practical implementation of EIS protective measures, organisations may allow certain deviations provided they are properly documented and justified in a manner that ensures compliance with the system's security requirements. Managing deviations does not imply circumventing compliance; rather it supports risk-based, adaptive protection. Well- documented deviations promote flexibility, sustainability, and the optimal use of resources.

Types of individual deviations (control-based approach)

When implementing protective measures (controls), an organisation may, in certain cases deviate from the application of a specific control based on a documented risk analysis and appropriate justification. The types outlined below serves to structure common deviation scenearios.

- Control not relevant in the operating environment: When a control (e.g., wireless network encryption) cannot be applied because the system does not contain any wireless connections, the measure is unnecessary. Under these circumstances, the organisation documents the inactivity of the control referring to the absece of the relevant technology in the operating environment.
- Control already provided by another mechanism: Sometimes the objective of the required control is already fulfiled by another existing measure. For example, if physical access control is provided not by an access control system but through permanent security guards and key management, and this approach is appropriate for the risk level, the deviation is documented as the use of a functionally equivalent alternative.
- Control not applicable for legal or organisational reasons: A control may be inapplicable due to data protection or employment law requirements. In such case, the organisation documents the deviation with reference to regulatory compliance and implements other measures to mitigate associated risks.
- Control can only be introduced gradually: A given control (e.g., multi-factor authentication) cannot be implemented immediately on all affected systems for technical or financial constraints. In this case, the organisation develops a detailed implementation plan including appropriate compensatory measures. The deviation is justified by the need for phased compliance and the management of the transitional risks.
- Control is not relevant to the system function: Certain measures (e.g., robust logging) are unnecessary for a static, public website that does not require login or interactive data processing. Justification for deviation: the control is not applicable to the system's operation.
- Control applies only to specific system components: Complex systems may consist of components with differing security requirements. For example, if the internal administration module is isolated and operates in a separate network zone, access control may be stricter there, while less stringent for the public interface. Justitfication for deviation: control is applied differently across system components based on the system's architecture.
- Control cannot be implemented temporarily: A measure (e.g., regular risk

reassessment) cannot be temporarily ensured due to technical or human resource burdens. The deviation is only acceptable if there is a documented compensation mechanism is in place, such as manual controls or more frequent monitoring. The duration of the deviation and the review plan must be recorded.

If necessary, these categories can be combined: for example, a control may be both legally inapplicable and technically irrelevant. The key is to document all deviations with:

- written justification,
- risk-based analysis,
- determination of compensating controls (if necessary),
- management approval, and
- a plan for periodic review.

The management of deviations is an integral part of the practical application of requirements and plays a key role in ensuring that security is not merely a formality, but a truly sustainable and proportionate approach. A flexible yet well-defined deviation mechanism allows the organisation to achieve a level of protection that is appropriate to its resources, operational characteristics, and technological realities, while remaining compliant with the NIS2 Directive.

The key to success lies in transparent justification, regular review, and management approval of decisions. Derogations are not loopholes, but tools for conscious and risk-balanced protection when used properly.

09

Documents and records to be prepared

Information security is not merely a technical issue; it relies on an appropriate regulatory and documentation framework. The NIS2 Directive and national legislation require all organisations to establish policies, procedures, and records that define security principles, processes, and responsibilities. These are not just formal documents, but essential components of risk management, protective measures and compliance. The information security policy (ISP) sets the overarching framework, internal rules specify operational procedures, procedures and protocols provide the steps for implementation, records ensure traceability, and the system security plan (RBT) consolidates all of these elements at the system level. Together, they enable organisations to maintain the confidentiality, integrity, and availability of data and systems even as threats evolve. The following chapter offers a detailed analysis of these elements.

9. Documents and records to be prepared

Written by: Dr. Ágota Albert, Alexandra Enyedi, Zoltán Sipos

9.1. EIS security and risk management documentation

The MK Decree sets out the security requirements for EISs, specifying the documentation that organisations must prepare and maintain, including risk management records, security measures, and the related internal policies, procedures.

Risk management documentation

Annex 1 of the MK Decree sets out the documentation obligations regarding EIS risk management. Its purpose is to promote risk awareness within the organisation and to support a deliberate and proportionate development of information security controls.

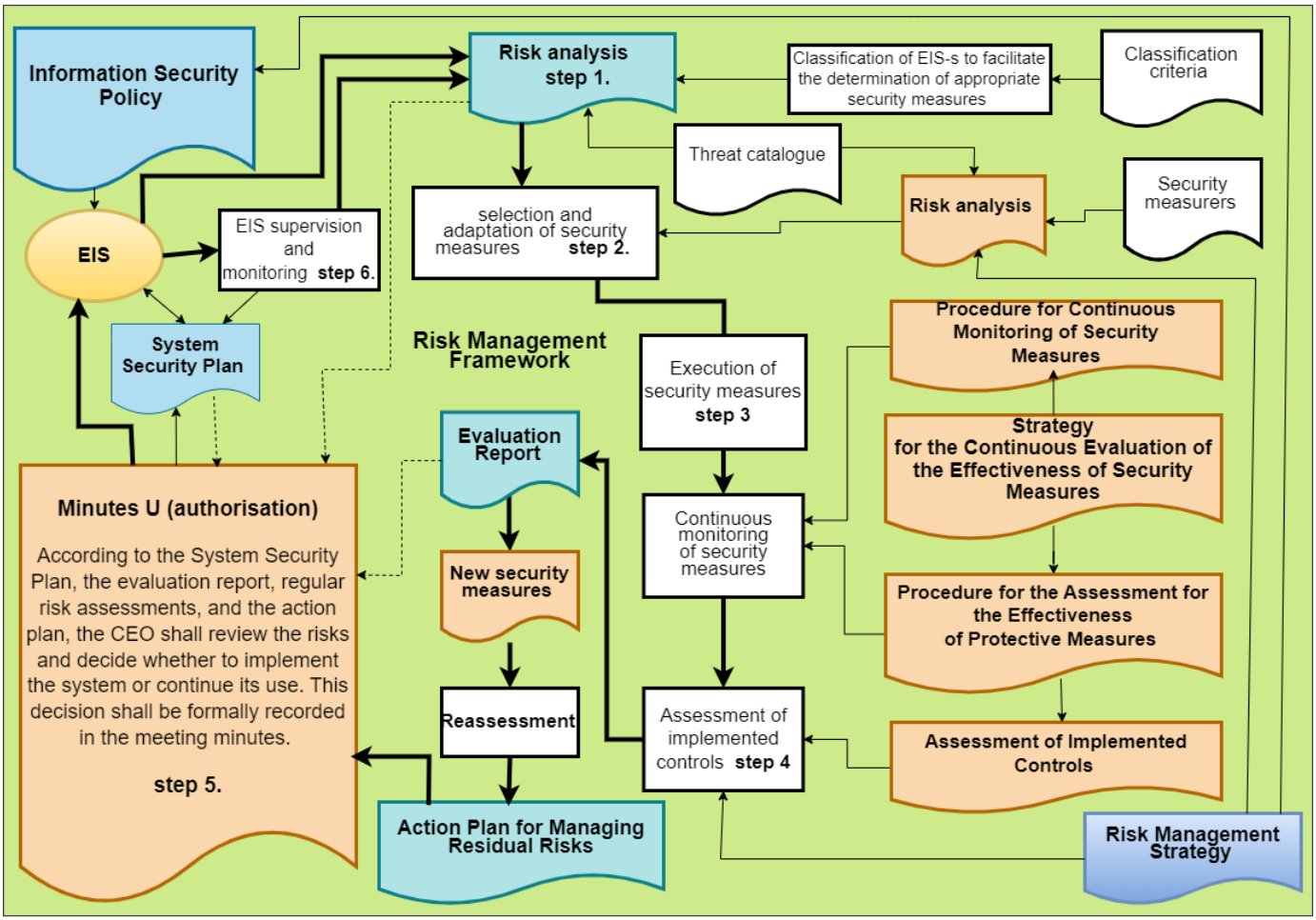
In preparation for the implementing the risk management framework, the following must be defined and documented:

- the roles, responsibilities, tasks and decision-making authority related to the protection of EISs
- the risk management strategy, describing how security risks are identified, assessed, managed, and monitored,
- the security monitoring strategy, which sets out the ongoing monitoring of the effectiveness of protective measures, including the frequency of monitoring activities related to such measures.

EIS documentation

With regard to EISs, the following must be defined and documented:

- the business objectives, functions and processes supported by the EIS
- the persons or organisations involved in the design, development, implementation, operation, maintenance, use, and control of the EISs
- the assets involved,
- the organisational and technological boundaries of the EIS,
- the data sets processed, stored and transmitted by the EIS together with their lifecycle,
- the assessment and management of security risks arising from threats to the EIS,
- the location of the EIS within the organisational architecture, where such an arhitecture exists



.

6. figure, Risk management documents – EIR level[45]

In accordance with the continuous monitoring strategy, procedures are develpoed for the ongoing monitoring of the effectiveness of protective measures for the EIS, followed by prioritisation and implementation of selected controls as documented in the system security plan.

The implemented security measures are evaluated according to the evaluation procedure defined in the evaluation plan for implemented security measures. An evaluation report is prepared to document the assessment including comments and recommendations.

Based on the findings in the evaluation report, additional measures are introduced to address the identified the requirements, then the protective measures are re-evaluated and an action plan is prepared to mitigate the remaining risks.

Risks associated with the commissioning or operation of the EIS are assessed based on documents relating to its safety status (system safety plan, assessment report, system risk analysis, action plan). The decision to commission or continue using the system is made by the head of the organisation, in a non-delegable capacity, and is recorded in a formal report.

Through continuous monitoring, it is ensured that protective controls remain proportionate to the risks in the event of changes in the organisational, technological, or security environment. In this context, the following actions are undertaken:

- changes in the EIS or its operating environment that affect the system's security status are monitored, and relevant documents are updated accordingly.
- implemented security controls in the EIS are evaluated based on the continuous

45 Dr. Ágota Albert, own compilation

monitoring strategy, and their status is regularly reported to authorised personnel.
- the security status of the EIS is periodically reviewed to ensure that identified risks remain acceptable to the organisation.
- the plan for withdrawing the EIS from live operation includes measures to address any potential risks.

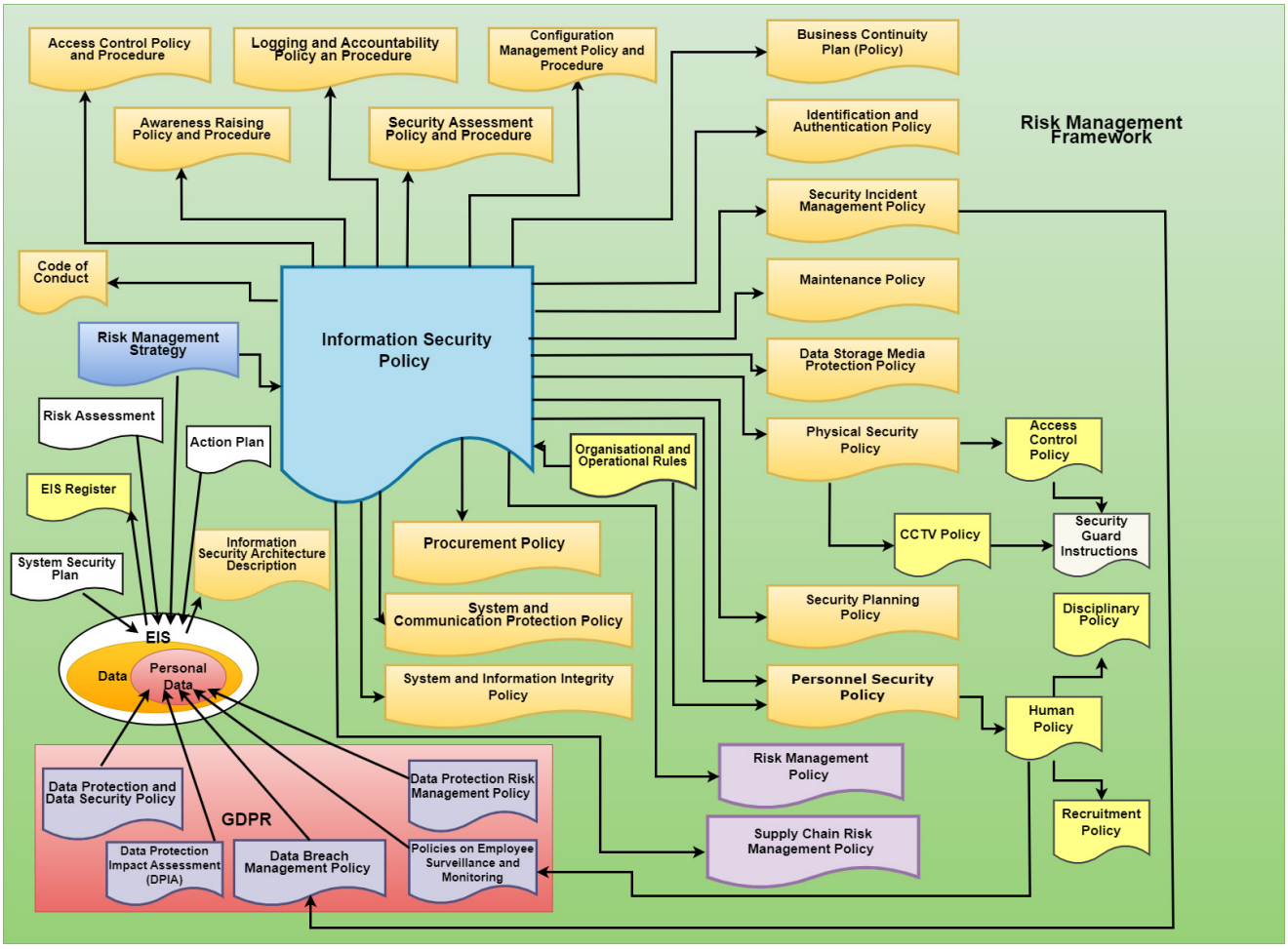
Organisation documentation

Annex 2 specifies the scope of the protective measures, which are aligned with the three principles of confidentiality, integrity, and availability and are documented in the following categories:

- Policies: e.g., information security policy (ISP), physical security policy, risk management policy, code of conduct, etíc.
- Procedures: e.g., incident management, authorisation management, backup procedures.
- Protocols: e.g., communication protocols, access process descriptions.
- Records: such as asset, access, incident, and audit log records.

.

Figure 7, Risk management documents – organisational level[46]



46 Dr. Ágota Albert, own compilation

9.2. Information Security Policy (ISP)

The Information Security Policy (ISP) constitutes the core document of the organisation's information security management system. Its purpose is to protect EISs, data assets, and operational processes from risks, while ensuring compliance with the MK Decree and the NIS2 Directive.

Purpose and role of the ISP

- Establishes information security controls and protective measures.
- Defines security objectives, applicable rules and responsibilities.
- Ensures the confidentiality, integrity and availability of information assets.
- Defines the framework for managing information security risks.
- Supports compliance with relevant legislation, in particular the provisions of the MK Decree and the requirements of NIS2

.

Content requirements of the ISP

The basic requirements of the ISP can be derived from the Annex 7 of the SZTFH Decree and other ISMS frameworks. The policy must include the following elements:

- General provisions (purpose and scope of the policy, references to legislation, organisational units and systems covered)
- Security objectives and principles (risk-based protection principle, minimum requirements for the protection of systems and data, and the foundation of the organisation's security strategy),
- Organisational roles and responsibilities (ISO, DPO, managers, system administrators, user responsibilities, relationships with internal audit and IT operations),
- Regulation of security areas (access management, physical security, operational security, encryption, incident management, network security, third-party management, procurement, personal protection and similar areas),
- List of related documents (procedures, other regulations, records),
- Review and updating (regular scheduled reviews and mandatory reviews in the event of significant changes, including documentation and tracking of changes).

The ISMS is an organisational-level framework that defines the security rules and requirements applicable across the entire organisation. It may take a form of a single document or a collection of documents.

The system security plan and the ISP together provide a comprehensive view of the organisation's security requirements and the protective measures implemented. Where necessary, the ISP may reference separate system security plans or procedures that contain lower-level provisions.

Events that may trigger an update of the ISP include findings from assessments or (re)reviews, security incidents, or changes in applicable laws, guidelines, regulations, standards, and recommendations.

According to the position of the National Cyber Security Institute[47], the mere restatement of the required security measures does not constitute organisational rules or procedures.

47 National Cyber Security Institute: Application Guide for the Catalogue of Cyber Security Requirements for Electronic Information Systems and Organisations, Program Management, Version 1.0, p. 4.

9.3. Other internal regulations

In addition to the ISP, specific internal regulations must be developed to govern individual security processes in greater detail. Their purpose is to define operational and technical activities comprehensively and at an enforceable level.

What internal regulations should be established?

The „Risk Management Documents – Organisational Level (... figure)" presents the regulatory requirements of the MK Decree. All legally required security measures and that address the risks identified in the risk analyses must be documented. The internal regulations cover, but are not limited to, the following areas:

- password management (minimum length and complexity, expiration and repetition prevention, use of multi-factor authentication, etc.),
- data backup and recovery (backup frequency, testing procedures, on-site and remote backups, archiving and deletion rules, etc.),
- mobile devices and remote access (terms of use for organisational and BYOD devices, mandatory use of VPN and encrypted channels, steps to be taken in case of loss or theft),
- software use (prohibition of unauthorized software, license management procedures, update and patching protocols, etc.),
- physical and environmental security (access zones and permissions, camera and access control systems, power supply, temperature and humidity control, fire protection, etc.),
- remote working and home office (permitted devices and applications, encrypted data communication requirements, user behaviour and security awareness expectations, etc.),
- vulnerability management and updates (scanning cycles, prioritsation of critical vulnerabilities, version management practices, etc.),
- access rights management (authorisation procedure for new users, changes and revocation rights, annual authorisation review, etc.),
- procurement (minimum contract content, procurement criteria, etc.),
- risk management (EIS and supply chain considerations, etc.),
- incident management and response procedures etc.,
- personal protection (job descriptions, rules of conduct, access agreements, and related safefguards etc.).

Documentation requirements

Policies are not merely formal documents, but constitute the cornerstones of an organisation's operations and security. Policies must comply with the following requirements:

- Currancy and relevance. All policies should be up to date and tailored to the organisation's specific operations. Versions downloaded from the internet or created solely for formality will not be acceptable.
- Content requirements. The policy should:
  - address the risks identified by risk analysis,
  - be consistent with other regulations,
  - use language that is understandable and appropriate for those affected,
  - define the scope,
  - identify responsible parties and their areas of responsibility,
  - include sanctions, where necessary.

- Governance. The involvement of specialist areas, approval procedures, version management and scheduled reviews are mandatory. Policies must be published in a manner that those affected individuals can access and understand them.
- Accessibility and training. Policies must be made available to employees and understanding must be supported through appropriate (role-based) training.
- Data protection considerations. If the policy includes employee monitoring, applicable data protection requirements must be observed in consulatation with the data protection officer.

Policies are effective only when properly implemented and enforced. Department heads are responsible for ensuring adherence to active policies, and any amendments or newly identified areas requiring regulation must be promptly communicated to management.

Typical mistakes

When developing and managing policies, several common mistakes can reduce the effectiveness of the document, hinder compliance, or may even result in regulatory non-compliance. Typical mistakes include:

- Assuming that „IT will take care of it,"
- Using copied/downloaded, or automatically generated policies that do not reflect actual operations and remain mere Word documents,
- Conducting inadequate risk assessments, or assessments that do not lead to corrective actions,
- Omitting of the data protection officer when processing personal data in of EISs creating conflicts between information security and personal data protection requirements,
- Implementing poorly measured/monitored performance, or relying on superficial (window-dressing) policies and procedures,
- Providing insufficient training and awareness for personnel,
- Lack of accountability regarding roles, responsibilities, and scope; uninvolved individuals may not feel responsible, and tasks cannot be delegated entirely to IT.
- Faiulre to enforce policies effectively. Policies must be both developed and actively enforced through the following actions:
    - formally announced,
    - made accessible in a verifiable manner,
    - compliance activel required and monitored, and
    - non-compliance sanctioned, where necessary.

9.4. Procedures and protocols

The NIS2 Directive and its implementation in Hungary – particularly through the MK Decree and the SZTFH Decree – place strong emphasis on the security-conscious operation of organisations. This includes the documentation, maintenance, and enforcement of key procedures and protocols. These measures ensure that IT system-related operations are conducted in accordance with predefined, auditable procedures rather than on an ad hoc basis.

The procedure

Procedures are documented process descriptions that define the steps, participants, escalation points, and deadlines for handling specific events and situations. In accordance with the MK Decree, procedures facilitate the implementation of regulations governing the relevant area and associated controls.

Regulations and related procedures must aligned with the organisation's risk management strategy. When developed in accordance with the appropriate quality standards and criteria, they significantly contribute to maintaining organisational security.

According to the guidance from the National Cyber Security Institute (NKI)[48], policies and related procedures must be consistent with each other and integrated into the overall information security environment. The NKI's position[49] is that the use of organisational-level security policies and procedures is generally preferable, as this can eliminate the need to develop separate policies and procedures for different organisational objectives or systems. Where justified by the organisational structure, requirements at the policy level may be implemented in organisational policy(ies), while procedures containing system- and role-requirements can be incorporated into the system security plan.

Procedures are required to be established and maintained through regular updates. Modifications may be necessary in response to findings from evaluations or (re)assessments, security incidents, or changes in applicable laws, guidelines, regulations, standards, and recommendations.

The National Cyber Security Institute repeatedly emphasises that the mere repetition of required security measures does not constitute organisational rules or procedures."[50]

The MK Decree specifies a number of procedures, such as

- procedures for the continuous monitoring of the effectiveness of protective measures[51],
- evaluation procedure specified in the evaluation plan[52],
- risk analysis and risk management procedures[53],
- procedures related to regulations (e.g., access control, awareness and training, security incident management, physical and environmental protection, personal security, procurement, supply chain risk assessment and risk management, etc.).

It is required not only to develop, document, approve, issue and communicate the relevant policies and procedures, but also ensure that they are communicated to the appropriate parties in a documented manner and that their contents are effectively implemented.

Quality criteria

The procedures should be concise, role-based, and applicable to daily operations, while addressing not only technical, but also organisational, administrative, and legal aspects. Their validity, maintenance, and revision history must be documented.

Procedures are inadequate if they are not known or accessible to the intended audience, if they are overly technical or complex, unrealistic, or incomprehensible to those expected to follow them. Where necessary, training must be provided, and periodic checks conducted to ensure the alignment between documented procedures and actual practice.

48 NKI EIR guide

49 e.g.: Application Guide for the Catalog of Cyber Security Requirements for Electronic Information Systems and Organisations, Access Control, Version 1.0. pp. 9-10

50 e.g.: Application Guide for the Catalog of Cybersecurity Requirements for Electronic Information Systems and Organisations, Access Control, Version 1.0. Page 10

51 MK Decree Annex 1, Section 1.1.3

52 MK Decree Annex 1, Section 1.1.5.3

53 MK Decree Annex 1, Section 3.2.7, Section 4.2.2 and Annex 2, Section 15.1

Protocol

Protocols are typically shorter, situation-specific action plans that complement organisational procedures. While the procedures set out general rules, steps, and roles, protocols are designed to enable rapid, coordinated, and repeatable responses to a given context (e.g., security incident, data loss, crisis communication).

Protocols are usually scenario-based and define immediate actions, responsible persons, communication steps, and external reporting obligations (e.g., towards authorities or affected customers). A clear example of this is a cyber security incident management protocol, which can prescribe necessary actions with hour-by-hour guidance.

It is crucial that protocols remain up to date and regularly tested (e.g., through tabletop exercises), and are available and understood by the relevant employees.

Protocols are not standalone documents within the information security system, but practical guides closely tied to procedures. Their primary role is to ensure the organisation's ability to respond swiftly and effectively, particularly when meeting the incident management, communication, and recovery obligations set out in NIS2.

9.5. Records and record-keeping

Professional record-keeping is essential for maintaining the security of EISs.

The MK Decree requires organisations to operate a risk management framework that includes the maintenance of up-to-date records. This encompasses documentation necessary for classifying electronic information systems into security categories and implementing protective measures, including risk analyses, threat catalogues, and records of applied controls.

The catalogue of protective measures, provided in Annex 2 of the Decree, specifies the record-keeping requirements in detail. These cover access control, logging and accountability, and configuration management. Organisations must ensure that all events and system configuration changes are accurately documented, enabling traceability and the rapid identification of incidents.

Another key purpose of record keeping is to monitor changes in risks and to continuously evaluate the effectiveness of protective measures. Records should be reviewed and updated regularly, particularly when new threats emerge or significant changes occur in information systems.

Checklist for records

Risk management and security classification:

- Documentation of the security classification of electronic information systems in accordance with Annex 1
- Records of risk analyses and assessments,
- Review and documentation of threat catalogue elements,
- Implementation and monitoring of risk management measures.

Records in accordance with the catalogue of protective measures (Annex 2):

- Programme management: documentation of security policies and procedures,
- Access control: recording access rights and modifications,
- Awareness and training: security awareness training and participant records,
- Logging and accountability: regular logging activities including analysis and review records,
- Evaluation, authorisation, and monitoring: documentation of system evaluations and authorisation processes

- Configuration management: recording system configurations and changes,
- Contingency planning: documentation of business continuity and disaster recovery plans, including test records,
- Security incident management: recording security incidents,
- Maintenance: documenting system maintenance activities and schedules,
- Data storage and transfer protection: documenting the management and protection measures for data storage and transfer,
- Physical and environmental protection: recording physical security checks,
- Personal security: employee security screening and access rights documentation,
- Risk management: documentation of risk management strategies and measures,
- System and service procurement: recording procurement processes and supplier information,
- System and data integrity: recording system and data integrity measures and controls,
- Supply chain risk management: documenting security risks related to suppliers and third parties.

9.5.1. How can all these records be kept and maintained?

Use of an integrated record-keeping system

The most effective approach is to implement a centralised, integrated record-keeping system capable of managing all required records in a structured and up-to-date manner. Such a system may include, for example:

- GRC (Governance, Risk, Compliance) platform,
- ISMS (Information Security Management System) solution,
- a customised document management system (e.g., SharePoint, Confluence + Power Automate, or Matrix42, ServiceNow).

Key features to consider, may include, for example:

- version tracking,
- permission management,
- logging,
- automatic reminders for updates,
- template-based records (e.g., for risk analysis, configuration changes).

Assignment and delegation of responsibilities

A record-keeping system of this scale cannot be managed by a single individual. Therefore, it is mandatory to:

- assign responsibilities for each area (e.g., IT operations, HR, procurement, physical security, etc.),
- establish a clear ownership model, ensuring that every record has a designated responsible person,
- conduct regular internal audits to verify data quality and timeliness.

Automation and integration

Many types of records (e.g., access changes, logging, configurations) can be automaticaly collected and documented using technical tools:

- SIEM systems (e.g., Sentinel, Splunk, QRadar) for logging and event identification,
- Identity & Access Management (IAM) systems for authorisation management and logging,
- CMDB tools for automated configuration management,
- Security tools (EDR, NDR) for recording of events and responses.

Templates and standardised documentation formats

Maintenance is simplified when predefined templates are available for all records, such as:

- Risk analysis forms,
- Incident report forms,
- Authorisation change templates,
- Test reports (e.g., disaster recovery)
- Supplier evaluation tables.

This makes administration faster, more transparent, and more consistent.

Establish regular maintenance timeline

To ensure the effectiveness and sustainability of maintenance, it is recommended to define periode update cycles, for example:

- Quarterly: review of authorsations, audit of logging,
- Semi-annual: risk analysis, updating supplier risk assessments,
- Annually: testing and updating system configurations and security plans.

This maintenance timeline can be coordinated with internal audit schedules and compliance preparation activities.

9.6. The System Security Plan (SSP)

The purpose of the system security plan (hereinafter referred to as: SSP)[54] is to document the security posture of the given IT system, the security measures taken, and the organisational and technical controls in place.

The SSP must be approved by the head of the organisation or the individual responsible for the security of the EIS.[55] Like the IT Security Strategy, IT Security Policy, and Risk Assessment and Risk Management Policy[56], the System Security Plan is a high-level management document.

The measures selected and documented in the SSP must be prioritised and implemented in such a way that plan is regularly updated based on the actual implementation of the safeguards and any deviations from the original plan.

The SSP serves as the basis for deciding whether to commission the system or continue its operation. During an audit, the type of the SSP is classified as an „assurance" document and cannot be excluded from the assessment.

What are the requirements for the SSP?

Structural and content requirements:

- be consistent with the organisational structure
- define the system components that constitute the EIS, including its scope, core functions, and administrative and business services it supports,
- identify the individuals responsible for the roles and duties with the EIS,
- define the types of information processed, stored and transmitted by the EIS,
- determine the security classification of the EIS in accordance with applicable legislation, supported by appropriate justification.

Security and operational requirements:

- list the specific threats affecting the EIS,
- define the operating environment of the EIS and its links or dependencies on other EISs or system components,

54 MK Decree Annex 2, Section 13.2. System security plan protection measures

55 MK Decree Annex 1, point 1

56 1/2025 (I.31) SZTFH Decree Annex 5, Section 1.2.1.2.1

- define and document the basic security requirements for the system along with any additional protective measures applied, if necessary,
- define the current or planned protective measures that meet the requirements, including any enhancements and their justifications,
- record the security-related tasks that require coordination, collaboration or planning between different organisational roles.

The SSP shall be approved by the person responsible for, who shall:

- review and approve it prior to implementation,
- ensure that the plan, including any updates, is communicated to the designated persons and roles, and that it is protected from unauthorised access or modification,
- review the plan at predefined intervals,
- update the plan in the event of changes in the EIS or its operating environment or when issues are identified during the implementation of the plan or the evaluation of the protective measures.

Among the protective measures, several are mandatory components of the SSP, e.g.: as Section 2.88. Activities permitted without identification or authentication. The relevant legislation also defines the basic requirements for the SSP[57].

To support the implementation of the MK Decree, the National Cyber Security Institute of the National Security Service has published SSP templates for all three security levels (basic, significant, high)[58].

How should an SSP be developed?

Developing an SSP should begin with assembling an interdisciplinary team that includes representatives from the IT, data protection, compliance, and the business units that use the system. Templates should be thoroughly customised and tailored to the specific organisational context, based on realistic, system-specific risk analysis. If the SSP is treated merely an outdated, generic system description, using standard text, lacking version control, skipping updates, and ignoring training for stakeholders, it quickly loses its practical value and fails to serve its intended role as a management and operational tool.

57 1/2025 (I.31) SZTFH Decree Annex 7 K13.002 reference code.

58 NKI system security plan templates updated in accordance with the MK Decree

10

Audit process

As with all audits, last-minute preparation is not recommended. As outlined in the legislation, failure to comply may lead to serious consequences, including court proceedings, the obligation to undergo a repeat audit, or disqualification of responsible managers. The key to a successful audit is structured, schedule-driven and itemised preparation. Having rules and procedures in place is not sufficient on its own, evidence is required to demonstrate that the documented measures have been effectively implemented in practice. For each security measure, an action plan must be developed including strict deadlines, responsible persons and appropriate financial planning. If a measure has not yet been implemented due to time or budget constraints, the action plan should be revised with realistic and justifiable and updated financial estimates to reflect the available resources and ensure feasibility. This chapter outlines in detail the steps of the audit process, the required documentation and evidence, as well as best practices to support succesful preparation.

10. Audit process

Written by: György Arató, Alexandra Enyedi, Csaba Mészáros, Dr. Anett Novák, Edina Mandrik, Dr. Dániel Váczi, Dr. Andrea Jeney

10.1. Preparation and collection of evidence

Proper preparation, collection, and organisation of evidence are critical to the success of the audit. During this process, particularly when compiling evidence to demonstrate technological compliance, non-conformities may surface that were either overlooked during internal audits or gap analysis or not examined in sufficient detail.

If the organisation prepares for the audit according to the requirements otulined in Annex 7 of the SZTFH Decree, there is an opportunity to take necessary protective measures or implement technological adjustments in advance, thereby addressing any identified deficiencies before the audit takes place.

It is recommended that the evidence be categorised in accordance with Annex 7 and prepared based on the specific requirements, so the organisation can demonstrate compliance in a focused and effective manner during the audit.

It is recommended that the categorisation be carried out in accordance with Annex 6 of the SZTFH Decree and the evidence identified therein for mandatory testing or document analysis should be properly prepared and collected.

Evidence related to document analysis primarily concerns the organisation's ISMS regulatory environment and all operational and development documentation related to information security. Consequently, if the organisation already maintains a well-structured and properly documented ISMS, collecting this evidence should not pose any difficulties. For regulatory documents, it is recommended each piece of evidence be clearly marked to ensure easy retrieval e.g., in the case of the Information Security Policy, references can consist of page numbers, chapter headings, and paragraph identifiers.

For controls designated for testing, technological checks may be required, for instance, to verify perimeter protection solutions. In such cases, one piece of evidence is typically the documentation of the technology or solution in place, while another is usually a screenshot confirming its operation. Additionally, log files may serve as evidence by verifying that system operates as intended.

For both document analysis and technical testing, it is recommended that evidence be stored and organised in a way that makes it easily traceable to the relevant control point. This can be achieved, for instance, by applying a consistent naming convention or by tracking file names in an Excel table or another indexing format.

10.2. Preparation of persons involved in the audit

Based on Annex 6 of the SZTFH Decree, for controls marked as „Mandatory interview," the auditor is expected to engage with personnel across various roles within the organisation. During these discussions, the auditor will verify the practical implementation of the protective measures specified in the organisation's ISMS regulatory framework. Consequently,

the success of the audit largely depends on the confidence, professionalism, and completeness of the responses provided by the colleagues involved. It is therefore recommended that adequate time be allocated to preparing them during the audit preparation phase.

The following aspects should be considered during preparation:

- The auditor will primarily access the practical implementation of the organisational and technological controls as defined in the regulations, procedures, and other documentation;
- Colleagues designated for interviews must have a solid understanding of the processes relevant to their area of expertise and the specific IT solutions used in those processes to ensure practical compliance.
- Similarly, interviewers must also have a thorough knowledge of the regulations, procedures, and work instructions related to their field of expertise.
- During the conversation, colleagues must be able to demonstrate the application of regulatory and procedural controls in practice, if requested by the auditor. Therefore, it is recommended to review the relevant applicable rules and regulations at least once before the audit

In summary, colleagues designated for interviews must possess the following knowledge prior to the audit:

- the organisational and technological controls outlined in regulations, procedures, and other documentation relevant to their field of expertise;
- the business processes within their field of expertise;
- the IT solutions that supports business processes;
- the intersection of these areas: how the business processes, IT solutions and regulatory requirements interrelate in practice.

The communication and behavioural style of the interviewee also significantly influence the success of the interview. When preparing and selecting interviewees, it is important to emphasise the following soft skills:

- confident but not overly dominant communication;
- precise and concise responses, addressing questions directly without tension;
- calm demeanour, and the ability to handle stressful situations effectively;
- active listening, ensuring questions are fully understood before responding;
- sincerity, even when exact information is not available, using constructive phrasing;
- conscious use of nonverbal signals such as eye contact, open body language, and controlled movements;
- relevance in answers, keeping the conversation on topic, and avoiding unnecessary digressions that may highlight shortcomings.

10.3. Interpretation and presentation of the scoring system through practical examples

One important innovation of the Hungarian audit procedure under NIS2 is that it does not access controls using a simple binary (yes/no) basis. Instead, it evaluates their existence, functionality, and effectiveness in a qualitative and structured manner. The methodology is based on the Audit methodology described in Annex 5 to the SZTFH Decree, which follows the assessment logic of NIST 800-53A Rev. 5.

The purpose of the assessment is not merely to verify the existence of a rule or procedure, but also to determine how effectively it operates in practice. As a standard practice, the auditor evaluates each basic requirement along three dimensions:

- Proper documentation: Are there documented policies, procedures, contracts, or instructions in place? - Example: Does the organisation have a written access management policy that defines the authorisation management process?
- Operation: Are the documented provisions implemented and functioning in practice? - Example: Access rights are assigned in accordance with the policy, but removal and periodic review do not cover all systems, or there is no automated support for these processes.
- Effectiveness: Do the controls achieve their intended purpose? Do they reduce risk and prevent errors or incidents? - For example: No critical authorisation issues were identified during internal audits, but a previous incident revealed delays due to manual revocation processes.

When reviewing the groups of requirements, the auditor first identifies whether each group of requires an organisational level (OL) or electronic information system (EIS) assessment. This classification is predetermined and listed for each group of requirements in the table in Annex 6, and is not subject to auditor's discretion.

- OL-type requirements: These are assessed once at the organisational level; the auditor performs a single assessment covering the entire organisation.
- EIS type requirements: These must be assessed separately for each information system included in the scope of the audit.

The auditor then evaluates the applicability of each requirement group. If a requirement is not relevant to the organisation or system, for example due to a technological or operational cararcteristics, it is classified as „not applicable" and excluded from the audit. It is important to note that Annex 6 specifies certain requirement groups that cannot be disregarded. These always must be assessed and can not be rated as not applicable. The responsibility for determining the applicability or exclusion of each requirement lies with the audited organisation. This information must be clearly documented, as failure to do so may result in penalty points and findings of non-compliance.

In the next step, the auditor selects the appropriate examination methods. Annex 6 contains a table indicating whether document review, interviews or testing are mandatory for each requirement. Usually, a combination of these methods is required.

Next, the auditor identifies which specific elementary requirements in Annex 7 correspond to the requirement gropus listed in Annex 6. Since each group consists of multiple elements, compliance is assessed individually for each element. However, the overall rating is assigned at the group level, which can be one of the following:

- NA (not applicable): the requirement is not applicable in the specific context.
- NM (non-compliant): no evidence is available or the organisation does not meet the requirement.
- M (compliant): sufficient evidence exists and the requirement is demonstrably fulfiled.

If all elementary requirements receive a rating of „Compliant" or „Not applicable", the overall rating for that requirement group is Compliant. However, if at least one elementary requirement is rated „non-compliant," the auditor must assess the severity of deviation. The identified deviations are factored into the

security compliance index (VMI) of the information system under review. This index reflects the degree of non-compliance of the EIS with the applicable regulatory requirements. The following scores are assigned to the requirement groups based on the severity of the deviation:

Classification	Interpretation	Value
Compliant	All basic requirements are met or not applicable	0
Negligible deviation	The deviation does not significantly affect the safety of the EIS.	1
Minor deviation	The measure is partially effective but essentially fulfils its purpose.	4
Significant deviation	The measure is essentially ineffective.	10
Critical deviation	Significant risk, whether from a data protection, business or operational perspective.	1000

The VMI is calculated using the following formula:

$$VMI = 100 - 100 * \frac{\left(2 * \sum_{i=1}^{n} b_i + \sum_{j=1}^{m} t_j\right)}{(20n + 10m)}$$

Interpretation of the formula:

- Requirements vary in importance. Each requirement group belongs to a predefined type. „Assurance" requirements are the core controls.Failure to meet them may compromise the basic functioning of the EIS. Examples include the existence of policies, assignment of responsibilities, or critical security settings. „Supporting" requirements are also important, but supplementary in nature. They enhance the effectiveness of assurence measures, but are less critical on their own.
- Deviation values indicate severity. Each non-compliant requirement is assigned a deviation value reflecting the seriousness of the deficiency. These values are listed in the table above and can be 0, 1, 4, 10 or even 1000 points.
- Weighted evaluation. The system does not simply count the number of deficiencies; it considers both the type of requirement violated and the severity of the violation. Deviations in „Assurance" requirements are weighted twice as heavily as those in „Supporting" requirements. This is achieved by doubling the score for the assurance points, counting support points once, and dividing the total by a denominator that reflects the weight of the requirements examined (20 points for each assurance point, 10 points for support point).
- Resulting peprcentage. The result of this calulcation is a percentage indicating the extent to which the system complies with the requirements. The interpretation is as follows:

VMI value	Compliance rating
≥ 95	Compliant
90–94	Compliant with low risk
80–89	Compliant with significant risk
70–79	High-risk compliant
< 70	Does not comply

Let's take a concrete example from the „System and service procurement" requirement family, which contains both organisational level (OL) and electronic information system (EIS) requirements. In this case, we are focusing on one OL requirement, namely group 16.1. This requirement group consists of so-called P (parameter) elements and O (operational) elements. P-type elements must be defined by the organisation, while O-type elements must be implemented on the basis of these parameters, substituting the specified value. (The table below does not list all the lines set out in Annex 7.)

The auditor assesses the compliance with each P and O requirement individually. In this case, the auditor identified one element that was not fulfiled. As a result, the entire requirement group was rated as „non-compliant" (NM). The severity of the issue was classified as a minor deviation, and therefore the group received a score of 4.

As this is an SZ-type requirement, it is sufficient to assess it once at the organisational level; however, it is factored in all EIS VMI calculations. In addition, it is a „Supporting" type requirement, and it is assigned a single weight in the calculation. Example:

16.1. Rules and procedures		**SZ**	**Supporting**	**NM**	**4**
K16.001_P[1	The persons or roles to whom the procurement rules must be communicated have been determined.	The parameters have been defined			
K16.001_P[2	The persons or roles to whom the procurement procedures must be communicated have been identified	The parameter has not been defined			
...					
K16.001_P[8]	the events that require procurement procedures to be reviewed and updated have been defined	Completed			
K16.001_O_16.1.1.(a)	Procurement rules have been developed and documented.	Completed			
K16.001_O_16.1.1.(b)	The procurement rules have been communicated to the persons or roles specified in K16.001_P[1] .	Not deviating from the parameter			
...					
K16.001_O_16.1.1.1.2.	The procurement rules are consistent with applicable laws, regulations, rules, policies, standards, and guidelines	Compliant			

The following set of requirements illustrates group 16.66, applicable at EIS level. Consequently, the auditor shall conduct the assessment for each EIS subject to audit. Furthermore, as this group qualifies as an Assurance-type requirement, it is given considerably higher weighting in th calcuation formula. However, since all elementary requirements are met, the gorup receives a rating of 0.

16.66. Developer security testing		EIR	Insurance	M	0
K16.001_P[1]	One or more of the following PARAMETER VALUES have been selected: {unit, integration, system, or regression testing}	The parameter was defined			
K16.001_P[2]	The frequency of testing and evaluation has been determined	The parameter has been defined.			
K16.066_P[3]	The depth and coverage of the test type according to K16.066_P[1] shall be determined	The parameter has been determined			
K16.001_O_16.1.1.(a)	The developer of the system, system component or system service is required to develop a plan for continuous security assessments in all phases of the system development life cycle following the design phase.	Completed			
K16.001_O_16.1.1.(b)	The developer of the system, system element or system service is required to implement the plan for continuous security assessments in all phases of the system development life cycle following the design phase.	Completed			
...					
K16.066_O.16.66.5	the developer of the system, system element or system service is required to correct any errors identified during testing and evaluation in all phases of the system development life cycle following the design phase.	Completed			

This is how the auditor evaluates each group of requirements and determines the VMI index for each EIS.

The SZEKI (organisation resilience index) reflects the overall security posture of an organisation's information systems. The formula prescribed by legislation is as follows:

$$SZEKI = \frac{\left(\sum_{i=1}^{n} VMI_i\right)}{n}$$

In practice, the SZEKI is calculated as a simple average. Sum all the EIS VMI values and divide by the number of systems. For example, if there are 3 systems and the VMI values of 95,

87, and 72, then SZEKI = (95 + 87 + 72) / 3 = 84.67.

The SZEKI assessment is summarized in the table below:

SZEKI	Rating	Result
≥ 95	Compliant with negligible risk	Compliant
90–94	Compliant with low risk	Audited
80–89	Medium risk	
70–79	High risk compliant	
< 70	Critical risk Not compliant	Does not comply

10.4. Role of subjective factors in the audit

The purpose of information security audits is to evaluate the extent to which an organisation complies with relevant applicable standards, and its own internal requirements. The SZTFH Decree stipulates that the assessment methodology is based on the NIST SP 800-53A Revision 5 standard. This framework provides a structured, goal-oriented, and objective evaluation of information security and data protection controls following the determination-statement approach. Nevertheless, subjective factors continue to play a significant role in the audit process; such factors are widely recognised and inherent to all audits.

The natural presence of subjectivity in auditing

Although NIST SP 800-53A offers an objective approach in principle, certain subjective elements are unavoidable in audit practice:

- The auditor's professional judgment: Determining whether evidence is sufficient or the extent to which a control is fulfiled often depends on the auditor's experience and expertise.
- The organisation's risk tolerance culture: The same technical control may be assessed differently depending on the organisational environments.
- Tailoring options: Customising the standard provides useful flexibility, but also increases the potential for differences in interpretation.

These factors pose challenges to the consistency and objectivity of audits, particularly during the interpretation and rating phases.

OSCAL: supporting objectivity

The SZTFH prescribes the use of the OSCAL (Open Security Controls Assessment Language) format, which provides a machine-readable structure for documenting, evaluating, and sharing controls. OSCAL aims to ensure standardisation, transparency, and traceability. Maintaining the audit trail in OSCAL format helps to reduce distortions arising from subjective interpretation and facilitates subsequent validation.

The following methods can help mitigate the impact of subjectivity:

- Multi-level professional review: Engaging multiple auditors or subject matter experts in the assessment to enhance objectivity.
- Standardised assessment templates: Applying uniform assessment formats to minimise variability in interpretation.
- OSCAL-based audit trail: Maintaining structured and traceable documentation of audit decisions.
- Automated control checks: Validating technical controls automatically using objective tools.
- Bias awareness development: Training professionals to recognise cognitive biases.

Conclusion

Subjective factors cannot be completely eliminated from the audit process. However, they can be managed through appropriate methodological and technical tools. The critical elements are transparency, proper documentation, and the establishment of a common framework for interpretation. Adherence to the following recommendations can improve the reliability and comparability of audit results:

- Precise formulation of controls: Clearly define controls and their associated expectations.
- Multiple perspectives and expertise: Involve several auditors or subject matter experts to provide diverse viewpoints.
- Comprehensive documentation: Record all decisions and interpretations, serving as a key defense during an audit.

Ultimately, the success of professional audits depends on structured prorcesses, consistent application of audit procedures and assessment criteria, and deliberable management of human factors.

Audit repeatability

A fundamental requirement for all audits is repeatability, providing assurance that results are consistent whenever the audit is conducted. This principle must be applied uniformly across all audits.

10.5. Methodological differences among auditors

The regulatory environment for evaluating information security controls has evolved significantly in recent years. The SZTFH Decree together with the NIST SP 800-53A Rev.5 established a structured and goal-oriented foundation for evaluating security controls. Despite this, significant methodological variations between individual auditors remain evident in practice.

Sources of differences

The observed differences are not solely a result of individual auditor styles, but stern from deeper factors, such as:

- Professional experience and background – An auditor with technical expertise may focus on different aspects than a colleague with a background in management systems.
- Risk sensitivity – Attitudes toward the organisation’s risk culture can significantly influence the assessment.
- Interpretation practices – Variations in reasoning may lead auditors to assign different ratings in identical situations.

For instance, one auditor may concentrate on detailed technical analysis of evidence (e.g., validating log files), while another may palce greater emphasises the consistency of documentation and the coherence of processes. In practice, the balanced outcome is typically found somewhere between these two approaches.

Critical areas where methodological differences arise

Experience shows, that metodological differences are most likely to occur in the following areas:

- Assessment of evidence: Determining the sufficiency and adequacy of available evidence.
- Evaluation of partial fulfilment: Judging and weighting controls that are only partially implemented.
- Severity classification: Establishing the severity of deviations in relation to risk.
- Compliance with statutory structures: Deviations from the legally prescribed assessment-point structure.
- Scope of compliance: Expecting full compliance for each EIS and subsystem, instead of or in addition to sampling.
- Contextual tailoring: Adjusting the assessment to the specific characteristics of the organisation.

Such differences can be particularly challenging in larger organisations where multiple auditors or audit bodies operate in parallel, or in time-series assessments where consistency and comparability with previous audits is essential. Furthermore, these variations may also reflect deeper interpretive differences between organisational-level and EIS-level assessments.

Options for addressing methodological differences

To maintain consistency and comparability in assessments, the following methodological and organisational measures are recommended:

- Establishment of internal benchmarks and reference values: Supports consistent interpretation of organisation-specific requirements.
- Standardisation of rating criteria: Harmonising assessment logic reduces variations stemming from personal interpretations.
- Peer review and role rotation: Incorporating multiple perspectives helps mitigate individual bias.
- Use of OSCAL format (mandatory by the authorities): Uniform documentation enhances transparency and enables subsequent analysis and comparability of audit assessments.
- Adherence to the principle of repeatability: Ensures reliability and reproducibility of audit findings.
- Quality assurance within the audit organisation: Ongoing quality control during the audit process strengthens credibility.

Summary

Methodological differences between auditors are inevitable but can be effectively managed within a regulated framework. A structured assessment model, consistent application of standards and integration of technical tools (e.g. OSCAL) are key to securing an audit process that is objective, comparable and reliable.

Organisations engaged in future audit processes should focus on continuous methodological enhancement and systematic sharing of professional experience. Special emphasis should be placed on the principle of repeatability, as it forms a cornerstone of a stable and sustainable methodological approach.

10.6. Preparation for penetration testing (penetration tests)

As part of the audit, penetration testing (penetration tests) may be required to be conducted by the organisation for EIS classified as high security. The auditor shall determine a time window for such tests, within which the testing may be performed at any point subject to the parameters agreed in advance (e.g., persons involved, organisational units, technical areas, equipment). The following preparatory steps are recommended prior to carrying out penetration tests:

- System selection and scheduling. The auditor determines which systems are to be tested. The responsible system owner and the IT operator must be consulted to determine when testing can take place —during business hours, after hours, or on weekends. The auditor may specify a time window within which the tests may be conducted taking into account the predefined parameters (personnel, system components, technical domains, tools).
- Contact information: Collect the contact details of the responsible personnel and share them with the ethical hacker performing the test. These contacts may be needed if critical vulnerabilities are discovered, in which case immediate notififcation is required.
- Use of non-production environments: Best practice and regulatory guidance is recommended, that penetration testing can be conducted on a a UAT, DEV or TEST environment, which is a stimulated environment reflecting the live system, but contains no live data. The tester must perform the testing strictly, within the defined framework, which must be explicitly defined in advance.
- User accounts. It may be necessary to create and provide multiple levels of user accounts for the testers. Typically, two accounts per user level are requested (e.g., two admin accounts and two standard user accounts).
- Network access for internal applications: For applications accessible via an intranet, VPN settings will need to be shared to allow external testers to access to the internal network Any such access must comply with relevant regulations and be approved through a formal, regulated process.
- Security tools configuration. Certain security tools may require their external IP addresses of testers to be whitelisted. Testers may request this access prior to the testing.
- Vulnerability remediation and retesting. Coordinate with system administrators to schedule development time for remediation or identified vulnerabilities and ensure that remediations are documented, through a regulated change tracking process. Most penetration testing providers will retest vulnerabilities found after remediation. If not explicitly included in the agreement, it is recommended to request a retest to confirm that previously identified vulnerabilities have been successfully resolved.It is important to note that new vulnerabilities may be introduced during the remediation process, making system verification essential.

10.7. Conflict of interest

Conflict of interest in general

This legal concept exist both public and private law and primarly serves to protect public trust and prevent conflicts of interest in specific roles or positions. Its core principle is that an individual cannot simultaneously hold multiple positions that are inherently incompatible.

In public law, incompatibility is particularly evident; for example a member of the National Assembly cannot simultaneously serve as a mayor or as an officer of a business association.

Conflict of interest is also regulated by private law in certain procedural rules, within the framework of so-called exclusion.[59] The purpose of exclusion in procedural law is to prevent bias, specifically to ensure that person who has previously acted in the case or participated in the proceedings, in another procedural role does not take part in the decision-making process.

It is important that an individual concerned is aware of the conflict of interest and reports it within the prescribed deadline. Failure to do so, or reporting after the deadline, renders their decisions invalid and they will be obliged to eliminate the conflict of interest (e.g. resigning from office). If the conflict of interest is not resolved, a situation of legal violation arises, which may be accompanied by other sanctions or legal consequences (such as criminal or disciplinary proceedings, termination of office or position, etc.). The specific legal consequences are determined by applicable legal regulations.

Conflict of interest as a criterion

Auditors are subject to mandatory rules regarding conflicts of interest, and several international standards expressly include this requirement.

The ISO/IEC 17021 standard states that the certification body must be impartial and independent, particularly from the organisation it certifies. Within this framework, the auditing body is prohibited from prodiving consulting or related services to the organisation being audited.

Similarly, the ISO 19011:2018 mandates independence and conflict management among audit methodologies specifying that the auditor may not be the designer, implementer, or operator of the system under audit. ISO/IEC 27006 also requires an independent audit team and the exclusion of potential conflicts of interest. These international standards collectively underscore the stringent obligations associated with the auditor's role: impartiality, independence, and objectivity.

Elements of independence

The concept of independence is defined under law as follows: organisational, financial, and professional independence.

- Organisational independence: The auditor is not dependent on the organisation being audited, and remains structurally separate from it.
- Financial independence: The auditor has no direct financial interest in the audited organisation.
- Professional independence: The auditor conducts the audit in accordance with the methodology and methods required by law determining the course of the audit based on their professional judgement.

NIS2 and independence

In the context of NIS 2, the above dilemma may arise concerning auditors. In this regard, Section 4(10) of the Cybersecurity Act defines auditor as: *„an independent economic entity authorised to perform cybersecurity audit activities in accordance with this Act."* This definition explicitly stresses out independence as a

59 Act CXXX of 2016 on Civil Procedure (hereinafter referred as to: Pp.) Section 12

fundamental criterion and emphasises that the auditor must be an organisation, meaning that a contract cannot be concluded with a private individual to perform the audit.

By contrast, the SZTFH Decrees on auditors do not provide further detailed rules, and offer an explicit legal solution to this dilemma.

The preamble to the SZTFH Decree [5] states: *„The purpose of a cybersecurity audit is for an independent auditor to examine the resilience of the electronic information systems of the organisations subject to the audit against cybersecurity threats."*

The word *„independent"* appears several times throughout the SZTFH Decree. However, the Decree does not elaborate further on this concept, such as how independence is verified, or the legal consequences of violating independence requirements, etc.).

Decree 2/2025. (01.31.) SZTFH addresses supervisory fees and the remuneration of auditors, but does not mention the legal status of auditors.

Decree 3/2025 (04.17) SZTFH otulines the rules for performing of tasks related to cybersecurity supervision and official control, and similarly does not clarify the legal status of auditors.

The dilemma

In light of the above, the following question emerges regarding the applicability of the principle of conflict of interest to NIS2 auditors?

The current legislation does not contain any detailed rules, exclusions or sanctions regarding conflicts of interest. As a result, there are no formal grounds for exclusion on the basis of conflict of interest for auditors appointed and contracted by organisations subject to NIS2 audits. In other words, the selected auditor may even be responsible for preparing the organisation for NIS2 compliance. In such cases, the auditor is still authorised to perform audits according to the organisation's security classification. However, both professional standards and ISO requirements stipulate that the same person should not participate in both preparation and auditing processes. Therefore, in practice this dual role should only occur if the organisation has a sufficient number of qualified professionals to maintain proper separation of duties.

The parties are free to stipulate the terms and conditions in their contract of engagement and the details in the auditor's engagement letter within the framework of contractual freedom, but the law leaves the specifics of the agreement to the discretion of the parties.

This arrangement raises questions regarding its ethical and practical implications. An auditor who provides preparatory training will inevitably familiar with the weaknesses and documentation of the audited organisation. While this can enhance the efficiency and effectiveness of the subsequent audit, it may also challenge the principles of impartiality, independence, and professionalism, as well as potentially compromise the very objectives that NIS 2 was designed to achieve as a legal instrument.

For now, this remains an open issue, with concrete answers likely to emerge only after NIS2 audits have been conducted. Nevertheless, it would be advisable to implement an auditor independence model based on the ISO family of standards for NIS2 audits as well. Additionally, a clear legal definition of the concept of conflict of interest could serve as a useful recommendation for the legislator.

11

Supply chain security

With the ever-increasing interconnection of the digital space, supply chains have become significantly more complex and exposed to various vulnerabilities, especially in critical sectors. One of the key innovations of the NIS2 Directive is the elevation of supply chain security from a secondary consideration to a central pillar of cyber resilience. The objective is clear: an organisation must ensure that its cybersecurity is not compromised through its relationships with external partners, such as suppliers or service providers. Past cyberattacks have repeteadly demonstrated that threat actors often exploit the weekest link in the chain, targeting less secure partners to gain access to otherwise well-protected systems or sensitive data. These so-called „supply chain" or „third-party" attacks are typically difficult to detect, and can lead to considerable reputational and financial damage. This chapter explores how supply chain security can be effectively managed from contractual, risk management, and operational perspectives in light of these challenges. It also highlights how robust supply-chain security can serve as a key driver of business continuity, resilience and customer trust.

11. Supply chain security

Written by: Dr. Ágota Albert, Patrik Cseh, Vencel Cserháti, Dr. Andrea Jeney, Róbert Major, Márk Máté, András Végh

11.1. Review of existing contracts

The risk-based approach of NIS2 requires not only that new contracts align with mandatory security measures, but also that existing agreements be systematically reviewed, and, where necessary, updated.

Information security requirements for contracts

The first step in reviewing current contractual agreements is to ensure that information security requirements are explicitly articulated, particularly in cases where the supplier/business partner has access to essential EISs or processes personal data. The contact review should access whether the following elements are adequately addressed:

- clearly defined minimum level of security measures
- access control policies and resstrictions
- confidentiality obligations and non-disclosure terms
- requirements for logging, monitoring and incident detection
- compliance with data protection laws, including the GDPR and relevant national legislations.

Section 16.7 of the MK Decree on security measures further stipulates that uniform language must be used in contracts related to procurement processes, including development, system adaptation, monitoring, and maintenance, and that the specific security requirements to be clearly defined and included in the contracts.

Extension of security requirements for subcontractors

A key element of supply chain security is that security and data protection requirements must extend not only to direct contractual partners but also to any subcontractors engaged by them. As part of the contract review process, it is essential to assess the following:

- whether the contract prohibits or restricts the use of subcontractors;
- whether there is a requirement to notify and obtain written aproval of subcontractors in advance;
- whether subcontractors are required to meet the same security and data protection requirements as the direct supplier;
- whether the contract includes provisions obliging subcontractors to comply with the same security and compliance terms as the direct supplier;
- whether there is an obligation to inform the customer in advance about the involvement of a direct third party;
- whether it is ensured that any third party involved complies with the security and technical requirements applicable to the direct supplier (e.g. network security, access management, data protection).

Security measure group of 16 as defined in the MK Decree specifies the requirements that must be enforced during procurement processes, depending on the classification assigned

to the relevant EIS. For example, the following obiations apply:

- the developer of the procured EIS, system component or system service must provide a description of the functional characteristics of the applicable security measures („basic", Section 16.8.);
- services provided under a service contract involving EISs must comply with the organisation's electronic information security requirements and implement the protective measures specified by the organisation („basic," Section 16.49);
- the developer of the EIS, system component or system service is required to supply design and implementation details regarding the protective measures. This includes security-relevant external system interfaces, high-level and low-level system design, source code or hardware specifications, and detailed design and implementation information as defined by the organisation („significant", Section 16.9.);
- the developer or supplier must specify the functions, ports, protocols, and services intended for use („significant," Section 16.13), among other requirements.

Regarding subcontractors, it is also important to highlight that if they also process personal data, Article 28 of the GDPR mandates that the data processor (contracted partner) can not engage another data processor (subcontractor) without obtaining the data controller's written authorisation, either on a case-by-case or through general approval.

A Spanish energy market participant, acting as a data controller, engaged the consulting firm ALBOR ENERGÍA S.L. to identify potential customers. Without obtaining the data controller's authorisation, the consultant firm engaged two additional subcontractors, a marketing company (as a sub-processor), which in turn outsourced the task to a call center (sub-sub-processor). The call center contacted customers on behalf of the service provider under the pretext of contract modifications. As the consultant firm was acting as a data processor therefore was permitted to process personal data solely based on the instructions the data controller, the involvement of additional subcontractors without the data controller's authorisation, constitutes a breach of Article 28 of th GDPR. Consequently, the Spanish data protection authority imposed a fine of €12.000 on the consulting firm for the unathorised engagement of sub-processors.[60]

Lessons learned from a NIS2 perspective:

- supply chain risks extend beyond the first-tier contractual partner. Subsequent data processors (sub-processor) may introduce additional risk, particularly when they engage further subcontractors without the knowledge or approval of the client;
- NIS2 requires transparent supply chain management, covering all data processors and their subcontractors;
- Contractual controls and regular audits are essential to mitigate the risk of unauthorised access to data and systems.

60 Spanish Data Protection Agency: No.: EXP202504911.

- a single weak point in the chain (e.g., a call center) can cause a serious cybersecurity incident or data breach.

If general written authorisation is granted for the involvement of subcontractors, the contractual partner should notify the client of any intended changes regarding the appointment or replacement of subcontractors (data processors). This allows the client to assess, and, if nececssary, object to the proposed changes. In accordance with the GDPR, any sub-processor must be subject to the same data protection obligations as those set out in the contract between the data controller and the primary processor. This requirement is also reflected in the NIS2 security measure (19.7), which states that information security requirements specified in the contracts related to the EIS must likewise be included in agreements between the main contractor and any sub-contractors.

Contractual auditability, compliance

When reviewing existing contracts, it is critical to ensure that appropriate audit rights in place to verify the activities both of the supplier and its subcontractors. These rights should include:

- the ability to conduct on-site audits,
- access to relevant documentation (e.g., logs, reports),
- contractual obligations to take corrective action in response to identified irregularities,
- clear regulation of audit frequency and cost allocation.

The MK Decree explicitly requires the continuous monitoring and evaluation of systems as well as implementation of protective measures. This obligation also extends to supplier relationships. In addition, organisations are also required to periodically assess and review the risks arising from the supply chain, particularly in relation to suppliers or contractual partners and the EIS, system components or system services they provide. The requirements can only be effectively fulfiled if cooperation with contractors is subject to formal controls, and the audit rights are not only contractualy-ly defined, but also proactively and regularly enforced.

The Polish data protection authority has pointed out that when entering into a contract under which a business partner processes personal data on behalf of an organisation (acts as a data processor), only those data processors may be engaged who are able to provide the guarantees required under the GDPR. Long-term cooperation without regular and systematic audits or verifications does not constitute sufficient assurance that the data processor will fulfil its contractual obligations appropriately. A history of positive cooperation may serve as a starting point, but it can not itself demonstrate that the data processor provides adequate guarantees for the implementation of appropriate technical and organisational measures. Furthermore, the mere signing of a data processing agreement is insufficient to fulfil the obligation to verify the processor's compliance with the requirements of the GDPR.[61]

11.2. Aspects of new contracts

For new contracts, information security and data protection aspects must be taken into account during the procurement process, including market research, tender invitations, evaluation of bids, drafting of contract documents, and risk assessment of prospective contractual partners.

61 DKN.5130.2215.2020,

Procurement policy

When entering into new contracts, procurement rules must include supply chain security requirements. The rules should specify:

- the pre-qualification requirements for suppliers and service providers,
- information security, data protection and data security requirements,
- mandatory requirements (e.g., ISO 27001, TISAX, SOC2),
- risk-based assessment criteria,
- incident management and reporting obligations to be included in the contract,
- clauses concnerning to the auditability of the contractual partner.

The procurement policy must define methods of cooperation within the organisation, areas of responsibility, and the responsible parties for conducting risk assessments. It is recommended that the policy requires not only a procurement risk assessment as a prerequisite for contract conclusion, but also an information security and data protection risk assessment (e.g. liability insurance requirements, penalty clauses, conditions for immediate contract termination, etc.).

It is important to adapt the procurement rules to the operation's of organisation, the specific characteristics of the sector and the risk classification of EISs, while avoiding general, template-like wording.

The MK Decree establishes requirements for procurement processes and supply chain risk management within a distinct set of protective measures. However, it is the responsibility of the organisation to define a specific content and ensure implementation.

Supplier screening

Article 21 of the NIS Directive requires organisations to proactively manage cybersecurity risks arising from their entire supply chain. This obligation extends to hardware, software, and service providers, including both direct and indirect (sub)contractors. To comply, organisations must be able to demonstrate that they systematically identify, assess, and continuously mitigate these risks. Effective supplier screening is a risk-based process covering the full lifecycle of a supplier.

The depth and complexity of supplier due diligence should be proportionate to the size and the level of risk exposure of the organisation. A two-step model offers a practical solution, dividing the process into basic and advanced methods. While the former is recommended for small and medium-size enterprises (SME-s), the latter is more suitable for large enterprises with complex supply chains.

For SME-s, the objective is pragmatic, risk-based protection that addresses the most significant threats while avoiding unnecessary bureaucracy. This constitutes a basic model.

Supplier categorisation: The process begins with the identifying and ranking suppliers according to their potential impact on the company's operations. The focus should be on critical suppliers (whose loss would result in an operational shutdown) and important suppliers (whose absence would cause significant disruption).

Simplified screening process: For selected suppliers, a simplified questionnaire is the most effeicient tool. The questionnaire should target the essential areas also emphasised by NIS2, including:

- Basic cyber hygiene: Implementation of fundamental protective measures such as antivirus protection, firewalls, regular software patching and updates.
- Data management practices: Accurate procedures for processing, storing and protecting customer and business data in compliance with data protection and cybersecurity requirements
- Incident response capability: Existance of incident response plan, including prorcess for detection, reporting and mitigating security incidents

- Physical security: Adequate safeguards to protect facilities, equipment, and other physical assets from unauthorised access, damage, or theft.

Large enterprises, due to their complex supply chains of large companies, extensive supplier base, and increased risk exposure, require a far more structured, comprehensive and continuously managed screening system.

Multi-level, risk-based screening: Supplierr segmentation is equally essential at this stage, but it must rely on a more refined criteria, such as the degree of data access, the extent of system integration, substitutability, and verall criticality. The screening high-risk suppliers should therefore compromise several interrelated components:

- Detailed questionnaires: Based on recognised standards and frameworks (e.g., ISO 27002, CSA CAIQ, SIG-Full, SOC2) covering a broad spectrum of technical and organisational security controls.
- Multi-layered checks: Collection and analysis of relevant documentation such as security policies, incident response plans and independent audit reports (e.g., results of penetration testing).
- On-site or remote audits: Verification of questionnaire responses and documentation through interviews, inspections and where appropriate, technical testing.
- Continuous monitoring: Employing external cybersecurity rating services to continuously track and access the supplier's digital footprint and exposure.

The possession of relevant certifications is a fundamental requirement for critical partners. Examples of such certifications may include:

- ISO/IEC 27001: Videly regarded as essential for high-risk suppliers.
- Industry-specific certifications: e.g. PCI DSS (finance), SOC2 or CSA STAR (cloud providers), ISO 27017, ISO 27018.
- NIS2 compliance statement/audit: Expected to become a key requirement in the near future.

Measurability and continuous improvement

The effectiveness of the supplier screening process shoud be assessed using three key performance indicators (KPIs):

- Percentage of suppliers screened (%), Proportion of suppliers that have undergone the defined screening process.
- Supplier certification coverage (%), Share of suppliers holding relevant security and compliance certifications.
- Average time to remediate critical vulnerabilities at suppliers (days). Average duration required to address and close high-risk findings.

It is important to emphasise that supplier screening is not a one-off initiative, but a continuous activity embedded within the organisation's risk management framework. Cyber

Confidentiality: Contractual requirements should define access control, data processing and storage, procedures and encryption. Data must be accessible only to authorised personnel.
Integrity: Contract must ensure the accuracy and reliability of data and systems at all times. This includes veryfifng and logging data integrity and manage changes in a controlled and auditable manner.
Availability: Contracts should include measures to guarantee the continuous availability of services, such as system redundancy, regular backups, defined recovery time objectives (RTO), and structured outage management procedures.

The C.I.A triad can be complemented with authentication and non-repudiation. These mechanisms ensure that a parties involved in a transaction or communication cannot deny their actions, the authenticity of their signatures or messages they send. They provide verifiable proof of origin and delivery, making it impossible for someone to falsely repudiate their participation or the integrity of the data.

resilience accross the entire supply chain can only be achieved through systematic and proactive management of supplier risks.

The contract must clearly and identifiably define the security ogliations that not only ensure the secure operation of services and the protection of data, but also guarantee business operations and compliance with applicable legal and regulatory requirements.

When defining contractual security requirements, the primary considerations are confidentiality, integrity, and availability (the CIA triad).

It is recommended to assign specific, measurable requirements to all security expectations, which can be assessed using key performance indicators (KPIs). Examples of such requirements include service availability percentages, response times, recovery objectives (RTO, RPO), or technical specifiifcations of data security, such as encryption standards or access management protocols. Continuous performance monitoring should be ensured through automatic monitoring tools, regular reporting, and periodic audits guaranteeing that service levels are transparent and met by both parties.

The contract should also require the supplier to extend the contractual security obligations to its own subcontractors, thereby ensuring the protection and resilience of the entire supply chain.

Service Level Agreement (SLA)

The SLA or an annex to a contract between an organisation (customer) subject to NIS2 and the service provider (i.e. the supplier). This agreement sets out in detail the scope of the services provided, the quality and quantity standards, the methods for measuring and verifying compliance, and the procedures to be followed in the event of a fault or non-performance.

The contract should allow for security requirements to be updated in response to change the legislation, the threat landscape or the organisation's operational needs.

The agreement shall also specify the consequences of non-compliance with security requirements or service levels. In practice, this may include penalties, fee reductions, suspension of services or even contract termination.

The precise conditions and scope of sanctions must be clearly defined in advance ensuring that both parties fully understand the consequences of any breach of security requirements or agreed service levels. Furthermore, it is reasonable to require that the supplier maintain adequate liability insurance to cover damages arising from a breaches of SLA obligations or contractual security requirements..

Incident management and reporting obligations

New contracts must include incident management provisions that ensure:

- timely reporting of incidents (including compliance with legal requirements that cyber security incidents must be notified to the supervisory authority within 24 hours and data breaches within 72 hours, where applicable)
- a joint incident management process: establishing coordinated procedures between the organisation and the supplier.

- cooperation during investigations: ensuring full collaboration in analysing and resolving incident
- compliance with regulatory reporting obligation: adhering to all applicable obligations to notify relevant authorities.

In the context of contractual provisions on incident management, reference to both the management and reporting obligations for cybersecurity incidents and the management of data breaches, with particular attention to the sanctions stipulated by the applicable legislation.

Legal and regulatory compliance

New contracts must ensure that suppliers and partners fully comply with:

- the NIS2 Directive,
- the GDPR,
- domestic data protection and information security rules (e.g. special requirements for security services, etc.),
- relevant industry standards (ISO, etc.).

It is recommended to request declarations of compliance during the procurement process, for example when soliciting bids, and to include contractual clauses specifying the consequences if a supplier fails to meet its compliance obligations.

These compliance requirements help ensure that supplier relationships do not introduce any hidden risks to the organisation, whether from a technical or legal perspective.

11.3. Risk analysis along the supply chain

A NIS 2 irányelv megköveteli, hogy a szervThe NIS 2 Directive requires organisations to not only identify but also actively manage the cybersecurity risks arising from their supply chains. This entails a structured, continuous, and well-documented risk management process that identifies vulnerabilities, assesses their potential impact, and assigns appropriate mitigation measures. The objective is not to completely eliminate risks—which is unfeasible—but to manage them in a well-informed, business-oriented manner and reduce them to an acceptable level.

Risk analysis should be conducted according to Whitepaper 5.7. However, special considerations should be taken into account when implementing risk mitigation measures, as these measures need to encompass the entire supply chain.

Contractual and legal measures

Supplier contracts should include specific clauses related to cybersecurity and data protection. These should outline the required technical and organisational measures, grant audit rights, and define obligations for incident reporting.

Technological measures

Risks originating from the supply chain can be mitigated through the implementation of the following measures:

- Access management: Enforce the principle of least privilege and require multi-factor authentication (MFA) to minimise unauthorised access.
- Secure communication: Ensure the use of encrypted communication channels (e.g., VPN, HTTPS) for all data exchanges.
- Network segmentation: Isolate systems accessed by suppliers from critical network components to prevent potential breaches from affecting other systems.
- Software integrity: Application of the „Security by Design” principle. Use a Software Bill of Materials (SBOM) to enable traceability and facilitate rapid identification of vulnerabilities.

Organisational and process measures

In addition to technological controls, well-designed organisational processes also play a critical role in enhancing supply chain security. Key measures include:

- Supplier screening: Consistent implementation of the process outlined in Section 11.2 prior to contract signing.
- Insider threat management: Raising awareness among employees, subcontractors, and suppliers through targeted training and education programs.
- Adherence to international standards: Compliance with widely recognised standards such as ISO 27001 or IEC 62443 establishes a common language and framework for security assessment.
- Shared incident management practices: Joint testing of incident response plans jointly with critical suppliers ensures effective coordination during emergency.
- End-to-end traceability: Tracking the lifecycle of all components and software from their origin to the end user is strongly recommended, enabling rapid identification of the source of faults often within hours.

Continuous monitoring and risk management processes

Supplier risk management is a continuous, iterative process, not a one-time project. Its key components incldue:

- Regular reassessment: Conducting annual audits of critical suppliers.
- Threat intelligence: Continuosly monitoring emerging attack techniques and vulnerabilities affecting suppliers or the technologies they use.
- Performance and incident log analysis: Ongoing review of access logs and security incidents related to suppliers.

Information gathered through monitoring (e.g., zero-day vulnerabilities) must be reintegrated into the risk management process. This enables the organisation to re-execute identification, assessment and mitigation steps, ensuring it adapts to the evolving threat landscape.

11.4. What information should be requested from suppliers?

To support the contracting process and to ensure the effective integration of the supply chain into risk and security incident management, the following information must be collected and regularly updated at intervals defined by the organisation:

- basic information about the supplier's organisation and personnel including contact persons (particularly with incident management and contractual reporting obligations), as well as any certifications and qualifications required by the organisation;
- cybersecurity protection measures, as defined by supplier and service provider pre-qualification criteria, along with the information on the supplier's level of information security maturity, e.g. in the form of a self-assessment questionnaire;
- assessment of supply chain risks – including suppliers, service providers and their subcontractors – related to the relevant EISs, system components and system services. This may contain data confirming compliance with a cybersecurity requirements questionnaire.

Security requirements for suppliers and partners

Administrative, physical, and logical cybersecurity requirements must be defined for the supply chain in connection with the relevant EISs, system components, and system services proportionate to the level and nature of each supplier's involvement.[62]

Incident management in the supply chain

The incident management requirements of the NIS2 Directive extend across the entire supplier ecosystem, making proactive cybersecurity operations to a strategic priority for organisations. A single supplier-related incident can trigger a domino effect throughout the value chain; therefore, the resilience and business continuity of partners largely depend on the preparedness of their suppliers.[63]

In this context, risk management must go beyond traditional IT security frameworks. Continuos monitoring is essential not only for direct subcontractors but also for third- and fourth-party neetworks. A key component of this preparedness is 24/7 security monitoring, which includes real-time threat detection, identification of anomalies in partner behaviour, and automated alerting mechanisms.

Reporting obligations under the NIS2 Directive is strict. Supply chain participants must submit an initial report without undue delay and, in any case within 24 hours of becoming aware of a cybersecurity incident. A follow-up report must be provided within 72 hours of the initial awareness of the cybersecurity incident without undue delay. The final report must be submitted no later than one month after the initial report. If the primary communication channel is unavailable, public announcements or notifications via professional organisations may be used as alternatives.

If the incident also involves personal data, the organisation must comply with the data breach notification requirements. It is recommended that the relevant deadlines and responsibilities be clearly defined in the data processing agreement concluded with the supplier.

Incidents should be categorised on their severity. The incident response protocol, which must be initiated immediately upon detection, should include provisions for isolating affected systems, assessing the extent of damage, triggering the communication plan, and engaging both internal and external experts.

To ensure effective recovery, joint exercisees can be organised with business partners, and relevant information should be continuosly shared. Recovery steps must be coordinated across all stakeholders. During the recovery phase, priority should be given to maintaining the continuity of critical services, restoring data integrity, strengthening existing controls, and monitoring the effectiveness of implemented measures.

Effective communication must be based on a multi-layered, secure infrastructure. In addition to primary encrypted communication channels, backup lines, emergency protocols, and if necessary, public platforms should be established. Sensitive data should be transferred with using end-to-end encryption, supported by multi-factor authentication and audited logging.

Clear assignment of responsibilities is fundamental. It is strongly recommended to appoint a dedicated incident manager to lead the incident response process, supported by well-defined escalation routes to facilitate timely decision-making. Collaboration among representatives from relevant departments plays a key role, and external consultants may be engaged when necessary. Contracts should explicitly specify reporting deadlines, liability and compensation frameworks, audit rights,

62 See also: MK Decree 16, Group of protective measures, Chapter 16.2.1

63 ENISA: GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY. June 2023. doi:10.2824/805268 TP-03-23-145-EN-N.

and applicable sanctions concerning to both information security and data protection.

To ensure continuous improvement, staff should receive regular training and new technologies should be introduced, where necessary to enhance defense capabilities. Compliance should be contnuously monitored, deficiencies addressed promptly, and up-to-date industry best-practices consistently applied.[64] Strategic investments in information security can yield long-term cost savings, increased customer satisfaction, regulatory advantages and more favourable insurance terms.

The NIS2 Directive also promotes technological modernisation[65]: artificial intelligence-based threat detection, automated response systems, cloud-based security services, and integrated platforms are increasingly becoming part of the supplier environment. Companies that can effectively coordinate detection, response, communication and accountability will emerge as trusted partners and gain a competitive advantage in the security-conscious digital economy.

Continuous compliance and audit

Supply chain inspections, as well as information security and data protection audits, must be conducted at predefined intervals, either on site or through data requests, to verify compliance. Audits and their evaluations by developing are formalised by developing recommended methodology and request supporting evidence to ensure cybersecurity and audit compliance. The audit plan must be communicated to the supplier in advance.[66]

Education, awareness, and training

Training and awareness-raising among supply chain participants are vital for mitigating supplier-related risks. This involves sharing relevant policies and emergency response plans, conducting practical exercises, and distributing regular cybersecurity briefings tailored for the recipients.

Emergency planning and recovery

Suppliers, service providers and their subcontractors critical to business continuity must be identified and their roles precisely outlined within the relevant plans. Risk analysis should take into account potential service interruptions and ensure that redundancy or alternative solutions are in place to maintain continuity.

11.5. What information should be disclosed as a supplier?

Under the NIS2 Directive, suppliers are required to provide information about the information security maturity level to their business partners. This enables partners to assess the risks within their supply chains. This requirement is a key pillar of transparency for NIS2 compliance and the secure operation of the information security management system.

Information to be shared with partners

The scope of the information to be shared depends on the nature of the service and the specific requirements of the busienss partners. In general, it is recommended – and is often stipulated in contractual agreements – to provide the following information:

- Information on organisational security measures:
  - Information security management system (ISMS): declare the existence of an ISMS (e.g., ISO 27001

64 e.g.: ENISA: CYBERSECURITY ROLES AND SKILLS FOR NIS 2 ESSENTIAL AND IMPORTANT ENTITIES - Mapping NIS 2 obligations to ECSF. June 2025. doi: 10.2824/8870995.

65 pl.: ENISA: TECHNICAL IMPLEMENTATION GUIDANCE. June 2025, version 1.0. doi:10.2824/2702548.

66 See also: 11.1.3. Contractual auditability, compliance

certification) or provide a high-level summary if such a system is in place.
    - Security incident management: describe internal incident management processes and protocols, deadlines, and notification chains. These aspects are also typically covered in data processing agreements.
    - Risk management approach: provide a concise description of the risk management framework, including how security risks are identified and addressed.
    - Technical protection: high-level description of relevant layers of protection (e.g., firewalls, endpoint protection, antivirus protection, physical security measures).
    - Data backup and recovery: information on business continuity and disaster recovery plans
- Contract-specific security guarantees:
    - Service level agreements (SLA): contain security commitments, description of technical and organisational measures (TOM, GDPR Article 32).
    - Auditability, audit rights: the audit rights defined in the contract (Note, that partners may have differing expectations regarding the scope of the audit).
- Data processing and data protection compliance:
    - GDPR compliance: statement on data protection and data security compliance and, where applicable, execution of a data processing agreement (GDPR Article 28).
    - Data storage: information on where data is stored. The region/jurisdiction may be required to ensure compliance with data protection requirements.

Information that can be shared

- The following information can be shared securely: public data, high-level summaries and policies (without confidential technical details), compliance statements (e.g. certificates), contact details of designated personnel, availability of reporting interfaces.
- Information that should not be shared or subject to strict conditions: sensitive technical configuration data (e.g., network topology, encryption keys, access credentials), detailed results of internal vulnerability assessments and penetration tests (summary statements on regular testing are acceptable), personal data (only with proper legal basis and safeguards), trade secrets, and intellectual property. If the requested information is not essential, the principle of proportionality should be applied. In such cases, only the cover page, summary, table of contents, and/or on-site access should be provided.

Principles for disclosure

- Necessity and proportionality: share only what is strictly necessary to prove that a security measure is implemented and effective.
- Risk assessment: assess the risks and the protection measures (e.g., encrypted communication).
- Transfer of personal data: define the legal basis of prcessing personal data, and if necessary, perform balancing tests.

- Non-disclosure agreement (NDA): for sensitive data, requirement of execution of an NDA, and with regard to a data processing agreement, adhere strictly to the terms specified therein.
- Contractual obligations: comply with obligations such as maintaining certifications, ensuring the availability of incident reporting channels, and supporting the enforcement of data subject rights, among others.
- Communication: Be transparent with partners and propose alternatives if necessary.

As a supplier, it is essential to foster proactive collaboration, but all information should be shared on a need-to-know basis with zero trust. The goal is ensure transparency, without introducing additional vulnerability or risks.

12

Useful tools and automation options

One of the biggest challenges in achieving of NIS2 compliance is not simply understanding the regulatory requirements, but integrating them into daily operations. To succeed, organisations need tools and automation solutions that facilitate transparent risk management, ensure auditability, and provide a solid basis for management decisions. From basic spreadsheets to comprehensive GRC platforms and AI-driven applications, there is a wide array of options, each suited to different levels of organisational maturity and available resources. This chapter aims to present the most commonly used solutions and provide guidance on selecting the tool that best aligns with the organisation's need, size and strategic objectives.

12. Useful tools and automation options

Written by: Dr. Dániel Váczi, Gergő Csarnai, Csaba Mészáros

12.1. Excel-based solutions

Excel is one of the most widely used and easily accessible tools used for recording, managing, and reporting cybersecurity and compliance tasks. Its advantages include ease of customisation, quick creation of tables, reports, and charts, as well as widespread availability of basic user knowledge. It supports data sorting and filtering, the use of various formulas and functions, making it suitable for risk analysis, task tracking, or audit plan compilation. The flexible format also enables tailoring to specific processes and requirements without significant development resources.

However, regulatory requirements, such as those set by MK Decree have become increasingly complex. While Excel can address basic needs, ensuring detailed and continuos compliance is demanding. This is particularly evident in organisations managing a large number of EISs, where spreadsheet maintenance, data updates, and evidence organisation require substantial resources. Within corporate groups, the challenges are further amplified: uniform management, consolidation, and tracking of data across subsidiaries or organisational units in Excel is frequently complicated, time-consuming, and prone to errors.

Despite these challenges, many organisations have made efforts to implement the complex requirements in Excel. This has led to a variety of approaches and table formats, which may pose difficulties during audits, especially if the structure, data model, or labeling system is inconsistent. The lack of uniformity in format and content not only hinders internal monitoring but also complicates the work of auditors. For this reason, reliance on the NKI OVI form[67] or the catalogue of protective measures[68] may serve as a useful starting point. Although this does not provide a comprehensive, integrated solution that fully addresses NIS2 requirements, it can offer a solid foundation for structuring compliance efforts and for establishing a uniform documentation framework.

Further limitations and risks related to the use of Excel should also be highlighted. A key drawback is the difficulty of version control, notably when files are exchanged via email or shared network folders. This often leads to parallel use of multiple, versions, increasing the risk of data consistency. While cloud storage solutions can help mitigate this problem to some extent, careful configuration of assess permissions remains essential.

From a security perspective, Excel files can be easily copied and transfered, and the built-in password protection is relatively weak, making it insufficient for securely stoing sensitive data. In addition, Excel lacks a detailed a built-in audit trail, making it challenging to determine precisely who made specific changes and when. This shortcoming undermines its suitability for compliance audits.

67 NKI forms

68 NKI EIR guidance

Another functional limitation is the absence of role-based access control and advanced permission settings, which hinders effective segregation of user rights. Performance may also degrade with large datasets or complex calculations, potentially leading to instability. While automation features such as macros and Visual Basic Applications (VBA) scripts offer certain benefits, they fall short of the level of integration and workflow management available in dedicated Governance, Risk, Compliance (GRC) or specialised management systems.

Excel may serve as a practical solution for smaller organisations, temporary use cases, or for tasks requiring a fast, flexible, and cost-effective tool. Howevere, for long-term, complex processes, extensive data processings, and strict compliance requirements, the use of dedicated information security or GRC platforms is recommended. These tools offer more reliable version control, enhanced auditability, and robust security.

12.2. GRC and management tools

Compliance with NIS2 Directve is not merely a legal or technical task, but a complex, process-based transformation that impacts the entire organisation. Implementation of an information security management system is required according to the Directive in which information is maintained consistently, kept up-to-date and made accesible in a transparent manner. GRC[69] platforms and other specialised management tools play a key role in achieving this.

Medium-sized organisations, and even large companies, frequently attempt to rely on Excel spreadsheets, Word documents, file sharing folders, and emails to manage the complex tasks necessary for compliance and auditing. While this approach may work in a short term, managing the comprehensive requirements of NIS2-based ISMS without a multifunctional, risk-oriented system proves to be highly challenging. Accoring to Hungarian legislation, organisations should consider not only the requirements outlined in the MK Decree, but also the fundamental requirements and supplementary details specified in the SZTFH Decree, which further clarifies these obligations to facilitate a successful audit. Moreover, these two frameworks are not entirely compatible: the audit methodology not only disaggregates requirements that do not have sub-levels (e.g., 1.1.1.1), but it also addresses higher-level requirements, (such as 1.1.1.) specifying parameters at the second level (e.g. 1.1). Implementing this structure in Excel is complex and burdensome. Beyond these structural challenges. responsibilities must be clearly reviewed and communicated to auditors, risks and countermeasures be properly linked, and continuous information flow must be ensured throughout the audit process.

A new dimension of NIS2 is that „paper-based" compliance is no longer sufficient. Authorities and auditors increasingly expect process-based, dynamic evidence demonstrating that an organisation's ability to respond to threats promptly, manage risks effectively, and document incidents accurately.

GRC systems are designed to integrate various areas involving different individuals, teams, and processes. A well-implemented GRC or NIS2 management tool not only provides technical checklists, but also facilitates the monitoring of processes and EISs, management of document versions and decisions, recording and assessment of risks, task allocation and deadline tracking, and the registration and investigation of incidents.

A wide range of tools available on the market: some are optimised for managing financial or IT risks, while others focus specificaly on cyber defense or compliance. For NIS2, it is essential that a tool addresses technical

69 GRC: Anacronym for Governance, Risk, Compliance.

compliance requirements, but also captures the full scope of organisational operations, from management decision support to execution levels.

A carefully selected management tool can bring structure to what would otherwise be a fragmented preparation process beginningat the outset of implementation. Features, such as automated notifications, visual status maps, and transparency through dashboards help support the fulfilment of management responsibilities, which are one of fthe most crucial aspects of NIS2 compliance.

In addition, these tools promote auditability by tracking all decisions, deadlines, and activities; assess organisatitonal maturity and compliance through structured questionnaires and interfaces; and foster knowledge sharing and internal collaboration by allowing different teams (e.g., IT, legal, compliance, management) to work on a unified platform. Ultimately, they integrate risk-oriented thinking into day-to-day operations.

The introduction of NIS2 indicates the end of the era in which organisations could rely on ad hoc Excel lists and email-based consultations. Supervisory authorities are now focused on not only existing policies, but also in how processes operate in practice, how incidents are responded to, and how risks are actively managed.

A well-integrated GRC or management system allows organisations to take a proactive approach, going beyond mere compliance by measuring operational performance, optimising processes and consistently gaining insights from them.

Choosing the right tool is not solely a matter of functionality and budget. It primarly depends on the organisation's maturity level, the extent to which it aims to establish, long-term internal controls and how much value it places on transforming compliance from a mere obligation into a competitive advantage. While there are a variety of international solutions available on the market, in recent years, several Hungarian developments have emerged. These solutions incorporate domestic legislative and industry-specific features to different extents, making them particularly beneficial for organisations looking to implement NIS2 requirements in line with the Hungarian regulatory environment.

Organisations that succeed in not only achieving NIS2 compliance but also embedding it into daily operations will gain a strategic advantage, which requires well-designed and customised management support.

12.3. AI application opportunities

Although the AI Act does not fall within the primary scope of this Whitepaper, it is relevant to note that organisations using (or possibly developing) AI systems for NIS2 compliance purposes must also comply with the requirements of the AI Act. Therefore, where NIS2 compliance is the sole motivation for introducing AI systems, that organisation simultaneously falls under the scope of another legislative framework, which brings additional obligations[70]. Where the proposals presented in this chapter align with the provisions of AI Act, reference are made accordingly.

An AI system as defined by the AI Act[71]: *„a machine-based system that is designed to operate with varying levels of autonomy and and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."*

70 The AI Act imposes obligations on service providers (developers) to ensure the quality and reliability of the (AI-based) products they produce. This can provide a guarantee for organisations (users) using AI systems.

71 REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Chapter 1, Article 3

It may seem like a trivial observation, yet it should be emphasised that AI/MI systems operate on the basis of the input they receive, whether this consist of instructions to be executed, training data for model development, or operational data processed by the system. The well-established *„garbage in - garbage out"* principle applies in this context as well. Accordingly, it can be assumed that organisations that ensure a sufficient level of data quality, enabling the reliable use of AI-generated outputs, will derive the greatest benefit from using AI to support legal and regulatory compliance.

Prompt engineering

„Prompt engineering referes to the process of formulating instructions (prompts) in a way that can be interpreted and processed effectively by an artificial intelligence model."[72] The wording, structure and the level of detail of a prompt significantly affect the quality and reliability of the generated output. For this reason, practicing prompt design - with using synthetic data rather than proprietary or sensitive data is advisable. Digital twins can play a key role in this process. A variety of courses, publications, books, and whitepapers are available to help build exptertise in this field.[73]

AI hallucination

Certain generative AI systems may provide answers even if the underlying data is incomplete or insufficient, which can result in outputs that are inaccurate or misleading. An illustrative example is a NIST 800-53 GPT[74] (Generative Pre-trained Transformer), which claims to „assist in writing the regulatory implementation details of system security plans that comply with the NIST SP 800-53 rev 5 standard and guide you through the entire assessment and authorisation (A&A) process." However, when tested, the output contained two significant inaccuracies: first, the PE-14 controls (found in the MK Decree are included under „12.37. Environmental protection measures") are in fact already applicable to the basic safety class; second, PE-14(3) controls do not exist.

Human oversight[75]

Even if it not mandatory under the AI Act, the principle remains that the more complex significant, or risk-sensitive performed by an AI system[76], the greater the need for human oversight. It must be ensured that the quality and accuracy of system-generated outputs are sufficient for their intended purpose. For instance, when an AI system is used in rule-making, questions arise such as whether the AI-generated rule contains requirements that the organisation is unable to fulfil, or whether any tasks or responsibilities have been assigned to roles that do not exist within the organisational structure. Care must be taken to verify that all assigned tasks and responsibilities correspond to existing roles within the organisation.

Low-risk tasks

Writing Excel functions: Excel is often linkened to a Swiss Army knife, and complex tasks frequently require correspondingly sophisticated functions and macros. Various AI models can provide substantial assistance in this context.

Preparing training materials and summaries: compliance with relevant legislation is typically requires robust rules and procedures. The mere existence of such documents are insufficient; they must be communicated effectively and adhered to. These documents often

72 Prompt design – Wikipedia Stable Diffusion Prompt Book openAI

73 White Paper | The Cyber Security Professional's Guide to Prompt Engineering | Check Point Software

74 ChatGPT - NIST 800-53 Risk Management Framework GPT

75 REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Chapter 1, Article 14

76 REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 3.

Step 1: Identify Applicable Baseline for PE-14 Control

According to **NIST SP 800-53B (Control Baselines)**, the PE-14 control applicability is as follows:

Control ID	Control Name	Low	Moderate	High
PE-14	Environmental Controls		✔	✔
PE-14(1)	Automatic Controls		✔	✔
PE-14(2)	Monitoring with Alarms and Notifications		✔	✔
PE-14(3)	Redundant Systems			✔

Explanation:

- **Low Baseline**: PE-14 is generally **not applicable** at the Low security categorization level.
- **Moderate Baseline**: PE-14 **and enhancements (1), (2)** are required.
- **High Baseline**: PE-14 **and enhancements (1), (2), and (3)** are required.

define responsibilities within the organisation to varying degrees (e.g. using frameworks such as RACI). Compliance with and enforcement of these rules can be facilitated when the individuals to whom the expectations apply receive targeted training. AI-based systems can support this process by collecting role-specific requirements, preparing training materials or summaries, or even converting written text into speech or video formats.

Cybersecurity – embedded AI functions

In the context of automated analysis of large volumes of data, such as log entries, network traffic, it is difficult to envision a cybersecurity service or tool today that does not incorporate AI at some level. Examples include endpoint protection systems that continuously monitor endpoint behaviour rather relying solely on signature-based virus detection, or email filtering systems, that scan incoming and outgoing messages for malicious code. Considering the current state of science and technology (see also: GDPR Art. 32), it is unrealistic to comply with NIS2 without the use of AI, even where the organisation does not explicitly implement AI, as many systems already contain embedded AI functionalities.

AI in the context of the MK Decree
Certain protective measures under the legislation that explicitly require the use of AI, for example:

- 10.24. Maintenance in a timely manner – Automated support for predictive maintenance
- 15.8. Risk analysis and risk management procedures – Predictive analysis

These measures rely on predictions generated through the analysis of large volumes of data, highlighting the integral role of AI in fulfiling these regulatory requirements.

Agentic AI

The complex challenges faced by organisations indicate that those with multiple EISs and classified as significant/high security category will require substantial (human) resources to achieve NIS2 compliance. Tasks such as collection and storage of audit evidence for mandatory internal audits, or locating specific policies buried within extensive documentation, can be resource-intensive. Certain activities, however, may be performed more efficiently by AI agents, provided that appropriate safeguards are in place.

In the context of complex and often interrelated policies, processes, implementation guidelines, and the associated training materials and agreement, changes to one component may not be immediately reflected in other documents, which can lead to interpretation and compliance issues. AI agents can help mitigate such errors.

Moreover, self-checking tasks typically review historical data spanning the past 1/3/6 months. Properly configured AI agents can perform these checks in real-time, or at least with higher frequency, provided they have the necessary access and permissions.

Low-code, no code solutions

A Hungarian developer was able to recreate a copy of the „X" (formerly Twitter) platform in three weeks using low-code, no-code solutions during a challenge[77]. While there is no guarantee that an in-house NIS2 application developed using similar methods will achieve the same functionality as purpose-built software, the combination of creativity, developer and management support, and a limited budget may make it worthwhile to consider developing custom application for the organisation's own use.

77 BOBCATTER: OUR AI-ASSISTED NO-CODE "X-PERIMENT" What we learned from cloning X using only AI tools?

13

Incident management and crisis communication

Cybersecurity incidents and other crisis situations pose significant risk to an organisation's operation, potentially impacting not only the security of IT systems, but also business continuity, the financial stability and reputation. Ad hoc responses are insufficient for managing such events: instead, pre-planned procedures, designated personnel, and coordinated communication are essential. The purpose of crisis communication is to ensure that the organisation delivers consistent, accurate and controlled messages to all stakeholders during a crisis.

Effective crisis management goes beyond technical aspects, requiring coordinated efforts across management, legal, Public Relations (PR) and partner relations functions. For this reason, preparation, regular exercises, and a clearly defined roles and responsibilities are of pararmount importance. This chapter outlines the general framework for these measures and provides a foundation for the scenarios, reporting obligations and communication tasks discussed in subsequent sections.

13. Incident management and crisis communication

Written by: Krisztián Frey, Dr. Andrea Jeney, Dr. Anett Novák, Dr. Dániel Váczi

13.1. General framework

Crises can have major impact on the functioning of an organisation, as they may not only disrupt daily operations, but also seriously affect business continuity, financial stability and reputation. A crisis – such as a cybersecurity incident (or near-incident) or a cyberattack – typically arises unexpectedly and suddenly. Its management cannot be embedded within the framework of normal business processes, but instead requires a distinct organisational approach and a dedicated communication strategy.

It is therefore essential that organisations are consciously prepared for crisis situations. A well-developed, rergularly tested contingency plan enables stakeholders to respond effectively under pressure, provide accurate information to employees, partners, and the public, and manage both stressful situations and potential false reports. Such preparation allows the organisation to focus on resolving the crisis and restoring operations as quickly as possible.

According to the three-stage model of crisis communication, a crisis can be divided into three main phases:

- Pre-crisis phase: the period before the crisis, including preparation, awareness-raising and the development of preventive measures;
- Acute crisis phase: the crisis itself, requiring rapid, targeted, and coordinated responses;
- Post-crisis phase: the aftermath of the crisis, encompassing recovery, evaluation and the incorporation of lessons learned.

In the case of cybersecurity incidents, these phases can be clearly distinguished and documented at the organisational level. The crisis communication plan and incident management policy are particularly important in this context. These documents define:

- the persons or organisational units responsible for each process,
- the procedures and protocols to be followed,
- and the content and target groups of communication messages.

Effective incident management and crisis communication require regular exercises and ongoing awareness-raising among employees. Equally important is the integration of lessons learned from previous incidents and crises into existing documentation structures and templates.

This chapter provides a detailed overview of practical cybersecurity incident scenarios, identifies the competent authorities and organisations involved in incident management, and offers templates that serve as practical guidance on what information should be shared

with whom and what form during a cybersecurity incident.

With all this elements in place, the organisation will be able to respond to crises in a well-prepared and proactive manner, minimising negative impacts and enabling a faster recovery.

13.2. Practical scenarios

This chapter on practical scenarios outlines two complementary processes that unfold in parallel during a security incident: incident management and crisis communication. Incident management focuses on technical and organisational measures taken from detection to recovery, while crisis communication ensures the timely and accurate dissemination of information to authorities, customers, business partners, and the public, in accorandce with legal requirements. Since the two processes operate on similar timelines and involve partially overlapping stakeholders, their overall effectiveness depends on close coordination.

13.2.1. Incident management scenario

The purpose of the incident management scenario is to highlight the process step by step, from detection to recovery and post-analysis, ensuring a rapid, coordinated and well-documented response. The scenario follows the key phases of incident managament, progressing from detection and reporting to assessment, response, and recovery, and finally the integration of lessons learned.

Phase 0: Prerequisites

Before actual incident management can commence, a well-developed and tested Incident Response Plan (IRT/IRP) should be in place within the organisation, a designated CSIRT or IT security team, communication templates and a list of pre-prepared contact persons should be established in advance, along with up-to-date contact information for competent authorities (e.g. NKI/CSIRT-Hungary, NAIH).

Phase 1: Incident detection and identification (0–2 hours)

The obejctive of this phase is to ensure that events are detected as quickly as possible, the occurrence of an incident is confirmed, and its priority is determined. The process begins with the handling of automatic or manual alerts (e.g., SIEM system, EDR), followed by a rapid technical investigation of logs and network traffic. Once clessified (critical, high, medium, low), the crisis team is convened immediately if necessary.

Phase 2: Escalation and initial communication (2–6 hours)

The aim of this phase is to ensure that key stakeholders (e.g., IT management, CISO, legal department, senior management) are notified promptly, and the competent authorities are informed within the required time frame (e.g., NKI/CSIRT-Hungary within 24 hours). At this stage, the crisis communication team is activated, initial messages for the spokesperson channels are validated, and, if necessary, customers, business partners, and suppliers are informed.

Responsible persons: CISO, communications manager, lawyer.

Phase 3: Analysis and isolation (6–24 hours)

In this phase, the scope of the incident is assessed and measures are implemented to prevent further damage. This includes isolating the affected systems, conducting a forensic investigation to identify the point of attack and any malicious activities, and evaluating the impact to determine the extent of data loss and service disruption. Continuous communication with management and designated authorities is maintained throughout the process.

Responsible parties: IT security team, forensic analyst, communications team.

Phase 4: Recovery and restoration (1–5 days)

The goal of this phase is to safely restore the affected systems. This is achieved by restoring from reliable backups, applying security updates, and updating authentication credentials. During recovery, employees receive continuous, factual, and timely internal status updates, while customers and the press are informed as necessary. Care is taken regarding the potential impact of the communicated information. Unnecessary details should be avoided at early stages and only facts that are both necessary and sufficient are shared. The tone of communication should remain confident and transparent, avoiding the creation of panic. The overall objective is to maintain trust and reinforce the organisation's capacity to manage the situation effectitvely, both externally and internally.

Responsible parties: IT Operations, CISO, communications manager.

Phase 5: Reporting and post-analysis (1–30 days)

The organisation prepares a detailed report for the authorities within 72 hours and subsequently compiles a final report within 30 days, following the submission of the interim report. These documents detail the causes of the incident, the response measures implemented, and the risk mitigation measures taken. During the „Lessons learned" phase, these insights gained are incorporated into future processes to improve preparedness and response.

Responsible parties: CISO, legal department, IT security, Compliance.

Phase 6: Corrective measures (1–2 months)

The objective of this phase is to address the weaknesses identified during the incident and to strengthen the organisation's defenses. This involves remediating vulnerabilities by applying security updates (patches) and adjusting firewall rules, updating the incident management and communication plans, enhancing employee security awareness through targeted training (e.g., phishing simulations), and reviewing the security compliance of partners and suppliers.

Responsible parties: IT, HR, Procurement, Compliance.

Phase 7: Learning

Once the incident has been closed, its causes and progression must be thoroughly examined to identify areas where the impact could have been prevented or mitigated. Based on the findings of this investigation, appropriate measures must be adopted to prevent similar incidents in the future or to reduce their potential impact.

+1 post-mortem analysis

This phase includes evaluating detection, response, and mitigation procecdures, reviewing associated documentation, conducting a detailed analysis of the identified causes, and revising the action plan as necessary.

To maintain preparedness, it is recommended that tabletop exercises and live simulations be conducted at least once a year to test the team's responsiveness, validate plans, and ensure a rapid and effective response.

13.2.2. Crisis communication scenario

The purpose of the crisis communication scenario is to ensure timely, coordinated and legally compliant communication within predefined time frames following the detection of the incident. The time periods indicated in parentheses for each phase are calculated from moment the incident is detected.

Phase 1: Initial assessment and decision-making (0-2 hours)

At the inital stage, the incident management team must immediately inform senior management, including C-level executives, the communications manager, and representatives of the legal department, about the nature, severity, and potential consequences of the incident. The objective is to enable a rapid assessment and determine whether activation of the crisis communication team is required.

Where activation is deemed necessary, the pre-designated crisis communication team immediatley begins its operation. The team typically consists of the communications manager, PR specialist, legal representative, senior management spokesperson, and IT or security contact. It is responsible for coordinating communication activities and defining the core messages.

Concurrently, preparations begin for the initial incident report to the NKI in accordance with NIS2, which must be submitted within 24 hours of detection. The legal and incident management teams work together to ensure compliance with applicable legal obligations and initiate timely notification of the relevant authorities.

Phase 2: Information gathering and message preparation (1-3 days)

During this phase, the crisis communication maintains continuous contact with the incident response team to remain fully informed of all developments. This involves identifying the root cause of the incident, determining the systems affected, assessing the extent of any data loss, and monitoring the progress of recovery efforts.

Based on the information collected, the crisis communication team prepares key messages tailored to different target audiences. These messages should be reliable, transparent, and reflect the organisation's proactive and responsible approach.

At this stage, the team also determines who needs to be notified and in what order of priority. Notification of the national supervisory authority (NSA) is required, along with other competent regulatory bodies such as the national data protection authority (NAIH) in the event of a personal data breach. Primary target groups include senior management, employees, directly affected customers, and key partners, while secondary audiences may include the media, investors, or the wider public.

Furthermore, this phase also encompasses the preparation of a detailed notification required under NIS2, which must be submitted within 72 hours of becoming aware of the incident. This notification must outline the probable causes and consequences of the incident, the remedial actions implemented to date, and the planned steps for mitigation and recovery.

Phase 3: Communication and response (3–+ day)

In this phase, it is essential to ensure that information is regularly updated and that communication remains continuous. Ongoing monitoring of social media platforms is also strongly recommended.

Internal communication typically takes place within 1-4 hours of detecting an incident. A briefing is sent to employees summerising the incident, the response measures implemented, and any actions required of them. The purpose is to keep staff informed, maintain morale, and prevent the spread of misinformation and rumors.

External communication generally occurs within 4–48 hours of the incident, and should be initiated when the incident has a significant public impact, such as in cases of widespread service outages or data breaches. This may include issuing a press release, publishing official updates on the organisation's website and social media channels, directly notifying affected customers or business partners via email or letter. Constant oversight of media coverage and social media comments is vital to respond

to questions, and correct misinformation quickly and accurately.

At the same time, continuous contact should be maintained with the authorities, particularly with the NKI. Any new informamtion or significant changes must be promptly communicated to ensure compliance with the NIS2 continuous notification requirements.

Phase 4: Post-incident assessment and improvement

After the incident is resolved, the crisis communication team conducts a comprehensive review of the entire communication process, often referred to as a post-mortem. This assessment examines the effectiveness of the messages, wthe timeliness of the the information delivery, media coverage of the the incident, and the efficiency of internal communication.

Lessons learnt from the incident are used to develop specific recommendations aimed at refining the crisis communication plan and related processes. To maintain operational readiness, tabletop exercises and simulations are conducted at regular intervals, as recommended, in line with NIS2 requirements, involving of the crisis communication team to test plans and ensure a prompt and effective respond in future incidents.

The process also includes the preparation of a final report that transparently summarises the incident, what measures implemented by the organisation, and planned future actions. To foster long-term trust, a campaign presenting a strenghtened security program is launched, a transparent audit process is implemented, and feedback can be gathered from affected parties via questionnaires. Where appropriate, closing interviews may also be conducted as part of press relations management.

Key Crisis Communication Principles NIS2 Context

In crisis situations, the quality and speed of communication directly influence how the organisation is perceived and how effectively the situation is managed. Beyond the strict reporting obligations established by the NIS2 Directive, clear principles are essential to guide communication. The following guidelines help ensure that incident response communication is timely, coordinated, and confidence-building.

- Speed: Compliance with the 24- and 72-hour reporting deadlines under NIS2 is fundamental. Communication sholud also be fast, precise, and accurate.
- Transparency and honesty: The incident should not be concealed. Open and honest communication helps maintain long-term trust.
- Consistency: Messages must be uniform across all communication channels, with no contradictions.
- Empathy: When the incident impact customers or users, it is vital to demonstrate inderstanding and empathy.
- Fact-based: Only verified information should be shared and speculation should be avoided.
- Proactivity: Anticipate questions from the media and stakeholders rather then waiting to respond.
- Authorities and responsibilities: Clearly define who is authorised to communicate and under what circumstances.
- Liaison with authorities: Maintain transparent, cooperative communication with the competent national supervisory authority.

13.3. CSIRT reporting obligations

The NIS2 Directive introduces stricter and more detailed reporting obligations for reporting cybersecurity incidents. The aim of the Directive is to facilitate the rapid, structured,

and consistent flow of information between the relevant organisations and the competent authorities, particularly the national CSIRTs.

According to Article 23 of the Directive, essential and important entities must report any incident that „may have a significant impact on the provision of services."

The reporting process shall be carried out in accordance with the following steps[78]:

Initial Notification

Upon detection of an incident or becoming aware of a significant event, the organisation shall notify the national CSIRT or the competent authority without undue delay, and no later than 24 hours.[79]

Notifications may be submitted through the following official channels:

- https://nki.gov.hu/intezet/tartalom/incidens-bejelentes/
- https://nki.gov.hu/intezet/tartalom/incidens-bejelentes-anonim/
  (anonim bejelentés lehetősége)

The initial notification serves primarily as an early warning, even if comprehensive technical information is not yet available. It should indicate whether the incident is likely to be the result of malicious or unlawful activity and whether it may have cross-border implications.

Detailed report (Incident Notification)

A detailed incident report must be submitted within 72 hours of the initial notification. It shall include an initial assessment of the incident, covering its severity and impact, any observed behavioural patterns and, any availabe technical indicators (e.g., Indicators of Compromise).

The report shall provide all information necessary for the competent authority or CSIRT to assess the significance and associated risk of the incident.

Interim reports

At the request of the competent authority or CSIRT, the organisation shall submit an interim report if the investigation or mitigation process is still ongoing. The interim report shall update the description of the incident, specify the affected systems and outline the technical, organisational, or communication measures implemented to date. This enables the authority to continuously monitor and evaluate the progress and risk level of the incident.

Final Report

A final report must be submitted no later than 30 days after the incident has been resolved. The final report must include a comprehensive description of the incident timeline, the identified root causes, the full extent of the impact, details of the response and recovery efforts, and the measures implemented to prevent similar incidents in the future. The final report must also contain an analysis of any cross-border implications.

In the case of ongoing incidents

If the incident has not been closed by the deadline for the final report, the organisation shall submit an interim report outlining the developments so far. The final report must then be submitted within one month of the incident's final closure.

Cooperation and reporting obligations

In addition to reporting, NIS2 requires the organisations involved to actively cooperate with the competent authorities and CSIRTs. According to Article 21 and 22, this cooperation covers the following obligations:

- supporting the investigation of the incident
- making information, logs, and documentation related to the incident available,

78 Source: Directive (EU) 2022/2555 on ensuring a high level of network and information security across the Union (NIS 2) Sections used: Article 23(1) and (3), Articles 21–22

79 Source: NBSZ NKI – National Cyber Security Institute (CSIRT) – https://nki.gov.hu

- enabling on-site inspections or audits,
- maintaining technical and managerial contact with the authorities,
- taking further measures at the request of the authority, where appropriate.

The authority is entitled to provide feedback on the adequacy of the measures adopted and may prescribe corrective or further preventive measures as deemed necessary.

Deadlines and cooperation

Reporting and cooperation obligations are fundamental requirements for the cybersecurity resilience of organisations. The primary objective of NIS2 is to enhance incident response capabilities and strengthen coordination among Member States. Timely, accurate reporting and constructive cooperation are essential tools to achieve this goal.

Failure to meet deadlines, provide inadequate or inaccurate information, or refuse to cooperate may result in sanctions, fines, and even operational restrictions.

13.4. Media, partners, supervisory authorities, NAIH – what, when, to whom?

In the event of an incident, communication shall be carried out in accordance with the crisis communication plan adopted by the organisation. This plan clearly defines scenarios for information sharing and outlines the roles and responsibities in the communication process. Incident-related communication follows a structured organisational protocol, that takes into account the target audiences and prevailing communication practices. Specific communication elements are determined based on a detailed risk assessment, which identifies potential vulnerabilities and threats.

A key component of the communication process is the establishment of a crisis team, which takes unified and coordinated actions to ensure that affected parties are informed promptly and effectively. External communication is conducted through the media and the partners, as these actors operate outside the organisation.

The key principles of external communication are as follows:

Legality and timeliness

Organisations are required to report incidents to the competent authorities (NAIH, SZTFH, NKI) in accordance with the applicable legal provisions, ensuring that both the content and timing of the report comply with the prescribed requirements. This obliagtion is essential, as failure to report in a timely an appropriate manner constitutes a breach of the law, which may result in sanctions, fines or ineffective incident management.

Under the NIS2 Directive information security incidents must be reported to the NKI (see Chapter 13.3.). In contrast, different procedures apply to personal data breaches, which must be notitfied to the National Authority for Data Protection and Freedom of Information (NAIH). The obligation to notify such beaches is set out in Article 33 and 34 of the GDPR. According to these provisions, the Data Controller is obliged to notitfy the personal data breach not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the fundamental rights and freedoms of natural persons. The responsibility for assessing this risk lies with the Data Controller.

Informing external partners and customers

Following notification of the competent authorities, external partners and customers must also be informed in accordance with the principle of controlled transparency. This involves proactive communication delivered in a

coordinated and carefully controlled way. The organisation acknowledges the occurence of the incident, but discloses only the essential factual information, as approved by legal and compliance representatives. Such proactive communication fosters trust, whereas uncoordinated or poorly handled disclosures may lead to adverse outcomes that can undermine the organisation's business operations and reputation, - consequences that must be avoided. All communication must be uphold the principle of accountability, demonstrating that the organisation treats the incident witht seriousness, is committed to resolve it as swiftly as possible and taking steps to prevent similar incidents in the future. Importantly, this communication does not constitute an admission of liability in a legal sense, as such a determination can only be made upon completion of the investigation. This approach enables the organisation to show strong commitment to incident response while maintaining its legal position.

Informing the media and the press

The media and press are informed according to the model defined in the organisation's communication strategy. The choice of communication model is crucial, as it has a long-term impact on how the organisation is perceived and evaluated. The following examples illustrate different communicatiton models that may guide the organisation's approach[80]:

- Press agency model: aims to influence public opinion in line with the organisation's objectives and to create a positive image.
- Information model: focuses on delivering accurate, factual information to the public.
- Two-way asymmetrical model: uses research to influence and persuade specific target groups, while feedback is limited or one-sided.
- Two-way symmetrical model: emphasises dialogue and mutual understanding, fostering long-term cooperation and trust.
- Personality cult model: inspired by Far Eastern practices, this model centres communication around the influence of a charismatic individual.
- Cultural mediator model: employs cultural adaptation techniques to effectively communicate with diverge audiences.

The media can be informed through various channels such as press releases, newsletters, informational materials, press conferences, or interviews. The organisation evaluates and select the most suitable options in accordance with its crisis communication plan and concludes decisions on a case-by-case basis. Selecting the appropriate communication model and strategy is crucial, as communication plays a decisive role in the success of incident management and in shaping the organisation's long-term reputation.

It is recommended that a spokesperson be appointed to coordinate communication, as this person serves as the voice and representative of the organisation. It is important that the spokesperson is well-prepared and familiar with the appropriate communication techniques, as poor conduct or messaging can easily escalate a crisis. The spokesperson is responsible for delivering accurate and consistent information to the targeted audience, making this role a cornerstone of effective crisis management.

80 Olivér Bor: Crisis Management and Crisis Communication (NKE, EIV training, 2024-25, second semester)

13.5. Involvement of management, PR and legal professionals

Cybersecurity incidents can have a serious impact on an organisation's reputation; therefore the traditional IT-focused approach is no longer sufficient and must be expanded to involve cross-disciplinary cooperation.

The core communication channels consists of managers, PR and legal professionals. As members of the crisis team, they play a crucial role in managing incidents effectively.

Manager

Management responsibility is essential in the event of incidents, as the head of the organisation determines the strategic response and the methods of incident management, including cooperation with external partners.

This responsibility is clearly reflected in all NIS2-related processes, as actions such as security classification[81] and risk assessment require managerial approval. Accordingly, all information related to information security must be communicated to senior management without delay to support timely and well-coordinated decision-making.

Given that the adoption of cybersecurity-related documents, procedures, and operating models is fundamentally a matter of governance, the head of the organisation must also pay an active role in crisis management.

According to the Cybersecurity Act, the head of the organisation is required to appoint the person responsible for the security of the electronic information system or to enter into an agreement with an external person (ISO). Prior to making such a decision, the head may consult the information security manager (ISO), who may offer expert advice and suggest alternative options, however, the final decision rests with the head of the organisation.

Documents that defines the roles and responsibilities are subject to cybersecurity audits and are therefore of particular importance.

The figure below illustrates a holistic approach to organisational communication, highlighting the critical role of each communication function. Effective organisational communication, especially during incidents, relies on close cooperation between managers, PR and IT professionals.

The role of PR

The Public Relations (hereinafter: PR) department plays different roles across the various phases of incident management: during the preparation phase, it develops, operates, and tests possible communication channels and participates in cybersecurity exercises.

In the event of an incident, the PR team must be provided with detailed information about communication protocols and the strategy for public communicating during the identification phase. The content and timing of any public statements are agreed upon separately with senior management.

Throughout the incident, the PR department distributes notifications, press releases, and messaging, while dedicated to maintaining the organisation's image and credibility.

During the recovery phase, the focus shifts to communicating recovery steps and, importantly, drawing lessons learned. It is crucial to emphasise that the PR team does not poses independent decision-making authority, as it operates according to a well-defined scenario. The elements of this scenario are determined by the legal department in consultation with senior management.

All communication should be clear, concise, and factual. It should explain what happened, what steps the organisation is undertaking, and the consequences of the incident. These criteria must be applied with due regard to the nature of the incident and the organisation itself.

81 Government Decree

The organisation's comprehensive communication

Olivér Bor: Crisis Management and Crisis Comunication (NKE, EIV training 2024-25, second semester)

Legal actors

Legal assistance should be sought as early as possible after the incident is identified, as this enables the development of the most appropriate legal response. To support this, the legal department must be fully informed of the incident's details and that the crisis team should include members with legal expertise.

Legal considerations become particularly important in the aftermath of an incident, especially regarding questions of liability. As an organisation may bear responsibility for the incident, there is a potential risk of legal claims or damages from third parties. The legal department therefore consults closely with senior management on matters of legal liability.

In response to the incident, it may also be necessary to draft new documents or revise existing ones to help prevent similar incidens in the future. This responsibility falls to the legal team.

The figure below illustrates the various actors involved in incident managament, highlighting that effective incident response requires complex cooperation across multiple roles. This integrated approach ensure that lessons learned are not limited to individual areas of expertise, but are embedded into broader, forward-looking preventive strategies.

Post-incident recommendations

Incident target	ISP/ICP	CERTs	Legal	Source of incident
COLLECT ALL AVAILABLE LOGS	RETAIN LOGS	MEDIATE CONTACT TO THE LOCAL ISP/ICP	SHARE LEGAL ADVICE	LOG EVENTS
DESCRIBE AN INCIDENT	ASSIST IN OPERATIONAL ACTION	ADVICE IN SIMILAR CASES	SUPPORT LEGAL ACTION	SEARCH FOR SUSPICIOUS USERS
Teach an incident / advise how to avoid it	Explain the mechanism	Share a lesson learnt	Inform about a result / propose a legal action	Advise how to avoid being "an attacker"

Anita Tikos: Incident Management Theory (NKE, EIV training 2024-25, second semester)

14

Physical security measures

The security of electronic information systems must be ensured through a comprehensive approach that integrates physical, IT and environmental safeguards. Protection levels should always be determined based on risk assessments. At the core of access control are elements such as risk classification, access systems, time-limited permissions, and the application of the „principle of least privilege." It is essential to document and regularly review access rights to ensure they remain appropriate and secure.

To mitigate environmental risks, especially in server rooms, a combination of mechanical and electronic tools such as surveillance cameras, fire and water alarm systems, and uninterruptible power supplies are commonly deployed. Passive fire protection measures (fire-resistant walls, doors and windows, seals) along with health-safe fire suppression systems, provide additional layers of safety. Securing output devices (such as monitors, printers, data carriers) is equally important. Ths can be achieved trough physical safeguards like locked rooms and geo-redundant storage solutions. Finally, the management of third-party vendors plays a key role in maintaining overall security.

14. Physical security measures

Written by: Tamás Lóth, Róbert Major, Dr. Balázs Gergely Tiszolczi

Protecting the security of electronic information systems (EIS) depends on the effective intergation of physical, IT, and occupational health safety measures. The level of protection and specific safeguards applied to systems and their components should always be based on the results of information security, physical security, and occupational safety risk assessments, as well as business impact analysis. A variety of safety protocols can be used to mitigate risks, allowing each organisation to adopt solutions that best fit its operational environment and risk profile.

To ensure proper control of physical access and define the necessary technical safeguards, it is recommended to identify and classify facilities, rooms, areas and storage locations supporting EISs based on their risk level. Various access control solutions can be implemented, such as electronic access systems, guarded entry points or accompanied access. Role-based access management is considered best practice, with access levels aligned with the roles and responsibilities defined in the risk analysis. To minimise the risk of unauthorized access, the „principle of least privilege" should be applied, granting users only the permissions required to perform their job duties. Access to high-security areas introduces elevated risk and should require separate, preferably written approval. Mandatory approval is required when high-security systems are involved, as this measure significantly contributes to risk mitigation. When engaging external contractors or suppliers, security is typically ensured through accompanied access. All access should be recorded in a retraceable manner to support audits or post-incident investigations. Certain periods, such as maintenance, office reorganisation, or events, can increase physical security risks. During such times, it is crucial to manage temporary access carefully, implement interim security measures, and address any short-term security gaps.

Various electronic and mechanical security devices can be employed to mitigate physical and environmental risks. Electronic tools may include video surveillance systems, intrusion detection systems, fire detection and suppression systems, and sensors that monitor environmental parameters. Mechanical protection instruments typically consist of locks, padlocks, security grilles, reinforced doors, structural barriers, and secure storage units. Additionally environmental sensors such as temperature, humidity, and liquid leak detectors, help monitor environmental crititcal conditions and trigger alerts when thresholds are exceeded.

These systems are particularly important in machine rooms (e.g.server rooms) where critical components are concentrated and environmental conditions can have a direct impact on IT operation. In such spaces, it is advisable to incorporate architectural and technical features that address common risks from the initial planning stage. These may include, avoiding the use of water, gas and other piping in partition walls; excluding fire-prone technologies from the immediate area; and implementing fire-resistant building structures and lockable, gas-tight rooms where necessary. To enhance power reliability, uninterruptible power supplies (UPS), backup generators, and surge protection should be considered. Physically protecting cables (using cable ducts, enclosed trays, other mechanical barriers) also contributes to the availability and integrity of systems. Where architectural measures cannot

fully eliminate the risk of water damage or other environmental threats, additional technical solutions may be required. For instance, installing water detection systems can provide early warnings of leaks or ingress, enabling a rapid response. All of the abovementioned requirements should be clearly specified in the design documentation.

Multi-layered solutions can be applied to reduce fire-related risks. In high risk areas or where critical technologies are deployed, it is advisable to install highly sensitive aspiration detectors as part of automatic fire detection systems. When combined with point-type optical detectors and dual signal verification, these systems significantly enhance overall protection. This setup enables early fire detection, while minimising false alarms, thereby reducing unnecessary interventions and avoiding technological downtime, which is critical from a business continuity.

In certain cases, particularly if personnel may be present, health and safety considerations must also be taken into account. In such environments, gas-based fire suppression systems that are non-hazardous to human health (e.g., inert or clean agent systems) are preferable. These systems do not require a prior shutdown of protected equipment and allow for safe human intervention during or immediately after the extinguishing process.[82]

In addition to active fire protection systems and equipment, passive fire protection also plays a key role in risk mitigation. The structural enclosure of the room, including walls, ceilings, floors, and doors, must comply with the fire resistance requirements based on the designated risk classification. It is also recommended to seal wall openings, as well as cable and mechanical penetrations, using fire-resistant materials. Automatic door closers, along with fire alarm-controlled doors and windows, further enhance passive protection. Although the use of low-smoke, halogen-free cables is now considered standard, maintaining documented proof of their installation is strongly recommended.

The room's electrical network should be isolated from the rest of the building and designed to allow for manual diosconnection. Emergency stop switches must be protected against unauthorised or accidental activation and positioned for easy access during emergencies. Additionally, the installation of emergency lighting, automatically activated during a power outage, further improves the safety of both personnel and equipment.

The selection and application of specific protective measures should be guided by best practices and a technical protection catalogue that helps to identify targeted, cost-effective solutions tailored to specific risks. This catalogue supports the design, modification, and commissioning processes, including the planning of new facilities and the protection of IT systems operated by external service providers. Responsibility of implementing and operating the approved measures lies with the designated organisational units or, in the case of an outsourced environment, with the contracted service providers. During implementation, it is essential to ensure the professional installation and configuration of the equipment and systems, along with continuous monitoring, maintenance, and documentation of their operation. Maintaining up-to-date documentation and regularly reviewing measures is fundamental for ensuring both compliance and operational security. These reviews must assess not only the functionality of equipment but also the current status of related policies, processes, access control, and audit trails. The reliability of physical security systems can only be maintained through regular testing and drills. Fire and intrusion detection systems must be tested at predetermined intervals, including verification of alarm response times. Additionally, regular

82 Dr. Balázs Gergely Tiszolczi (2019). The practice of designing and applying physical security controls in light of the requirements of the ISO/IEC 27001 standard. Hungarian Law Enforcement, 19(2-3), 233–249.

situational exercises should be conducted for operating personnel to ensure immediate and appropriate action in case of emergency. A key consideration is the coordination between fire alarm systems and uninterruptible power supply (UPS) equipment, particularly the ability to distinguish between drills and true alarm event, to guarantee uninterrupted operation during incidents.

At each site, protecting the data transmission network outside the server room is of paramount importance, both to prevent unauthorised access (e.g., eavesdropping or sabotage) and to avoid accidental damage (e.g., unintentional physical impact). Based on the IT risk assessment and business impact analysis, the organisation may implement the following measures in line with the required levels of confidentiality and availability:

- Lockable cable organisers and network distribution points. All rooms housing network equipment or cabling should be secured with locks and accessible only to authorised personnel. In areas where cables and network devices are concentrated, the installation of an intrusion detection system is advisable to trigger an alarm in case of unauthorised access.
- Use of cable ducts and protective conduits: To prevent physical damage, cables routed along external walls, should be placed in protective ducts or conduits.
- Use of shielded and optical cabling: The use of shielded copper cables or fiber-optic lines is recommended to minimise electromagnetic interference and reduce the risk of eavesdropping.
- Deactivation or physical locking inactive ports: To prevent unauthorised device connections, all unused network ports must be either disabled or physically locked. In production areas ports can also be rendered inoperative, by disconnecting them at a distribution panel located within the secured area. Access to ports, particularly for temporary or maintenance purposes, must be locked and monitored.
- Establishment of redundant data transmission paths: To enhance network resilience, multiple independent data transmission paths should be established, each following a different physical route. This ensures service continuity even in the event of a cable cuts or equipment failures.

In addition to securing data and power transmission channels, controlling physical access to the output points of EISs is also a fundamental requirement, especially when confidential information is displayed, processed or transmitted. The organisation must ensure that such data is only accessible to authorised personnel and protected from both intentional or accidental exposure to unauthorised paries. Effective control begins with identifing and documenting all EIS input and output points. Output devices include any interface through which data can be displayed, printed, recorded, exported or physically connected to other systems. This category may include monitors, printers, scanners, audio output devices, fax machines, copiers, the physical ports of individual IT devices.[83] Risk and impact assessments provide the basis for selecting targeted controls aligned with the identified protection needs, such as:

- Use of enclosed rooms: EIS output devices must be placed in rooms, that are physically separated from public or shared areas. A room is considered enclosed if it is secured by a controlled key system, and/or electronic access. Where multiple IT

83 Dr. Balázs Gergely Tiszolczi (2023): Fundamentals of Information Security. Protection and secure operation of security systems, university lecture notes.

servers, network devices, and other peripherals are concentrated, the use of additional physical protection (e.g., intrusion detection systems) may be warranted.

- Placement and protection of monitors and other displays: Displays must be positioned to prevent unauthorised viewing of on-screen information. To support this, the use of privacy filters is recommended. This requirement is applicable to all displays that are used for security or operational purposes, such as code keypad interfaces or monitoring dashboards.
- Use of printers and copiers: When printing sensitive information, access to the printed output must be restricted to the authorised user. This can be ensured through personal supervision or by requiring user authentication (e.g., ID card, PIN) before printing. Printed documents must be collected immediately to prevent them from leaving unattended.
- Use of audio output devices: When sensitive data is transmitted in audio form, headphones or earphones should be used. If that is not feasible, the room must remain closed during playback to protect against unauthorised overhearing of the information.
- Protection storage media and backups: A key aspect of backup protection is the use of geo-redundant storage, where data is stored in geographically separate locations to ensure recoverability in the event of a local physical incident (e.g., fire, destruction, or system failure). In addition to physical separation. Access to backup media must be strictly controlled, and all data movements must be logged and auditable.

The physical protection of facilities housing EISs involves more than just restricting access; it is also requires continuous monitoring and prompt incident response capabilities. Effective physical access control guarantees that the organisation can detect, log, and manage any event that may indicate unauthorised access to protected areas or sensitive technologies. The following control measures can also be implemented to maintain appropriate physical security:

- Continuous on-site presence or security service provision: Continuous physical presence must be ensured by designated security personnel or contracted security services, including coverage during brakes, rest periods and other service-related downtimes. This is particularly important in areas housing critical infrastructure.
- Utilisation of remote monitoring services: Alarm signals can be routed to a remote monitoring centre, which can also provide a response service if required. This approach may serve as an effective compromise during periods not covered by on-site personnel, such as outside regular working hours.
- Deployment of electronic intrusion detection systems: Intrusion detection systems and analytics-enabled surveillance cameras can automatically generate alarms upon detecting unauthorised access. Camera analytics also support the identification of abnornal or suspicious behaviour patterns.
- Monitoring of electronic access control systems: Access control systems must be configured to detect and report events such as forced entries, use of invalid credentials, and doors left open beyond an acceptable duration. These events should be logged automatically and trigger appropriate alarms.

- Alarm event management: Electronic alarms should be processed via multiple channels, such as email, SMS, integration with remote monitoring services, dispatch centres, or security operations centres (SOCs). It is important to ensure that every alarm is acknowledged and responded to by live personnel 24 hours a day, 365 days a year.

Besides responding to physical security incidents immediately, the organisation must also be able to detect them afterwards. To support this, physical access logs should be regularly reviewed and analysed in a targeted manner, particularly when there is a reason to suspect unauthorised access. Examples of suspicious activities may include access outside normal working hours, unusually long presence in a location, repeated entry into unfamiliar areas, or attempts to use invalid identification. Events, such as doors left open for extended periods or other anomalies recorded by access control systems should also be investigated.

Camera system footage can be used to detect irregularities such as the presence of unregistered visitors, multiple employees entering with a single ID, or tailgating (when someone gains access to a restricted area by following another person without proper identification).

A Security Information and Event Management System (SIEM) integrated into the organisation's information security architecture enables centralised and structured processing of events from physical security systems, such as intrusion alerts, sabotage alerts, forced entries, invalid movement alarms, or camera-generated events. By collecting and correlating log data in real time, the system can automatically identify suspicious behaviour patterns and generate alerts based on predefined rules (use cases).

The SIEM not only supports real-time incident response, but also facilitates the creation of regular and ad hoc reports on physical access events. These reports can be customised according to criteria such as time period, location, user, or event type, and automatically forwarded to the competent security or IT personnel. This significantly enhances transparency, supports retrospective investigations, and contributes to both the prevention and rapid resolution of physical security incidents.

Security requirements for electronic information systems operated by external service providers

If electronic information systems are hosted on infrastructure operated by an external service provider, even within a secure environment, the defined security requirements must still be enforced. When the service provider is responsible solely for the physical environment (e.g., data center infrastructure, power supply, climate control), while the IT systems and equipment remain the property and responsibility of customer, then the primary focus of security requirements should be on suitability of environmental conditions, physical access control, and incident management practices.

Physical security measures, such as access control systems, staffed security personnel, electronic surveillance technology, and fire protection solutions, must be thoroughly documented in the contract. The agreement should also outline the service provider's additional responsibilities, liability for damages, and grant the customer audit rights to enable regular and focused monitoring of the implemented security measures. It is further recommended that the contract should contain a clearly defined termination clause to ensure that the customer's equipment and data can be safely, completely, and intactly removed upon termination of the service. The agreement should specify the method of access, as well as the technical and logistical provisions for removal, along with the service provider's obligation to cooperate throughout the process. Moreover, the service provider is obliged to provide documented

proof, upon the customer's request, that any data stored within the service environment has been permanently erased, ensuring that no copies or access are retained after the termination of the service relationship.

However, if the service provider does not allow the specification of individual contractual terms, such as general terms and conditions (GTC), only those providers may be selected who clearly, verifiably guarantee the physical security and availability requirements identified through the organisation's risk assessment, and which also enforced for its internal systems. These guarantees must be documented in a service level agreement (SLA), either integrated clearly within the GTC, or provided as a separate agreement.

Access control must be established through transparent, documented processes that uphold the proper allocation and regular review of access rights as well as detailed logging of access events. The contract should also specify the reporting obligations, deadlines and procedural steps for incident management.

Compliance with these requirements is fundamental in sustaining and demonstrating the long-term security of hosted systems.

15

Continuous maintenance and compliance management

Upholding cybersecurity compliance is not a one-time task, but an ongoing process that requires continuous improvement and adaptation. It is not sufficient for an organisation to merely meet legal requirements; it must also be capable of responding promptly to emerging changes, new threats, and operational risks. This holds particular importance in the context of the NIS2 Directive and the regulatory requirements in Hungary, where continuous cyber resilience is mandatory. Ongoing risk assessments, regular internal audits, and the development of well-considered, thoroughly documented action plans are required to fulfil this obligation.

15. Continuous maintenance and compliance management

Written by: Dr. Andrea Jeney, Dr. Anett Novák

15.1. What are the key priorities in the next two years?

There are several elements that can and must be considered and integrated into existing processes to uphold this level of compliance.

Key performance indicators (KPIs) may include continuous risk assessment, business continuity and disaster recovery plans, (BCP-DRP) internal audits, incident management, and staff training. It is equally important to draw conclusions and extract lessons from the measurable and monitored indicators.

It is recommended to prepare quarterly status reports and to design and monitor dashboards that illustrate the implementation of action plans. A two-year period is a relatively short to achieve adequate preparation while simultaneously maintaining and improving the current state of readiness.

Following an audit, the findings must be thoroughly analysed, and, if necessary, action plans with clearly defined milestones should be developed to meet the level of preparedness expected not only by the legislator but also by the organisation itself.

15.2. Development of action plans

Action plans must be specific, measurable, achievable, relevant, and time-bound (SMART - Specific, Measurable, Achievable, Relevant, Time-bound). It is important to emphasise that these are not static documents; they should be regularly reviewed, adjusted and improved based on the findings of internal assessments.

A risk-based approach is recommended, meaning that each measure should be directly linked to a clearly identified risk that needs to be addressed. The action plan should be precise and unambiguous in defining what actions are to be taken. Not all deficiencies carry the same level of severity, therefore priority should be given to tasks that:

- Directly and critically impact legal compliance (e.g., regulatory reporting obligations).
- Represent significant risks to the Organisation (e.g., critical vulnerabilities).
- Serve as prerequisites for other essential activities.

The continuous risk management process allows the organisation to operate iteratively, following these key steps:

- Risk identification,
- Risk assessment,
- Development of mitigation measures,
- Implementation,
- Monitoring and reassessment.

This iterative model also ensures that measures reduce organisational vulnerability in a sustainable manner rather than as one-off actions.

- Prioritisation: Deficiencies posing the greatest threat to business operations are addressed first. The organisation holds primary accountability for these processes.
- Expected outcome (report): What will be the final result of the activity? This may include a document (e.g., updated policy), a system function [e.g., implementation of multi-factor authentication (MFA)], completion of training, or successful completion of a test.

- Assignment of responsibility: Identified gaps or areas for improvement should have clearly designated process owners and approvers who oversee and control the processes.
- Deadline setting: Deadlines should be realistic and achievable, which may require additional resources. Both external factors (e.g., legal changes, innovations) and internal resource constraints must be considered.
- Resource estimation: Estimated costs and the required human, technical, and other resources must be allocated to each task. This is essential for budget approval and proper resource management.

The measures can be grouped into four main categories:

- Organisational measures – for instance, defining information security roles and establishing a responsibility matrix.
- Technical measures – such as developing firewall and endpoint protection solutions, introducing comprehensive logging.
- Process and policy-based measures – for example, updating incident management policies, modifying backup procedures.
- Awareness-raising measures – for instance, training programs, simulation exercises, phishing test campaigns.

The development of an action plan is an iterative process and therefore requires constant review and adaptation to evolving circumstances.

15.3. PPT maturity level monitoring

PPT (People, Process, Technology) maturity model is recommended for assessing cybersecurity preparedness and compliance. It provides a clear visualisation of the current state, the desired target level, and the direction of development. Maturity levels are typically defined on a scale from 1 to 5:

- Level 1 (Beginner): Minimal response to threats and immediate needs with ad hoc security measures. There is no unified approach or documented process, and awareness is low.
- Level 2 (Basic): Some basic security controls are in place, but lack systematic application. Certain tasks are performed repeatedly, though not yet fully formalised. Some processes are partially documented, but there is no comprehensive strategy, and responsibilities remain unclear.
- Level 3 (Defined): Procedures, roles, processes are defined and documented, and risks are identified. Responsibilities are clear and key stakeholders are involved. A recognisable security program exists. This represents the minimum requirement under NIS2 and the Cybersecurity Act. At this stage, the organisation has the basic framework and documentation necessary for compliance, but efficiency and optimisation may still be limited.
- Level 4 (Managed and Measurable): Processes are actively managed and measurable. Performance indicators (KPIs) are collected and analysed to evaluate the effectiveness of the program. Regular testing (e.g., incident response exercises, penetration tests) is conducted and the results are used to improve processes.

Security is integerated into business operations. This level is the target for the next two years, where the organisation goes beyond mere compliance to actively and measurably maintain cybersecurity, substantially reducing risks and the potential for legal sanctions.

- Level 5 (Optimised): The cybersecurity program continuously evolves and proactively adapting to emerging threats and business needs. Best practices are incorporated and automation is advanced, and cybersecurity has become an integral part of the organisational culture, treated as a strategic advantage.

The organisation is constantly progressing up the maturity scale towards compliance and should be regarded as a sophisticated and complex system. To achieve this, it is essential to understand the current state and determine the desired level by defining and prioritising tasks appropriately.

Maturity assessment based on the PPT framework helps to:

- objectively evaluate the current state
- focus on targeted improvements in areas of weekness
- prioritise enhancements effectitvely
- sustain long-term compliance and protection levels.

15.4. Weighting of IT, security and business factors

The NIS2 Directive and its domestic legal framework adopt a holistic approach elevating cybersecurity to the managerial level. Consequently, close ooperation between IT, security, and key business domains must be a high priority both in the action plan and its implementation.

Cybersecurity compliance is not merely a technical matter, but also a crucial aspect of business risk management. Accordingly, collaboration among the three main areas is structured as follows:

- IT – technological tools, access, updates, backups.
- Security – policies, risk analysis, incident management.
- Business – critical processes, service continuity, cost and impact assessment.

The individual areas can be grouped as follows:

- IT (IT department): The primary responsibility of IT is to ensure the secure operation and maintenance of systems. This includes implementing technical solutions, managing updates and repairs, operating monitoring tools, and the technicaly resolving security incidents. IT is also responsible for enforcing security standards in day-to-day operations.
- Security (CISO and cybersecurity team): The Security department defines the professional regulatory framework. Its tasks include developing security policies, managing the risk management process, and coordinating incident response. It ensures continuous assessment of the threat landscape, legal compliance, and communication with competent authorities.
- Business (business units and senior management): Business areas are responsible for identifying critical services, systems, and data and for supporting their protection. Leaders incorporate cyber risks into decision-making, ensure the availability of necessary resources, and approve the cybersecurity strategy. Cybersecurity is fully integrated into business operations, contributing to competitiveness and customer trust.

These three pillars can ensure sustainability and compliance only through close cooperation and shared responsibility.

A suggested weighting for decision-making (guideline ratio) could be:

- IT: 30%
- Security: 40%
- Business: 30%

This proportion reflects the principle that security controls should neither impede business operations, nor be entirely subordinate to them. Achieving a balance among the three areas is essential for long-term sustainability.

It should be noted that this proportion represents the relative influence of each area in decision-making, rather than budgetary expenditure. The prevailing mindset often treats this field as an unnecessary expense until an incident occurs due to poor decisions or insufficient preparedness.

15.5. The role of SZTFH and/or NKI

The aim of the NIS 2 Directive is to strengthen the cyber resilience of key sectors and establish a common level of protection across the European Union. In order to accomplish this, it assigns new tasks and powers to the competent authorities of Member States to ensure continuous compliance with legal requirements.

The primary objective of compliance management is to maintain ongoing compliance by establishing a continuous control system that supports this goal. This activity particularly includes:

- the application of a risk-based approach,
- documented operation (e.g. ISMS) and regular review of management systems,
- continuous oversight of the technical and organisational measures implemented for EISs,
- active participation and regular training of relevant stakeholders (managers, IT specialists, legal officers) as part of knowledge management.

As designated authorities, the SZTFH and the NKI play a key role in this process. A brief explanation is neccessary to understand their responsibilities.

SZTFH

The Supervisory Authority for Regulatory Affairs (SZTFH) was originally established to oversee regulated activities, such as mining, tobacco trade, and gambling, and holds official powers in these areas. Its competence was later expanded to include the oversight and supervision of cybersecurity compliance. As a result, the SZTFH became the designated cybersecurity authority for market-based organisations typically falling under the scope of the Cybersecurity Act and the relevant legal framework. These responsibilities are based on Section 23 (1) of the Cybersecurity Act. Cybersecurity-related powers are exercised through the Cybersecurity Directorate within the SZTFH. However, certain sectors, such as public administration and the financial sector, fall under the jurisdiction of other competent authorities.

The SZTFH's official tasks are defined in Section 24 of the Cybersecurity Act and SZTFH Decree 3/2025. (IV.17.), which together provide a comprehensive legal framework governing its competence. These powers can broadly be grouped into the following categories: investigative and supervisory powers, as an authority, the SZFTH is entitled to conduct investigations and impose sanctions. In its advisory and consultative role, also issues recommendations and expert opinions on a wide range of information security matters. Within the framework of its registration responsibilities, organisations subject to NIS2 requirements must register electronically with the SZTFH

within 30 days of determining their in-scope status.

In addition, within the scope of its registration authority, the SZTFH maintains the register of cybersecurity auditors as well as the details of persons responsible for the security of electronic information systems (ISO). The authority also actively participates in information security awareness-raising activities and serves as the sole Member State contact point under the NIS2 Directive.The figure below illustrates its powers:

National regulatory framework - State responsibility (NBSZ NKI)
Organisations operating within the NIS2 sectors, except: finance and public administration

record-keeping	compliance monitoring	audit finding	auditor supervision
enforcement of measures	remediation order	extraordinary inspection	extraordinary audit
information security supervisor	guidelines, recommendations	awareness raising, practices	supervisory fee
COOPERATION – INTERNATIONAL REPRESENTATION – OPERATION-SUPPORTIVE ATTITUDE			

Based on the diagram used in Tünde Bonnyai's teaching material titled Cybersecurity Regulation in Europe (NKE, EIV training 2024-25, second semester)

With regard to NIS2 Directive, the SZTFH has the authority to adopt its own detailing the specific rules for NIS2 audits under the Directive.[84]

All organisations subject to NIS2 Directiveare required to notify the SZTFH of any changes to the information provided during registration. Failure to comply may result in fines, as stipulated in the relevant Government Decree. As part of its ongoing supervision, the SZTFH audits organisations' NIS2 preparedness through mandatory self-assessment reports and automated reporting systems. Organisations can demonstrate compliance by submitting appropriate documentation of their self-assessments.

The SZTFH is granted significant official powers with regard to NIS2 audits, including the authority to order corrective measures to remedy deficiencies identified during audits, conduct on-site inspections if necessary, mandate extraordinary audits (strong powers), request audit documents and access all information related to the audit. Regarding to its official powers, the SZTFH decides on imposing sanctions on a case-by-case basis. This decision takes into account the criteria outlined in Section 6(5) of SZTFH Decree 3/2025. (IV.17.) SZTFH, which governs cybersecurity supervision and task execution, the conduct of official inspections, and the role of the information security inspector, providing detailed rules for these activities. This criteria include factors such as duration and severity of the issue, repetitive nature, intentionality, negligence, and the conduct of the organisation concerned.

Furthermore, as the designated competent authority, the SZTFH plays a pivotal role in incident management, with NIS2 entities obliged to report any cybersecurity incidents directly to it.

In carying out these tasks, the SZTFH maintains close cooperation with partner authorities, such as NAIH, NKI, incident management centres, law enforcement agencies and others.

84 SZTFH Decree 2/2025 (01.31.) on the cyber security supervision fee

National Cyber Defense Institute (hereinafter: NKI)

The NKI is an organisation operating under the authority of the National Security Service, with its powers established by vairous legislative acts.[85] It serves as the national contact point for cybersecurity matters.

Its responsibilities include the prevention and management of threats and scbersecurity incidents affecting cyberspace. This involves receiving, investigating and recording cybersecurity incident reports, as well as maintaining continuous communication with competent agencies to effectively manage crisis situations.

The NKI also participates in the EUCyLON system, conducts vulnerability assessments and coordinates related tasks. Additionally, the NKI undertakes information and awareness-raising initiatives, such as preparing and analyses reports, and organising cyber exercises to raise awareness and promoting best practices incident prevention. The NKI also takes part in international cooperation, including within the CSIRT network.

The NKI has jurisdiction over cybersecurity incidents impacting public administration, local governments, and state-controlled entities.

An overview of the competences is presented in the figure below:

National regulatory framework - State responsibility (NBSZ NKI)
Public administration, municipalities, organisations under majority state control

identification of organisations	registry	ISO registry	security class validation
compliance monitoring	monitoring of developments	guidelines, recommendations,	standard
remediation order	post-incident procedure	information security supervisor	awareness raising, practices
COOPERATION – INTERNATIONAL REPRESENTATION – OPERATION-SUPPORTIVE ATTITUDE			

Based on the diagram used in Tünde Bonnyai's teaching material titled Cybersecurity Regulation in Europe (NKE, EIV képzés 2024-25. II. félév)

The Hungarian cybersecurity system funcitons within the broader state framework; the figure below outlines the legal and structural basis of each institution's competences.

National regulatory framework - State responsibility (NBSZ NKI)
Regulatory and NBSZ NKI responsibility frameworks, mandatory cooperation

NBSZ NKI	SZTFH	KNBSZ	MNB
Public administration municipalities	Organisations operating within the NIS2 sectors	Systems for national-defence purposes	Financial institution
Organisations under majority state control	Except: finance and public administration		

Based on the diagram used in Tünde Bonnyai's teaching material titled Cybersecurity Regulation in Europe (NKE, EIV képzés 2024-25. II. félév)

85 available in Hungarian: https://nki.gov.hu/intezet/tartalom/magunkrol/

16

Compliance-related tasks

NIS2 compliance is inherently interconnected with a range of other legal obligations and industry standards. As such, organisations should view it as part of a unified and comprehensive compliance framework. This is particularly important for entities operating across multiple sectors or jurisdictions, where complexity of overlapping requirements demands a higher degree of coordination, clearly defined responsibilities, and a cohesive compliance strategy.

This chapter provides an overview of the key regulatory and certification frameworks related to NIS2, including data protection obligations overseen by the NAIH, the requirements of the DORA Regulation, applicable to the financial sector, and internationally recognised information security certifications. The chapter highlights areas of overlap with NIS2 and outlines practical considerations to support coordinated and robust compliance efforts.

16. Compliance-related tasks

Written by: Dr. Ágota Albert, William Z. Apró, György Arató, Gabriella Biró, János Gedra, Dr. Andrea Jeney, Dr. Judit Kiss, Márk Máté, Dr. Dániel Váczi

16.1. NAIH obligations

In the context of NIS2, the National Authority for Data Protection and Freedom of Information (hereinafter: NAIH, Authority),[86] speciális szerephez jut, hiszen az általánosholds a distinct supervisory role, particularly in relation to personal data protection. As a supervisory authority under Article 57 of the General Data Protection Regulation (GDPR) acts as an independent body carrying out advisory, recommendation and coordination functions related to personal data processing activities. Within this scope, it monitors personal data processing operations and supervises the proper application of the GDPR. Consequently, organisations are under a continuous obligation to cooperate and maintain communication with the Authority to ensure that personal data is effectively protected throughout all data processing procedures.

The jurisdiction of the NAIH is defined in Section 38(2) of Act CXII of 2011 on the right to self-determination in relation to information and on freedom of information (hereinafter: Infotv.). Accordingly, the Authority is responsible for monitoring and promoting the enforcement of rights relating to the protection of personal data and access to data of public interest ground, as well as for facilitating the free movement of personal data within the European Union.

Based on the above, the Authority's competence is determined by the involvment of personal data. According to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person („data subject"); A natural person is identifiable if they can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. of that natural person. The concept of personal data is therefore broad and includes, for example, names, email addresses and credit card details. Information relating to the operation or management of a legal entity or other organisation does not constitute personal data and is therefore falls outside the scope of data protection legislation. However, personal data processed by legal entities remains subject to data protection laws.

Organisations covered by NIS2 Directive, that process personal data, are subject to the same obligations under the GDPR as any other data controller or processor, including accountability, documentation, and compliance requirements. To ensure accountability, organisations must maintain proper documentation (Data Protection Policy, Privacy Notice, Employment Contracts, Incident Management Policy), There are also required to appoint a data protection officer (DPO) in accordance with Article 37 of the GDPR, and to implement the data security principle both prior to the commencement of

86 A Hatóság önálló jogi személyiséggel rendelkező autonóm államigazgatási szerv, mely az adatvédelmi biztos jogutódjaként jött létre 2012-ben.

data processing activities and throughout the entire data processing lifecycle.

Communication with the Authority may be examined from two main perspectives: (1) regarding the appointment of a DPO, and (2) the notification of personal data breaches.

It is advisable to appoint a data protection officer in all cases, even when not mandatory under Article 37(1) of the GDPR, in order to facilitate effective communication with the Authority. The DPO acts as a professional point of contact who must be familiar with the organisation's data processing activities, support the timely detection of data breaches and ensure proper communication with the Authority. The DPO must be registered with the Authority using a dedicated electronic form.[87]

It is important to note that, beyond its coordinating and advisory role, the Authority also exercises official supervisory powers over data processing activities, which include the ability to impose sanctions for personal data breaches and for non-compliance. These powers extend to monitoring compliance with the GDPR (e.g. restricting or prohibiting certain data processing activities) and where necessary, imposing administrative fines. The Authority's decisions are always legally binding, ensuring that its decisions are enforceable.

In the event of a data breach, the Authority retains its fufll supervisory and enforcement competence. According to Article 4(12) of the GDPR, personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Cybersecurity incidents affecting NIS2-regulated organisations often meet the criteria for data breaches. However, it is important to recognise that, despite their overlap, the two types of incidents differ significantly in nature and regulatory response.

The figure below illustrates the key differences and overlaps between data breaches and cybersecurity incidents:

Incident types

Data breach	Cybersecurity incident
- Definition: Art.4. point 12. of the GDPR - sterns from a security breach - affects personal data	- Definition: Section 46 of the Cybersecurity Act (Act LXIX of 2024)
Definition: Art.4.point 1. of the GDPR	Data and sevices (CIA)

Own figure (Dr. Andrea Jeney - NKI - Crisis Management and Crisis Communication, 2024-25/II semester)

With regard to data breaches, affected organisations are required to act in accordance with Article 33-34 of the GDPR.

Article 33(1) states that the data controller shall without undue delay and, where feasible, no later than 72 hours after having become aware of the data breach, notify the competent supervisory authority in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

In this process, the DPO plays a fundamental role, being responsible for categorising the data breach and notify the Authority when the conditions set out in Article 33(1) of the GDPR are met. Article 33(3) of the GDPR specifies the information that must be included in such notification.

The categorisation of the data breach is therefore the responsibility of the organisation concerned; however, the Authority is entitled to reassess the classification. Proper categorisation is crucial, because, for data breaches that are likely to result in a high risk to the fundamental rights and freedoms of natural persons, require the organisation, as the data

87 https://www.naih.hu/adatvedelmi-tisztviselo-bejelento-rendszer

controller, shall communicate the data breach to the data subject without undue delay in accordance with Article 34 of the GDPR. It is equally essential that the data breach be thoroughly documented and that the notifiifcation be made in line with the principles of transparency and accountability.

In addition, the organisation is required to document any personal data breaches, including the facts related to the personal data breach, its impact and the remedial action takens according to Article 33(5) of the GDPR. The organisation shall make the documentation available to the Authority upon request, in order to ensure that the supervisory authority can effefctively exercise its supervisory powers. Obviously, these administrative and professional tasks are most effectively managed by a DPO.

Pursuant to Section 25/N(2) of the Infotv., the Authority organises an annual conference for DPO-s[88], offering a regular and interactive forum for discussion and collaboration. The purpose of this conference is to promote a consistent, transparent legal practices in the interpretation and application of data protection legislation.

Looking ahead, the Authority seeks to further promote the principles of proactive protection and sustainability in the data processing activities, thereby supporting the identification and mitigation of data security and cybersecurity risks for NIS2 organisations. Achieving this objective requires active knowledge sharing and the continuous improvement of data protection practices.

88 For more details, see: https://www.naih.hu/adatvedelmi-tisztviselok-konferenciaja

16.2. DORA compliance

The DORA (Digital Operational Resilience Act) — formally Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 — was published in the Official Journal of the European Union. The fundamental objective of DORA is to establish a harmonised set of requirements for the IT systems and environments of financial institutions across the European Union.

In line with this goal, the scope of DORA applies to the 20 types of financial institutions listed in Article 2 of the Regulation and as well as to third-party ICT service providers. Some of these entities are also classified essential or important under national rules implementing Article 3 of the NIS2 Directive, and are therefore subject to both DORA and NIS2. For financial institutions classified as essential or important, DORA serves as a sector-specific EU legal act (lex specialis) in relation to the NIS2 Directive. As a result, DORA's provisions take precedence and are applied first to financial institutions falling within the scope of NIS2. Another key distinctiton between NIS2 and DORA is that while the NIS2 Directive requires transposition into national law, DORA is a directly applicable EU regulation, meaning its rules apply uniformly and automatically to all organisations within its scope across the entire EU.

The main pillars of DORA are as follows:

- ICT risk management,
- ICT-related incident reporting,
- Digital operational resilience testing,
- Management of ICT risks originating from third parties,
- Information-sharing arrangements,
- Competent authorities.

With regard to ICT risk management and the establishment of other requirements in proportionate to the risks, the Regulation adopts the definitions of micro, small and medium-sized enterprises as set out in the NIS2 Directive.

From an operational perspective, the most significant overlap between the domains regulated by DORA and NIS2 is the obligation to report incidents. DORA requires incidents to be reported to financial supervisory authorities (in Hungary, the Hungarian Central Bank) and provides detailed rules and standardised reporting templates for this purpose. At the same time, for organisations falling within the scope of NIS2, incident reporting to the national CSIRT, may also be required by the regulator when transposing the directive into national law. In Hungary, as in several other EU Member States, institutions covered by DORA, also report major incidents to the CSIRT. (For more information on CSIRT, see 14.2.)

16.3. ISO 27001

The ISO/IEC 27000 series is a family of international standards and guidelines for information security. These standards provide best practice for managing information security risks by implementing controls within an information security management system (ISMS). Among them, the ISO/IEC 27001:2022 is the most important and widely adopted standard.

It is an industry-neutral, globally-recognised international standard that outlines a systematic approach for managing sensitive company information. This includes risk assessment and application of appropriate controls, through the implementation and ongoing improvement of an ISMS.

The primary objectives of an ISMS are to ensure the confidentiality (access to sensitive information is limited to authorised personnel), integrity (detecting, preventing, and correcting any compromise to protected data, including its unauthorised deletion or alteration) and availability (protected information is available to authorised users when needed and in the required form.) These three principles — Confidentiality, Integrity, and Availability — are commonly known as the CIA triad in English or BSR in Hungarian.

Organisational background

The ISO/IEC 27001:2022 standard was developed jointly by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). The first edition of the standard was published in 2005 and followed by revisions in 2013 and most recently in 2022.

Regulatory background for certification

ISO 27001 certification is a formal process through which an independent, accredited certification body verifies that an organisation's ISMS complies with the requirements set out in the ISO/IEC 27001:2022 standard.

The ISO/IEC 27001:2022 standard provides detailed guidelines on how to implement the information security controls listed in Annex A of the ISO/IEC 27002:2022 standard. Unlike ISO/IEC 27001, it does not contain mandatory requirements, but serves as a practical guidance to help organisations to effectively implement and manage these contols.

Scope of ISO 27001 certification

Organisations define the scope of their ISMS, based on their specific needs and context. However, the scope of the ISO 27001 audit is strictly limited to the boundaries established for the ISMS.

Internal audit

The ISO/IEC 27001:2022 standard requires organisations to conduct internal audits at planned intervals as part of their performance evaluation. These audits evaluate whether the ISMS meets both the organisation's information security management requirements and the ISO/IEC 27001:2022 standard, as well

as whether it is effectively implemented and maintained.

Certification audit

The certificate is valid for 3 years, however, an annual surveillance audit is required, and a renewal audit is conducted at the end of the three-year period. All audits are performed on-site.

Relationship between the ISO/IEC 27001:2022 standard and NIS2

There is some overlap between the ISO/IEC 27001:2022 standard and the NIS2 security measures required by the applicable Hungarian legislation in terms of organisational, personnel, physical security, and technological controls. However

- the overlap is not complete and the approaches are not necessarily identical.
- ISO/IEC 27001:2022 standard focuses on information security, whereas NIS2 compliance primarly addresses cybersecurity,
- the extent of alignment also depends on how the organisation has defined the scope of its ISMS,
- the required security level under to NIS2 further influences the degree of alignment,
- It is important to note that the ISO/IEC 27002:2022 standard, which provides practical guidance for implementing ISO/IEC 27001, is advisory, while the NIS2 security measures are mandatory legal requirements, based on the provisions of the NIST SP800-53 Revision 5 standard.

Based on the above, the degree of overlap varies between organisations. Whether an organisation with ISO 27001 certification is preparing for NIS2 compliance or vice versa, it is advisable to start with a thorough GAP analysis, since many of compliance requirements are likely already in place.

16.4. TISAX

In early July 2025, ENX published a 75-page compliance guide to support companies pursuing TISAX certification. Since ENX has has already provided a detailed analysis, this chapter only briefly notes that both TISAX and NIS2 compliance, or more precisely achieving compliance within the TISAX framework, is

Consideration	ISO 27001	NIS2
Object	Development and operation of an information security management system (ISMS)	EU-level cybersecurity compliance in critical and important sectors
Legal	International standard (voluntary, certifiable)	EU Directive (2022/2555), mandatory in all Member States
Scope of application	Industry-specific	Wide range of sectors: energy, healthcare, transport, digital, etc.
Legal basis	ISO/IEC 27001:2022	Kiberbiztonsági tv. Kormányrendelet MK rendelet NIST SP800-53r5 szabvány
Audit metodology	Voluntary, yet structured and conducted by an independent third party	Mandatory audits and regularatory reporting

Consideration	ISO 27001	NIS2
Certification	ISO 27001 certification	Certification N/A, subject to mandatory compliance requirement
Focus	Information security, minimum data protection	Cybersecurity
Affected organisations	Any organisation, regardless of size, industry or sector	Organisations falling under Section 1(1) of the Cybersecurity Act, including, among others:
Overlap	The extent of overlap varies between organisations however, whether an organisation with ISO 27001 certification is preparing for NIS2 compliance, or vice versa, it is advisable to start with a thorough GAP analysis, since many of compliance requirements are likely already in place.	

feasible and should be addressed jointly in the long term.

Trusted Information Security Assessment Exchange (TISAX) is an information security certification system established in 2017 at the initiative of the German Association of the Automotive Industry (VDA – Verband der Automobilindustrie).

The certification system was developed specifically for the automotive industry. Its main objectives are to:

- reliably assess and ensure the level of information security across companies – particularly suppliers – throughout the entire value chain,
- standardise information security requirements for stakeholders in the automotive sector,
- reduce the costs and complexity of audits,
- enable mutual recognition of audit results among industry partners.

TISAX certification is critical requirement for automotive suppliers, particularly those collaborating with German or other European manufacturers. In many cases, it is a prerequisite for conducting business within the industry.

Organisational background

TISAX is managed by the ENX Association, an independent international organisation founded in 2000. Its members include car manufacturers, suppliers, and national automotive industry associations. The mission of the association is to facilitate secure and reliable collaboration among industry stakeholders, notably in the areas of information security, prototype protection, and data privacy.

Its main responsibilities arer as follows:

- acting as an governing and supervisory body for TISAX
- developing and maintaining industry-wide standards, such as the VDA ISA questionnaire, which serves as a foundation for TISAX assessments,
- accrediting TISAX service providers,
- operating the ENX data communication network, that connects participants across the automotive industry.

Regulatory background for certification

The industry's independent standards aim to provide a „one size fits all" approach rather than customised solutions. However, the VDA and ENX are working to transform this model

by tailoring TISAX certification to meet specific demands of the automotive sector.

TISAX certification is based on the ISO/IEC 27001 standard, but it is enhanced with industry-specific information security requirements, as detailed in the VDA ISA (Information Security Assessment) questionnaire. Notably, this questionaire also complies with the NIST 800-53 rev5 framework.

Scope and objective of TISAX certification[89]

When determining the scope of a TISAX audit, the organisation's information security management system (ISMS) serves as a baseline. However, the audit scope may be narrower, provided it includes all areas of the company that process partner data and confidential information. The scope can be defined in either standard or customised format.

By specifying the audit objectives, the company defines the applicable requirements that its ISMS must meet. These requirements are entirely depend on the category of data the company processes on behalf of its partners. At the time of publication of this document, the TISAX Participant Handbook for ENX TISAX partners outlines 12 audit objectives across 3 subject areas: information security, data protection, prototype protection. Companies are required to select at least 1 audit objective, but may choose multiple objectives depending on their business needs and data processing activities.

The audit objective(s) selected by the company determine the type of audit to be conducted. According to the ENX TISAX Participant Handbook current at the time of publication, there are three possible audit types:

AL 1	Elsősorban belső célokat szolgál, lévén, hogy az auditor a kitöltött VDA ISA tábla meglétét ellenőrzi, azonban annak tartalmát nem értékeli és nem vizsgál további bizonyítékokat. Lényegében egy önértékelésnek felel meg, így alacsony bizalmi szintet élvez.
AL 2	Az auditor az önértékelés (VDA ISA) plauzibilitási ellenőrzését végzi el (az értékelési körbe tartozó összes helyszínre vonatkozóan), amit a bizonyítékok ellenőrzésével és az információbiztonságért felelős személlyel folytatott interjúval támaszt alá. Az auditor az interjút általában webkonferencián keresztül végzi, de kérésre személyesen is van rá mód. Alternatív megoldás lehet, ha a plauzibilitás ellenőrzés helyett az auditor teljes távértékelést végez. Ezt a módszert néha „2.5. értékelési szint" néven emlegetik.
AL 3	Az auditor átfogóan ellenőrzi, hogy a vállalat megfelel-e az alkalmazandó követelményeknek. Az önértékelést és a benyújtott dokumentációt használja fel az értékelés elkészítéséhez, valamint a helyszínen: • tervezett interjúkat folytat a folyamatgazdákkal; • megfigyeli a helyi körülményeket; • megfigyeli a folyamatok végrehajtását; • nem tervezett interjúkat készít a folyamatok résztvevőivel.

89 TISAX Participant Handbook

The relationship between TISAX and NIS2

There is an increasingly close relationship between TISAX and NIS2, particularly in the area of information security compliance. Both aim to strenghten cybersecurity, but they apply different approaches and operate across distinct scopes.

The connection is further reinforced by the fact that the VDA ISA framework references to the NIST SP800-53r5 standard in the TISAX implementation guidelines, the same standard on which the current Hungarian NIS2 legislation is based. Conseuqently, if a company has attained TISAX compliance in line with the NIST SP800-53r5 standard, it can also fulfil a significant portion of the NIS2 requirements, and vice versa. Nevertheless, the degree of the overlap depends on the security level the company is required to achieve under NIS2.

ENX published a separate 75-page compliance document in early July 2025 to support companies and organisations holding or seeking the TISAX label.

Criteria	TISAX	NIS2
Purpose	Assessment and certification of information security within the automotive industry	EU-level cybersecurity compliance in critical and important sectors
Legal	Not mandatory, considered as industry best practice	EU Directive (2022/2555), mandatory in all Member States
Scope of application	Automotive industry players (OEMs, suppliers, partners)	Wide range of sectors: energy, healthcare, transport, digital, etc. (listed in the NIS2 Directive)
Legal basis	ISO/IEC 27001 + VDA ISA NIST SP800-53r5 standard	Cybersecurity Act Government decree MK decree NIST SP800-53r5 standard
Audit metodology	Voluntary, yet structured and conducted by an independent third party	Mandatory audits and regulatory reporting
Certification	TISAX label	Certification N/A, subject to mandatory compliance requirement
Focus	Information security, prototype protection, data protection	Cybersecurity
Affected organisations	Mainly automotive suppliers and partners	Organisations falling under Section 1(1) of the Cybersecurity Act, including: • state and public sector actors • actors in high-risk or critical sectors of the private sector
Overlap	If a company intends to base its TISAX compliance on the NIST SP800-53r5 standard, meeting the NIS2 legal requirements provides a solid foundation for this. Nevertheless, the degree of the overlap also depends on the security level that the company is required to achieve under NIS2.	If the company has established its TISAX compliance in line with the guidelines of the NIST SP800-53r5 standard, it can also meet the substantive requirements of the NIS2. Nevertheless, the degree of the overlap also depends on the security level that the company is required to achieve under NIS2.

16.5. The relationship between the NIS2 and the GDPR

The NIS2 and the GDPR have different scopes, however, in practice they frequently overlap, particularly in relation to electronic information systems that process personal data. Harmonising the requirements of these two legal instruments is essential for lawful and secure operations. To do so, it is necessary to understand the differences that arising from their distinct objectives.

The purpose of the NIS 2 and the GDPR

The NIS2 Directive *„lays down measures to improve the functioning of the internal market by achieving a high common level of cybersecurity within the Union"*[90], while according to the domestic law implementing the Directive, declares the following: *„Protecting the confidentiality, integrity, and availability of data and information processed in electronic information systems that are essential for the state and its citizens is a societal expectation, thereby safeguarding cyberspace, which contributes to the security, resilience, and competitiveness of Hungary and the European Union."*[91]

The GDPR *„protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data."*[92]

Both pieces of legislation take a risk-based approach, requiring organisations to implement technical and organisational measures that are appropriate to their activities and associated risk factors. Although the two legal instruments pursue different objectives, they often apply to the same datasets and information systems simultaneously. In cases where uncertainty arises regarding which framework takes precedence, the GDPR, the EU's directly applicable legal instrument for the protection of personal data, prevails over any national or directive-level rules. At the same time, the objectives of both legal sources should be taken into account and their provisions harmonised, wherever feasible.

AIntersection of NIS2 and the GDPR

For organisations falling within the scope of the NIS2 Directive, compliance with both GDPR and NIS2 Directive requirements may be necessary under certain circumstances. Typical situations include:

- EISs,that also processes personal data, for example HR systems, customer databases or similar platforms.
- The organisation acts as a data controller/joint data controller/data processor under the GDPR, for instance, in relation to employee management, operation of CCTV systems or similar activities.
- Cybersecurity incidents affecting personal data processed by the organisation, for instance, data loss, ransomware attacks, or other breaches may trigger reporting obligations to the competent authorities may arise under both legal frameworks. It is therefore advisable to establish internal procedures that address the requirementsof both the GDPR and the NIS2 Direrctive.
- Cybersecurity risk assessment for EIS involving high-risk processing of personal

90 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2016/1148 (NIS 2 Directive) (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Article 1(1)

91 Cybersecurity Act, preamble [2]- Note: This translation is provided by the translator, and is not official.

92 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, „GDPR"), Article 1(2).

data[93] for example, CCTV systems for employee monitoring, GPS tracking, or similar activities, that pose a high risk to the fundamental rights and freedoms of natural persons. Data processing activities that require a data protection impact assessment (DPIA) are published on the NAIH website.[94]

As personal data are involved in the incident, the data breach shall be notified to the NAIH according to GDPR without undue delay and, if possible, no later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the fundamental rights and freedoms of natural persons.[96] For breaches that are likely to result in a high risk to the fundamental rights and freedoms of data subjects, these data subject(s) must also be informed without undue delay.[97]

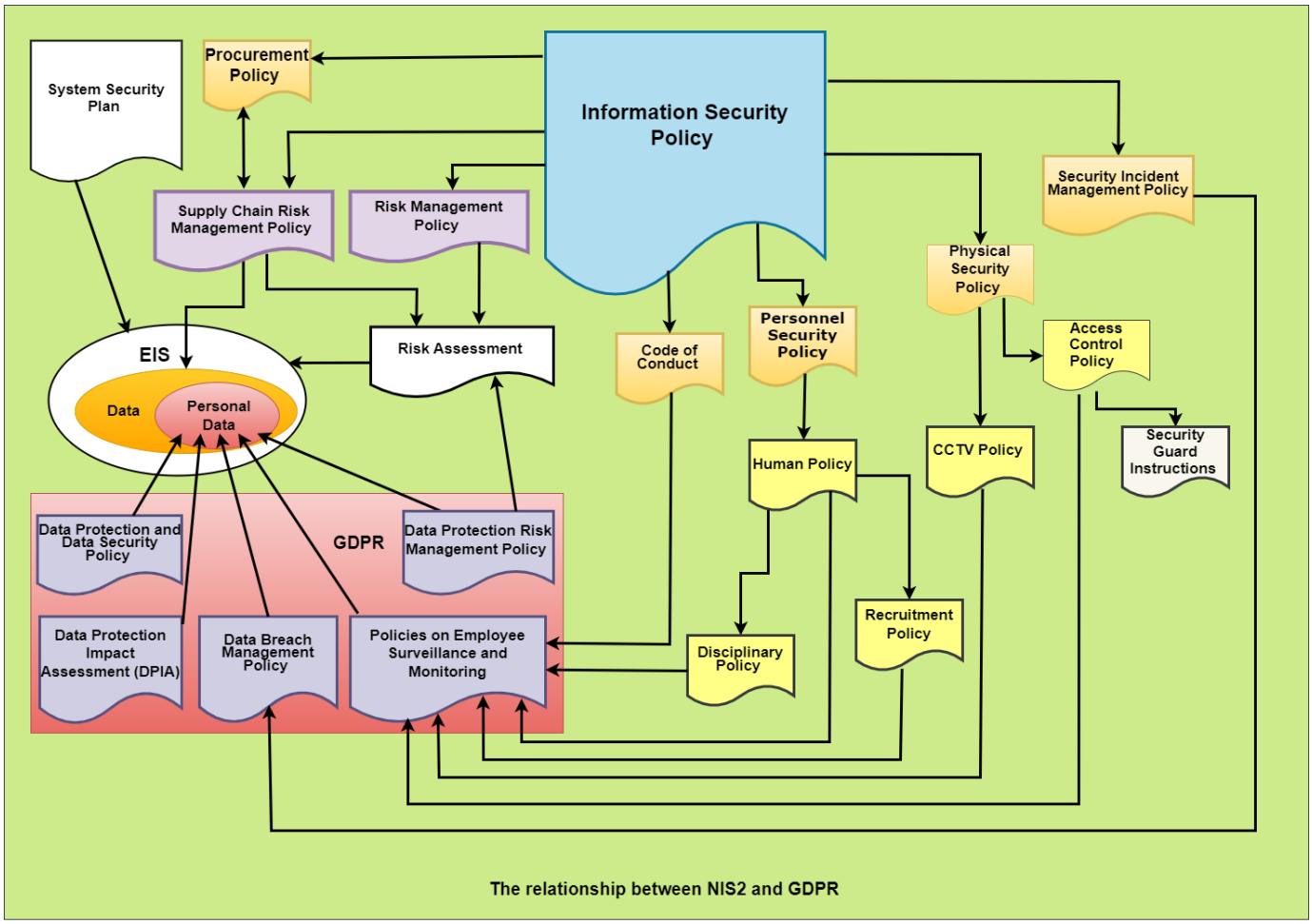


Figure 8: Links between NIS 2 and the GDPR[95]

93 GDPR Article 35(1)

94 https://naih.hu/hatasvizsgalati-lista

95 Dr. Ágota Albert, own compilation

96 GDPR Article 33(1)

97 GDPR Article 34(1).

Incident management and example of dual compliance: in the case of a company subject to NIS2 due to machine manufacturing not classified elsewhere, consider a scenario, where a ransomware attacker gains access to a server storing personal data of employees. As this case qualifies as an organisation under Section 1(1)(d) of the Cybersecurity Act, all threats, cybersecurity incident-related situations, and cyber security incidents that affecting the EIS, including operational cyber security incidents, must be reported to the National Cyber Security Incident Response Team (NCSIRT). Cybersecurity near-misses and cybersecurity incidents, including those cybersecurity incidents, which cause serious disruption or financial loss to the organisation's operations or services, or significant financial or non-financial damage to other natural or legal persons, must be reported to the national cybersecurity incident response center[98],without undue delay and in any case within 24 hours of becoming aware of the incident.[99]

Personal data as a risk factor in NIS2

NIS2 should not be regarded as a data protection regime, however:

- it stipulates that NIS2 *„respects fundamental rights and takes into account the principles recognised by the Charter of Fundamental Rights of the EU. This includes in prticular, right to respect for private life and private communications, the right to the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and the right to defense."*[100],
- it prescribes appropriate technical and organisational measures as protective safeguards,
- measures commonly known from data protection and data security compliance, such as data protection and information security policies, procedures for handling data breaches, data protection impact assessments, access management, and logging practices.

GDPR-based maturity therefore significantly facilitates compliance with the NIS2 Directive. In such cases, parallel compliance is mandatory, and can be achieved through the implementation of coordinated policies, procedures, and audits.

Conflict between NIS2 and GDPR

NIS 2 and the GDPR are not contradictory, however:

- the two frameworks pursue different objectives: the GDPR protects the rights of data subjects, while NIS2 focuses on information security
- the same events (e.g., data loss or a cybersecurity incident) are addressed from different perspectives
- organisations are subject to different expectations. For instance, while data minimisation and purpose limitation are required under the GDPR when personal data are collected, whereas logging, monitoring, and log collection are prescribed under NIS2. These measures under NIS2 may result in the technical storage of large volumes of personal data and processing

98 Act LXIX of 2024 on Cyber Security in Hungary, Section 66(2)

99 Government Decree 418/2024 (XII. 23.), Section 77(1)

100 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Recital 143

for purposes other than those for which the data were originally collected.

In real-world situations, conflicts can be resolved in the following approaches:

- coordinating information security risk assessments with data protection impact assessments (DPIA)
- developing internal policies (logging, access, data transfer, etc.) that not only comply with the mandatory protection measures set out in the MK Decree, but also incorporate the principles of the GDPR and, where applicable, the provisions of the Labour Code ([101])
- ensuring effective cooperation between the information security officer (ISO) and the data protection officer (DPO), going beyond mere formal stipulation.

Security measure in practice: employee screening and background checks

Ensuring compliance with NIS2 frequently requires conducting reliability, security, and suitability assessments („background checks") for employees, particularly prior to granting them access to significant or high-value EIS. However, the GDPR and the Hungarian Labour Code set clear limits on the purpose-bound, proportionate and lawful processing of personal data – especially regarding the collection of data on suitability, criminal records and private life (including the limitations on requesting certificates of good conduct).[102]

Example: violation of the principle of purpose limitation[103]

During a procurement project, a site visit is conducted by the procurement team. However, the participants are not documented on the attendence sheet. Consequently, movement data for that day are retrieved from the access control system to verify actual participation.

Why is this considered a violation?

- The access data was originally collected for security and access control purposes, specifically to monitor the movement of persons on the premises, not for administrative verification → Use of the data for a different purpose
- consitutes a violation of principle of purpose limitation.
- There is no legal basis for retrospectively altering the original purpose of data processing. For instance, the procurement process did not establish a valid legal basis for this secondary use, such as consent, contractual obligation, legitimate interest.
- Data subjects, including employees and visitors cannot reasonably expect that data collected for access control purpose will be used for purposes other than those for which they were originally collected, without a valid legal basis or without having been duly informed.

A more appropriate approach would have been for the organiser of the site visit to record the names of participants on an attendance sheet. In the absence of such documentation, access data could only have been used for administrative purposes, if explicitly permitted by internal rules, a valid the legal basis for processing had been established, and data subjects had been properly notitfied in accordance with the requirements of the GDPR.

101 Act LXXXVI of 2012 on the Labor Code (Mt.)

102 Act LXXXVI of 2012 on the Labor Code (Mt.) Section 11 (3)-(4)

103 „Personal data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with those purposes." GDPR Article 5(1)(b)

In what respects do the requirements of NIS2 conflict with the provisions of the GDPR regarding employee background checks?

Aspect	NIS2 (domestic implementation)	GDPR
Requirement	Only trusted persons shall be granted access to EISs[104]	Personal data may only be processed for specific purposes and on a valid legal basis (e.g. certificate of good conduct, previous employment, financial situation, etc.)
Cél	System security, reduction of human-related risks	Privacy protection and respect for human dignity
Kockázat	Failure to conduct background checks → results in system-wide vulnerability	Excessive background checks → reseults in unlawful data processing, violation of the rights and freedoms of data subjects

Table: NIS2 and GDPR considerations for employee background checks

An IT security company, citing NIS2, requests certificates of good conduct and references from the previous three employers of all new IT specialists, reviews their social media accounts, and commissions an external company to conduct a covert „trustworthiness interview." Consequences: such practices may constitute a violation of data protection laws, undermine employee trust, trigger an investigation by the National Authority for Data Protection and Freedom of Information (NAIH), and expose the company to litigation for infringement of privacy rights.

Increasing information security and data protection awareness

Both European authorities and ENISA emphasise that harmonising NIS2 and GDPR requirements represents one of the greatest challenges for organisations, particularly in the protection of critical systems that process personal data. Awareness training highlights this challenge most clearly.

Both legal frameworks require the organisation/data controller to provide training to all individuals who have access to these systems or process personal data within them. Accordingly, it is advisable to coordinate the training strategy harmonise its content, taking into account relevant risk assessments, past incidents, changes in legislation and law enforcement practices, and the expert opinions of our organisation's information security and data protection officers (CISO, ISO, DPO, etc.).

Ensuring consistency between the legal sources is not only a legal obligation, but also essential for fostering organisational trust and minimising risks.

Quantum threats in the era of NIS2

The NIS2 Directive seeks to strenghten the resilience of EU Member States against advanced classical cyber threats. However, it underestimates the revolutionary risks posed by quantum computing, which could fundamentally transform the digital security landscape in the next decade. Current regulatory frameworks – including encryption standards such as RSA and ECC, as well as incident reporting timeframes – are technologically outdated in an era where Shor's algorithm can break public key encryption within minutes,

104 Decree 7/2024 (VI.24) MK, Annex 2, Section 14.3, protective measure

Grover-optimized brute-force attacks compromise current passwords and session keys, and the convergence of quantum computing and AI, exemplified by RDSI deepfake attacks, makes reliable authentication of digital content effectively unattainable. As the DARPA Quantum Shield Program noted in 2025: „The shortcomings of NIS2 are not technological limitations, but strategic blind spots."

The risk of quantum-enabled attacks is already tangible, and several gaps exist in the NIS2 Directive. For example, SSH-Q (sub-second Secure Shell hijacking) exploits the lack of real-time detection, allowing administrative VPNs to be compromised in just 15 seconds without leaving a trace. CAQI (certificate authority quantum impersonation) enables attackers to take over state domains using fraudulent eIDAS certificates exploiting outdated RSA/ECC requirements. QCC (quantum chain collapse) exploits the absence of blockchain integrity protection and could cause losses of up to €14.2 billion in central bank digital currencies by 2030.

The proposed regulatory update addresses three key areas. First, post-quantum cryptography (PQC) must be made mandatory. In this context, the annexes to NIS2 should specify algorithms such as CRYSTALS-Dilithium or Kyber-1024, following the example of the EU's eIDAS 2.1 regulation, which will prohibit the use of RSA-2048 from 2027. Second, quantum-sensitive incident reporting should be introduced, leveraging sub-second anomaly detection, such as entropy drop patterns, instead of the current 24/72 hour-reporting deadlines. Third, quantum assurance of the supply chain is necessary, which would require key Tier1 suppliers employ HSM devices capable of supporting PQC algorithms.

Failure to take timely action could result in severe economic consequences in the short term (2025–2027). ENISA estimates the potential losses of €23.4 billion could be avoided, including digital currency theft resulting from QCC attacks, fraudulent SWIFT transactions resulting from CAQI-type certificate forgeries, and losses of up to €920 million in 2026 due to RDSI deepfake fraud. In the longer term (2028–2030), there is a growing threat of systemic risks, including energy grid blackouts caused by quantum time manipulation (TQNI), which could result in €49 billion in damage per day, or widespread illegal border crossings enabled by biometric forgery (BQSA). Moreover, the legal consequences would be significant: under such conditions NIS2 fines would loose effectiveness, as attackers remain undetectable. As the EU Cyber Council stated in 2026: „Quantum attacks leave no trace – only damage."

The recommended strategic measures should be implemented across three time frames. In the short term (2024–2026), critical infrastructures should complete migration to post-quantum cyriptography (PQC) and organisations subject to NIS2 should implement quantum Red Team exercises. In the medium term (2027–2029), it is advisable to introduce quantum-resistant certificates—such as SPHINCS+ or FALCON-1024— and to enhance Five Eyes-type cooperation for the sharing quantum attack benchmarks. In the long term (from 2030 onward), organisations should ensure cryptographic agility, including the ability tho switch algorithm within 24 hours, and deploy quantum-aware SIEM systems capable of Grover-resistant anomaly detection.

Quantum threats are not speculative: they represent real capabilities currently being developed by state actors. Updating NIS2 is therefore not optinal, it is a matter of survival. Delaying decisive measures risks both significant financial damage and strategic disruption within the digital ecosystem.

17

Communication with management

The NIS2 Directive and the corresponding national implementing rules impose oblligations that go beyond purely technical or legal requirements, encompassing resource-intensive strategic tasks. However, NIS2 Directive is not merely a set of IT duties; it also covers areas such as business continuity and legal risk management. For this reason, management support is crucial in areas not only for securing budgets and approving organisational changes, but also for making informed decisions on r sensitive issues, such as background checks and monitoring, even cxyíwhen these are not strictly mandated by law.

17. Communication with management

Written by: Dr. Ágota Albert,
György Attila Kovács

17.1. Key messages and talking poins for management

The basis for the successful implementation of any project is regular, accurate, and transparent communication with management, not only to share information but also to enable well-founded decisions regarding the allocation of financial, human, and organisational resources. Tasks and requirements must be presented in a clear, non-technical language, as decision-makers may not have an IT background. ENISA highlights that management is „*responsible for approving cybersecurity measurest*[105]*, and must undergo cybersecurity training"* [106].

The question arises as how and what should be communicated to management. Simply stating *„as an organisation is subject to NIS2, appropriate and proportionate technical, operational, and organisational measures must be implemented to manage the risks to the security of the network and information systems used for operations or to provide services, and to prevent or mitigate the impact of incidents on customers or other services"* may not be well received, and the „tell the truth[107] and run" approach is unlikely to appropriate in this context.

Communications with management should be framed in terms of „business" and „risk." Management is typically not focused on technical details such as firewall configuration, but with risks to business continuity, potential consequences of non-compliance with NIS2 requirements and the associated financial and reputational damage. It is crucial not only to present only the challenges, such as costs of implementation, but also the benefits. For example, „NIS2 compliance strenghten the organisation's resilience to cyberattacks, helping to provide continuity of operations even in the event of incident". To support effective communication, consider structuring discussions around the following three questions:

- What is the problem?
- What are the consequences?
- How can the damage be mitgated?

Priorities should be presented clearly and selectively, without overwhelming management with every detail at once. It is advisable to categorise them by urgency and impact. For example, short-term priorities (e.g., legal deadlines, upcoming audits, required regulatory preparations), medium-term priorities (e.g.,

105 See, for example: Act LXIX of 2024 on Cyber Security in Hungary. Sections 6, 8, 10(2)

106 ENISA: MAPPING NIS 2 OBLIGATIONS TO ECSF June 2025, doi: 10.2824/8870995.

107 e.g.: Pursuant to Section 30(3) of the Cybersecurity Act, if „the head of the organisation fails to comply with the obligations laid down in the legislation, the national cyber security authority may, after considering all the circumstances of the case, impose a fine in the amount specified in a government decree, and shall impose a fine in the event of a repeated infringement." and, where appropriate, pursuant to paragraph (6)(b), „may initiate proceedings before the commercial court for the temporary disqualification of the head of the basic organisation from performing his or her duties as a senior officer in that organisation."

improvements that reduce costs or support future audits) and long-term priorities (e.g., fostering and maintaining of cybersecurity awareness).

Communication should be clear, focused and supported with quantifiable data whereever possible. such as the estimated cost of audit, the financial impact of a day's lost production, potential business consequences of non-compliance (e.g., fallout from a ransomware attack), and the amount of any imposed fines.

Senior management relies on the information provided to determine next steps and allocate necessary resources. It is therefore crucial to present objective, evidence-based insights into any issues that arise. In most cases, the responsible person for compliance will be expected to propose actionable solutions. Offering mutiple options not only encourages management to actively engage with the issue, but also fosters a sense of ownership in the decision-making process and strenghten their awareness of accountability. Accordingly, it should be clarify from the outset that NIS2 is both time-consuming and resource-intensive, requiring sustained commitment across the organisation.

17.2. Reporting options

The project manager must provide senior management with concise updates, at a frequency that alignes with the company's organisational culture (weekly, biweekly, or most monthly), regarding the status of preparations and any new issues requiring senior management's support, such as key risk management, tasks related to upcoming deadlines, and measures that have been implemented and planned.

In the event of an incident, rapid reporting to senior management may be necessary. In such cases, it is recommended to present a succint summary that summarises what occured, the potential impact on business operations and organisational reputation, what recommended immediate measures, expected recovery time, and any reporting obligations under cybersecurity and data breach protocols.

Reporting on the NIS2 audit also be well-structured. Before presenting the audit findings, it is advisable highlight the expected obligations and any identified shortcomings, followed by the executive summary on the audit findings and recommended corrective actions.

17.3. Major cost elements

When planning the budget, two cost items are prescribed by law: the annual cybersecurity fee and the maximum fee for the cybersecurity audit.[108]

In contrast, the cost of implementing NIS2 requirements depends on several factors, notably the size of the organisation, the number of employees involved in the implementation, the fees of external consultants, and the procurement ofIT tools required to address deficiencies identified in the GAP analysis. Accordingly, the implementation costs must be determined on a cas-by-case basis for each organisation.

17.4. An obligation, not a choice – Management responsibilites and challenges

It must be clearly communicated to management that NIS2 compliance is mandatory for the organisation. The obligation is comparable to complying with applicable tax laws or

108 For the annual supervisory fee, see 2/2025. (I. 31.) SZTFH decree on the cyber security supervisory fee. The audit fee can be calculated based on Annex 3 of the SZTFH decree on the rules for conducting cyber security audits and the maximum fee for cyber security audits.

occupational safety regulations, it it not optional and there is no alternative.

The specfic tasks the organisation must undertake can be identified through an in-depth GAP analysis of the requirements set out in two relevant pieces of legislation[109] megfogalmazott követelmények részletes GAP elemzését követően tudjuk meghatározni.

Depending on the outcome of the GAP analysis, the necessary measures may include the adoption of new internal regulations, the amendment of existing regulations and procedures, as well as the acquisition of new IT hardware and software tools. The exact scope of these measures will largely depend on the organisation's current level of information security preparedness.

Common objections and recommended responses:

- „This will never happen to us" – This is a common misconception, but statistics consistently show that cyber incidents affect organisations of all sizes across all sectors. There are no exceptions — every organisation faces cybersecurity risks.
- „The organisation doesn't have the money for it" – While budget constraints are a reality, it's important to highlight the potential financial impact of inaction. Highlight recent ransomware attacks as case studies, showing the full financial impact of such incidents — from immediate financial losses and reputational damage to regulatory fines and penalties.
- Non-compliance is far more expensive. Under NIS2, fines can reach up to €10 million or 2% of global annual turnover (whichever is higher).
- „Then let's avoid documenting anything" – it is important to emphasise that documentation is essential. Both auditors and regulatory authorities always request documentation first. Well-maintained records of policies, procedures, and implemented measures are key for demonstrating compliance and facilitating audits or investigations. Without proper documentation, the organisation cannot prove evidence of compliance, which can significantly increases the risk of higher fines or additional scrutiny

. In general, if an organisation already holds an information security certification (e.g., ISO27001, TISAX), the number of addititonal policies and procedures required for NIS2 compliance may be around twenty. In contrast, for organisations without prior experience in information security, the number of obligatory documents can easily exceed fifty.

The preparation of these documents, as well as the procurement and implementation of necessary IT solutions, demands meaningful resources. From the outset, management must acknowledge that NIS2 compliance is a demanding, time-consuming, and costly effort.

If it is necessary to explain the tasks assigned to the organisation at an international level, the NIS2 technical implementation guide published by ENISA can be a valuable resource, particularly its „mapping table" versiona[110].

109 These are the following legal acts: :
1. Decree No. 7/2024 (VI. 24.) MK on the requirements for classification into security classes and the specific protective measures applicable to each security class.
2. SZTFH Decree No. 2/2025 (I. 31.) on the procedure for conducting cybersecurity audits and the maximum fee for cybersecurity audits, as set out in Annex 7.

110 ENISA: NIS 2 Technical Implementation Guidance és Technical Implementation Guidance Mapping table. June 26, 2025.

18

Understanding and communicating

Contrary to popular belief, information security is not solely a technical issue; it is a fundamental aspect of an organisational culture and daily operations. In accordance with the MK Decree and the NIS2 Directive, organisations are obliged to ensure that security requirements are embedded not only in internal policies, procedures and other formal documentation, but also in day-to-day practices. To support this, the establishment of internal coordination working groups and regular, targeted information and training for users is required.

This chapter outlines the role of internal working groups within the organisation in managing information security and details the measures implemented to promote security-aware user behaviour, including training programmes, communication channels, and feedback mechanisms.

18. Understanding and communicating

Written by: Dr. Ágota Albert,
György Attila Kovács

18.1. Internal working groups and user involvement

Project launch and management commitment

For an organisation subject to NIS2, an initial and most critical step is to involve the company owner or senior management. As with traditional certification frameworks, management commitment is vital for NIS2 compliance, particularly for securing the required resources and overseeing the successful implementation of all necessary measures.

Internal working group structure and selection of members

Once management support has been confirmed, the next step is to appoint a project manager capable of leading the preparation process. Taking into account the organisation's structure, it is also indispensable to identify the relevant departments or organisational units whose representatives should be included in the project team responsible for coordinating and implementing the compliance activities. In line with the mandatory security measures under the MK Decree, the following strategic areas are recommended for contribution subject to organisational structure and terminology:

- IT
- Physical security
- Information Security Officer (ISO) and Data Protection Officer (DPO),
- HR (organisational unit responsible for personnel/labour relations),
- Education, training (or relevant organisational unit responsible),
- Procurement
- Quality assurance,
- Facility management,
- Legal/compliance team,
- EIS owners or their representatives,
- Representatives of contractual partners involved in EIS operations,
- Representatives of contractual partners performing information security-related tasks (e.g., SOC service providers)

Depending on the internal dynamics of the organisation, it may also be beneficial to engage stakeholders who can influence long-term decisions and policy-making, such as informal opinion leaders or representatives of the Works Council.

It is essential to inform with the immediate supervisors of the experts selected for the project in advance, as participation may require a significant time commitment and adjustments to their regular duties.

Addititonally, it should also be determined which external resources may need to be engaged if the necessary expertise is not available in-house. For organisations that already hold an information security certification (e.g., ISO/IEC 27001:2022, TISAX), experience gained during the implementation of those systems can serve as a useful reference point when

evaluating whether external consultancy is required.

For organisations lacking prior experience with informamtion security management or audit preparation, the engagement an external consultant with proven expertise and relevant experience is strongly recommended to support effective and compliant implementation.

What questions might arise during the initial steps?

- Which representatives from which areas of expertise can be involved in specific decisions? It is recommended to create a stakeholder matrix, drawing on organisational and operational rules, the EISs' system security plans, and internal policies and procedures.
- Who should serve as a project manager? Ideally, the project manager should have project management experience, a comprehensive understanding of the organisation's structure both horizontally and vertically, and at least general familiarity with the national legislation implementing NIS2. While the information security officer (ISO) is often a suitable choice, other arrangements are also possible.
- How often should the project team meet and how should tasks and responsibilities be allocated?
- What type of action plan/action list should the project team prepare and how detailed should it be?

The best practice is to establish a framework where project team members provide updates on the progress of their assigned tasks during weekly project status meetings. Regular agenda items should include discussions of emerging issues and challenges as well as the addition of new tasks to the action list. To facilitate this process, the following questions should be considered to identify the tasks to be completed throughout the project:

- Project Plan Structure: How should the project plan be structured? What phases can be identified based on the tasks to be performed?
- Support Tools: What support tools should be used? For example, a project charter, a task tracking template (e.g., Gantt chart), internal communication protocols within the project team (ticketing/scheduling tool), etc.
- Gap analysis and roadmap: Who is responsible for performing the gap analysis and in which areas? How should a roadmap or action plans be developed? Who is entitled to define the related milestones, and what should be prioritised?
- Risk assessments: Are the necessary risk assessments in place for both EISs and the supply chain? If gaps exist, who should be involved to address them?
- Policies and procecdures: Who is responsible for updating specific policies and procedures regarding security measures, and who coordinates these updates?
- Employee training: How will employees be trained and how will information security knowledge be maintained up to date?

In this context, the role of the project manager goes beyond motivating the representatives from various fields; but also encompasses fostering effective dialogue to ensure that the preparations carried out efficiently and on schedule. The overarching objective is to establish an information security environment that not only meets expectations but is also practical and sustainable for the organisation.

The project manager is expected provide senior management with concise updates on the status of preparations and on any new issues

requiring their support. The frequency of these updates should reflect the organisational culture (weekly, biweekly, or at most monthly), while adhering to the principle of necessity and sufficiency.

Throughout the project, it is particularly important to apply a risk-proportionate approach, consistent with the legal environment. To achieve this, risks related to systems and services must be taken into account when setting timelines for individual tasks and phases, and especially when prioritising actions following the GAP analysis.

Cooperation is crucial not only during the project, but also in the long term and exceptional circumstances. Therefore, particular attention should be given to security measures that depend on collaboration across different areas of expertise, especially, business continuity, incident management and organisational communication.

18.2. Internal cooperation and organisational unit engagement

The project team, given responsibility for ensuring compliance with the legal framework will be expected to develop a comprehensive set of internal regulations. Some of these are entirely new elements to the organisation, while others will demand substantial updates to the current regulatory framework.

Many of the protective measures will also impact employees and external partners who are either involved in their implementation or have access to EISs. Accordingly, during the preparation phase, the project team must also consider areas that extend beyond the traditional scope of cybersecurity and information security.

Role, information and involvement of organisational units

The roles and responsibilities of each organisational unit should be clearly defined, with particular emphasis on their role in implementing protective measures, their level of access to EISs, and the level of risk associated with their activitities.

Key operational functions and and responsibilities (non-exhaustive list):

- Human resources management: responsible for integrating protective measures throughout the employee lifecycle, including recruitment, termination and internal transfers (e.g., background checks, exit interviews), Tasks also include drafting job descriptions, managing access and confidentiality agreements, conflict of interest declarations, organising basic and advanced security awareness training, and coordinating or conducting disciplinary proceedings, among others.
- Legal team: drafts and reviews contracts to ensure compliance with security-related measures, with respect to confidentiality agreements, basic requirements for subcontractors.
- Data protection officer (DPO): oversees and supervises data processing agreements, joint data processing and data sharing agreements, ensures that international data transfers comply witth data protection, data security and information security requirements. The DPO also responsible for managing data breach notifications.
- Procurement: enforces the integration of information security requirements within procurement processes and ensures their proper inclusion in contracts, tenders and technical specifications.

- Security services: coordinates physical security systems, informs relevant stakeholders about protective measures and ensures their consistent and effective enforcement.

Organisational units must implement security measures not only during normal business operations, but also in critical situations, such as cybersecurity incidents and data breaches (e.g., preparing response plans, investigating incidents, conducting risk analysis, executing measures outlined in the response plan, etc.), as well as address business continuity challenges that require timely resolution.

When coordinating the activities of organisational units, potential conflicts of interest must also be taken into account. For improved clarity and easier oversight, it is advisable to prepare flowcharts and responsibility frameworks, such as RACI matrices.

Risk-based action plans, up-to-date organisational and operational rules, and internal procedures, protocols and guidelines tailored to daily operations, can effectively support the review and management of tasks assigned to each organisational unit.

18.3. Role, information and involvement of users

During the preparation phase, it is essential to identify which of the protective measures must be understood by all employees of the organisation. These rules, or relevant excerpts from policies and procedures should be communicated effectively, and training should be delivered in a structured and planned manner, aligned with the organisation's established training processes. Beyond formal training designed to raise awareness and familiarise employees with the requirements, local communication channels can be employed to ensure the necessary information reaches everyone. Examples entail internal circulars, awareness posters, and dedicated intranet pages. This information should be tailored to the characteristics of the target audience, considering literacy levels, internet proficiency and familiarity with EIS terminology.

To ensure the effectiveness of security awareness training, users' prior knowledge should be assessed, and the knowledge gained should be monitored. For instance, a brief assessment conducted after the training can help verify that the information retention and evaluate its impact.

A variety of targeted tools are available to raise awareness and improve understanding of information security, internal rules and regulations. Therefore, it is worth considering e-learning or blended learning options, which enable scalable delivery of information while requiring fewer resources.

It is also essential to maintain up-to-date, auditable records of the training courses conducted, the information provided to participants, and the content and methods of knowledge transfer. Consequently, it is advisable to select a solution that encompasses not only preparation and delivery, but also monitoring and documentation.

In addition to general cybersecurity knowledge, employees should be particularly familiar with organisational internal measures, access agreements, codes of conduct outlined in regulations, confidentiality agreements, and their related disciplinary responsibilities.

Overall, attention should be given to the folloiwing areas:

- Role-based security awareness training should be developed. The primary prerequisite for this is the formal definition of each role within the organisation 's internal rules. At a minimum, it is recommended to distinguish between managers, users, IT operations staff, and physical security

personnel, taking into account their respective responsibilites.

- The content of each training programme should reflect the responsibilities and risk exposure associated with the given role. For example, managers should be aware of the decision-making responsibilities delegated by internal directives regarding information security and be able to recognise indicators of common threats, such as business e-mail compromise (BEC attacks). Personnel responsible for physical security should be familiar with the security zones and able to identify indicators of tailgating, or other forms of unauthorised access.
- Internal rules and procedures must be properly established, and made accesible to all relevant stakeholders.
- All rules must be implemented in a way that allows for demonstrable compliance.
- Data subjects must be transparently informed about the processing of their personal data such as logging, monitoring checks.

If data processors, joint controllers or their representatives have access to the EISs and the personal data stored therein, such access must be regulated by agreements that fully comply with the provisions of the GDPR.

External partners may be granted access to the organisation's systems. In such cases, it must be documented in writing how, for what purpose and to what extent access is granted to the relevant system (referred to as an „access agreement"). Such users may include external information secrity officer (ISO), data protectiton officers (DPO), auditors, lawyers, and other experts. These users should be made aware of the relevant codes of conduct, and their compliance with these rules should be formally ensured through contractual or procedural measures.

To develop an effective framework focused on security awareness, it is advisable to consider the provisions of Chapter 20 of this Whitepaper.

19

„Quick Win” list

Achieving successful compliance requires a comprehensive organisational approach, underpinned by active management commitment, expert guidance, and structured project management.

19. „Quick Win" list

Written by: Márk Máté

Active involvement of senior management and cross-functional cooperation

One of the most significant innovations introduced by the NIS2 Directive is the direct accountability of senior management. Under Article 20, senior management must approve and supervise the implementation of cybersecurity measures. This constitutes a fundamental shift, as cybersecurity respnsibilities can no longer be delegated solely to the IT department.

Meeting these obligations requires collaboration among the compliance, IT, and legal departments. Effective implementation depends on close interdisciplinary cooperation, including regular consultations among key stakeholders, clearly defined responsibilities and reporting lines, and the promotion of cybersecurity awareness at all organisational levels. As part of an integrated approach, organisations should foster the alignment of legal, IT, and business functions, establish coherent governance frameworks, and develop consistent incident management procedures to ensure proper compliance.

- Appointment of a dedicated responsible person: The appointment of a Chief Information Security Officer (CISO) or other dedicated cybersecurity officer is crucial. Pursuant to Section 6(3)(2) of the Hungarian Cybersecurity Act, the head of the organisation shall „appoint or designate a person responsible for the security of electronic information systems...". This function also may be undertaken by an external expert.
- Consulting support and training: Engaging experienced consultants may play a decisive role in accelerating compliance efforts. Consultants can assist in assessing the current maturity level, conducting gap analysis, and setting implementation priorities. They may also provide support in developing the project plans, selecting appropriate technical solutions, and designing effective processes.
- Establishing administrative, physical, and technical control environment: The NIS2 Directive requires an „all-hazards" approach, which requires multi-layered protection. Administrative controls include the development of policies and the definition of roles and responsibilities. Physical controls cover facility protection, access management, and environmental security measures. Technical controls include network protection, encryption, monitoring and logging systems.
- Integration of existing certification(s), if any: Holding relevant certification(s), such as ISO/IEC 27001:2022, provides a significant advantage in achieving compliance, as there are substantial overlaps between the respective requirements.
- Remediation milestones: A structured and phased implementation process is essential to achieve and maintain robust compliance.
    - Preparatory phase: securing management commitment, establishing

the project team, and assessing the current state.
- Planning phase: conducting a detailed gap analysis, developing a remediation plan, and allocating resources.
- Implementation phase: introducting technical solutions, developing processes, and delivering training.
- Testing and fine-tuning phase applying incident management practices, conducting internal audits, and driving continuous improvements.

Progress is monitored using objective indicators such as the number of controls implemented, the percentage of participants completing training, incident response times, and audit results.

- Pre-audit and compliance checks: Regular internal audits ensure ongoing compliance. Audit areas include the effectiveness of technical controls, adherence to estabilshed processes, documentation compliance, and the impact of training programs. Independent third-party assessment provides an objective evaluation of the organisation's preparedness. These assesssments validate the compliance status, identify opportunities for further improvement, and assess audit preparedness.

Achieving compliance is a complex yet well-structured process that can be effectively implemented by following the Quick Wins outlined above. Success depends on management commitment, the engagement of appropriate expertise, and fostering the culture of continuous improvement.

20

Sanctions and remedies

Violation of the NIS2 Directive and related national legislation not only increases cybersecurity risks but can also lead to legal and financial consequences. Sanctions are designed to enforce compliance, promote effective incident management, and strengthen the security of network and information systems. When making decisions, the competent authority takes into account the severity and recurrence of the infringement, as well as the organisation's cooperation and responsiveness, ensuring that the measures are proportionate. Consequently, the sanctions serve not only as a deterrent, but also as an incentive for organisations and auditors to regard compliance as a continuous, strategic responsibility.

20. Sanctions and remedies

Written by: Gabriella Biró, Árpád Robotka

20.1. Legal consequences for the organisation and its executives

If the organisation fails to comply with the security requirements and procedural rules established by law, or a cybersecurity authority of an EU Member State submits a request to Hungary under the framework of mutual assistance, the cybersecurity authority may impose legal consequences on the affected organisation. Such legal consequences may include corrective measures or financial penalties (fines).

The cybersecurity authority has the power to apply the following measures:

- issue a warning to the affected organisation to comply with the applicable security requirements and procedural rules;
- order the affected organisation to remedy identified security deficiencies, implement all necessary measures to ensure compliance, and fulfil its reporting and data disclosure obligations within a specified timeframe;
- require the affected organisation to cease the infringing conduct, implement immediate corrective actions, and where applicable, propose disciplinary measures to the employer;
- refer the matter to the affected organisation's supervisory body or the owner exercising oversight rights and request their cooperation;
- appoint an information security supervisor at the expense of the affected organisation.

If the organisation fails to comply with the cybersecurity requirements despite the measures imposed, the competent authority, having regard to all relevant circumstances, may impose a fine on both the organisation and its management.

The maximum amount of the fine that may be imposed is:

- for a basic organisation, the the higher of EUR 10 million (in HUF) or 2% of global turnover in the previous year;
- for an important organisation, the higher of the higher of EUR 7 million (in Hungarian forints) or 1.4% of its global turnover in the previous year;
- for the head of the organisation: a personal fine of HUF 15 million.

Furthermore, the cybersecurity authority may take the following measures:

- require the affected organisation to disclose the fact and circumstances of the violation;
- order the organisation to inform its service users about potential threats;
- publish information on its website in the event of a cybersecurity incident, or require the organisation to disclose relevant information by formal decision;
- oblige the organisation to notify the cybersecurity authority if crisis management or emergency response measures become necessary;
- for essential organisations that are not public administration bodies, initiate the

temporary suspension of the organisation's certification or license with the competent authority, and request the temporary disqualification of the head of the organisation's executive from performing senior official duties through the commercial court;
- if the organisation fails to comply with an official obligation or to implement the prescribed protective measures, resulting in a cybersecurity incident or near-incident, require the organisation to cover all costs incurred in the response.

In addition to the above, the SZTFH, acting as a cybersecurity authority:
- is entitled to prohibit the affected organisation from engaging in activities that would directly jeopardises compliance with security requirements;
- shall notify the competent supervisory authority of the fine and the underlying facts in the event that a fine is imposed.

20.2. Legal consequences for the auditor

If the auditor fails to comply with the cybersecurity requirements established by law, or the related procedural rules, the SZTFH shall be entitled to take the following measures:
- warn the auditor to comply with the applicable legal provisions and procedural rules;
- set a deadline for the adoption of necessary measures to achieve compliance;
- temporarily suspend the auditor from performing audit activities.

If, despite these measures, the auditor continues to fail in fulfiling its legal obligations, SZTFH may, having considered all relevant circumstances, impose a fine, which may be re-imposed in the event of continued non-compliance.

Where the SZTFH identifies a violation in connection with the auditor's activities that affects the audited organisation, it shall notify the organisation's information security officer (ISO).

20.3. Imposition of legal santctions

The cybersecurity authority may apply multiple legal consequences, having regard to the following circumstances:
- the severity of the deficiency or omission
- the duration of the infringement
- whether a significant or large-scale cybersecurity incident occurred or was imminent
- the impact of the incident had or could have had on the affected organisation or other organisations
- any financial or non-financial damage
- whether the incident unique or recurring
- any relevant previous breaches by the affected organisation
- whether the incident was intentional or negligent
- the conduct of the affected organisation, the measures adopted to prevent or mitigate the damage
- compliance with approved codes of conduct or approved certification mechanisms
- the level of cooperation with the competent authorities
- the effectiveness, proportionality and deterrent effect of the intended legal consequences.

The following shall be considered serious infringements:
- repeated infringements;

- failure to report or remedy significant events (incidents);
- failure to correct identified deficiencies despite instructions from the competent authorities;
- obstruction of inspection activities;
- provision of false or materially inaccurate information.

20.4. Legal remedy

No appeal may be lodged against a decision of the cybersecurity authority. However, an administrative action may be initiated against the final decision in accordance with the provisions of Act CL of 2016 on the Code of General Administrative Procedure.

This means that, although the decision of the cybersecurity authority cannot be challenged by a direct appeal, affected parties may seek judicial review of the decision through administrative proceedings.

21

Security culture and awarenes

While the NIS2 Directive only refers only to „basic cyber hygiene practices and cybersecurity training” and requires management-level training at a theoretical level, without specifing the number of hours, roles or format, the Hungarian implementation (Cybersecurity Act, MK Decree, 17/2025 EM Decree, etc.) takes a more detailed approach. It defines specific training requirements by role and duration and strictly regulates the content, frequency, documentation, and official supervision of the training. Although the tightening of legal requirements, and the specification of concrete training hours is a forward-thinking step, it is crucial to recognise that cybersecurity awareness - as a behavioural change - can not be fully achieved through regulatory measures alone.

©2025 Sólyom Ákos

21. Security culture and awareness

Written by Ákos Solymos

General safety awareness

The world is rapidly evolving toward a reality in which an increasing number of tasks are performed by automated entities, whether referred to as robots, chatbots or digital assistants. Nevertheless, at the end of every process or decision, it is still a human being whose level of awareness ultimately determines the outcome. This awareness extends multitple domains and has a far-reaching impact. Environmental awareness is concerned with the protection of nature and the environment. Conscious education aims to prepare children to become responsible, thoughtful adults. Safety awareness, in turn, encompasses to behaviours aimed at sefeguarding specific values, such as health, data and physical assets.

Safety awareness can originate from various sources: family upbringing, learned behaviours, intergenerational influences. It may also be shaped by immediate environment, such as the workplace or broader community. In many cases, a single incident, - such as data loss, or an uncomfortable situation- can act as a catalyst for individuals or even entire organisations to reassess and adapt their behaviour (as the Hungarian saying goes:Mohács is needed). Introducing security awareness at an early stage of education, would lay a strong foundation for the development of other forms of conscious behaviour. However, a detailed exploration of educational aspects falls outside the scope of this document.

It is generally observed that when individuals already posess a basic level of security-conscious thinking and behaviour, organisational security rules are more easily understood, internalised and accepted. Such individuals are also less likely to circumvent controls or disregard protective measures.

It is essential to distinguish between teaching security rules and raising security awareness. The terminology used in relevant legislation deliberately emphasises awareness raising, reflecting the recognition that the objective is not merely to transmit information, but to foster lasting behavioural change.

Practical aspects

This chapter outlines best practices designed to support organisations in both achieving regulatory compliance, and fostering sustainable, long-term changes in mindset.

Safety awareness should be core component of both the organisational andthe overall safety culture. While establishing such a culture initially requires significant investment of time and resources, it ultimately functions like a flywheel in a small vehicle: once set in motion, it keeps moving forward with little additional input, and periodic reinforcement becomes far more efficient than restarting the process.

When safety rules, practices, regular testing, and preparation are embedded in daily operations, users begin to perceive them as routine. In such an environment, new employees can adapt more rapidly and integrate seamlessly into this „flywheel” of awareness and compliance.

Moving beyond the one-size-fits-all approach of annual training sessions, the current legislative framework requires a more sophisticated, structured, regulated, and measurable approach to both awareness and training. While specific legal references are not included in this section due to space constraints,

it is important to emphasise the shift toward a more comprehensive and accountable system.

To exceed minimum compliance, both training and safety awareness should be evaluated from multiple perspectives—such as content, delivery methods, frequency, user engagement, and impact assessment.

In the long term, it is recommended that safety awareness activities be treated as a distinct from the formal communication of organisational safety policies and procedures, recognising their unique role in shaping behaviours and fostering a proactive security culture.

Time frame

When considering security training from a time horizon perspective, it is useful to distinguish between employee training and annual refresher training required by law. The most rigorous and secure approach is to restrict new users from IT systems access until they have succesfully completed the required onboarding security training.

A less strict, but inherently riskier method involves grouping new employees for monthly in-person basic security training. While this is more manageable from a logistical standpoint, it introduces delays between the onboarding date and the actual training session, thereby increasing the period during which new users may operate without adequate security awareness. The riskiest approach, short of omitting refresher training altogether, is to grant new employees immediate access and requirer them to attend the next scheduled annual refresher session alongside more experienced staff. This presents a significant security risk: if an employee joins just after the annual refresher, up to 11 months may pass before any formal security training is received by the employees.

During this extended period, the employees are likely to rely on informal guidance from colleagues and personal judgment, which may be inconsistent with official security policies. By the time they finally attend training, incorrect practices and misunderstandings may already be ingrained - making them more difficult to correct. In the worst-case scenario, this gap can increase the likelihood of cybersecurity incidents and make it more challenging for the employee to accept and internalise the expected behaviours and procedures.

Training methods

The choice of traing methods largely depends on available resources and management's attitude. Historically, classroom-style instruction was the norm, where such training was offered at all. However, given the varying levels of user receptivity, this approch is often ineffective. Moreover, HR departments freqently seek to optimise workforce allocation by consolidating multiple training topics into a single „training day", when employees attend back-to-back lectures, covering a wide range of subjects, including safety. Such intensive sessions typically result in a steep learning curve, and participants often struggle to retain information from the lectures, even horus later. The effectiveness of these sessions can also vary depending on factors such as the presenter, the topic, the time of day, as well as the audience level of fatigue, and cognitive overload. Additionally, it is nearly impossible to remove the entire organisation from its operational processes for a full day, which further limits the feasibility of this approach.

A more effective approach is e-learning. Although it requires a greater initial investment, such as operating an LMS (Learning Management System) and developing, commissioning, or customising teaching content, it offers considerable advantages. Users can progress at their own pace, while knowledge acqusition and learning outcomes can be tracked and assessed through exams. Language barriers pose fewer obstacles, and importantly, e-learning is accessible and can be automated regardless of time or location. When the LMS utilises a sufficiently large and diverse question bank, the risk of cheating or

collaborative testing during exams or knowledge assessments is significantly reduced.

The most effective security awareness campaigns are those that, despite competing with other internal communications, organisational priorities, and training materials, cover a broad range of topics and create a lasting impact. These campaigns should aim not only to convey information but also to provide opportunities for users to apply their knowledge in practice, for example, through social engineering exercises, lockpicking demonstrations or security-themed escape rooms. Effective campaign planning should begin up to six months in advance, allowing sufficient time for coordination and content development. Their impact can be significantly enhanced through gamification, competitions, and incentive-based elements such as prizes, all of which help to increase user engagement and improve knowledge retention.

It is also advisable to incorporate realistic simulations into these initiatives—controlled attack scenarios that allow users to respond to threats in a safe and structured environment. Such simulations serve as valuable tools for evaluating the effectiveness of training and awareness efforts.

However, awareness activities, should not need to be limited to periodic campaigns alone. They can - and ideally should - be embedded throughout the year. Regular intranet articles, presentations at company events, and interactive workshops can help keep security top-of-mind for employees on an ongoing basis.

Organisations may opt to develop their own security awareness training materials and campaigns, provided they have the necessary expertise, capacity, and internal resources. Alternatively, a wide range of domestic and international cybersecurity consulting firms offer professional awareness services tailored to this needs. Regardless of the delivery method, all effective awareness initiatives share a fundamental requirement: they depend on consistent time investment and active user engagement. Cybersecurity awareness cannot be passively acquired or achieved through a one-time solution—it must be cultivated through ongoing participation, practice and reinforcement.

Special areas - Training for information security managers and organisational leaders

At the time of writing, EM Decree No.17/2025. (VII. 24.) has been published, setting out detailed and specific requirements for training and qualifications of information security managers, but also of other key organisational roles. This development is significantly important, as experience from recent years, and even decades, has shown that security awareness and security training efforts often excluded senior leadership. Even when internal policies formally required comprehensive training, actual implementation was minimal. In many cases, it was considered a success if senior executives received a brief, 15-minute session once a year during a leadership meeting. However, such efforts were largely symbolic and had limited impact on meaningful awareness or behavioural change.

The law stipulates that the individual responsible for the security of the electronic information system must complete a minimum of 20 hours of training annually, covering at least three distint area, such as cybersecurity trends, risk management and organisational strategies, developments in EU and domestic legislation, incident management, technological advancements, cooperation with authorities, and the exchange of best practices. This approch supports continuous professional development and ensures complaince with the provisions set out in Section 3(1)-(2) of the EM Decree.

A notable and forward-looking additon to the legal framework is the requirement to extend cybersecurity training to the head of the organisation. Pursuant to the applicable rules, the executive leader must complete a minimum of

eight hours of basic training within one year of appointment, followed by at least four hours of annual training. These sessions must cover key topics on emerging cybersecurity trends, risk and strategy development, updates to legal obligations, incident management, and the sharing of best practices in accordance with Section 4 (1)-(2).

For both training obligations, programmes must be delivered by a registered adult education institution with at least three years of professional experience in accordance with Act LXXVII of 2013 on adult education. Additionally, the training program must be uploaded to the Fktv. data reporting system as required by Section 5 (2)–(3). The Decree also emphasises that the curriculum and the training format – whether e-learning, workshops, or practical seminars – should be designed to promote active participant engagement and ensure the practical application of acquired knowledge. This approch not only supports ongoing legal compliance, but also ensures that certificates issued upon completion are valid and verifiable during official inspections.

Special areas – IT operators and developers

A specific group, that has not been explicitly addressd is IT operators, including security infrastructure operators and developers. Neither the Cybersecurity Act nor the recently published legislation on qualifications specifically references this group, despite their crucial role in enhancing an organisation's cybersecurity resilience.

Training requirements for IT roles are not entirely separate from those applicable to general users and managers. The MK Decree specifies the detailed requirements for these roles. According to the Decree, specialised training is required to ensure that all personnel directly involved with electronic information system (EIS), including operators and developers, fully understand and are able to effectively apply the security measures and awareness controls relevant to their responsibilities.

Specifically, Annex 1 of the MK Decree along with the accompanying EIS guidance underscores the requirement for developers and operators to undergo both general and role-specific training within the „Awareness and training" control group. This covers topics such as security testing, vulnerability management, configuration hardening, and log analysis. The level of expertise required in these areas can only be achieved through specialised training programmes, which are more demanding and resource-intensive than standard security awareness training courses designed for general users.

When allocating the training budget, it is advisable to seek courses offered by established professional organisations (ISC)², CompTIA, EC-Council, Offensive Security (OffSec)).

In summary, security awareness and training have become critical and indispensable controls that can not be fulfiled merely by having employees sign an attendance sheet. Organisations that underestimate the importance of adequately training their staff, expose both themselves and their customers to substantial risks. Cybersecurity incidents continue to predominantly stern from human factors such as insufficient training, inattention, and inadequate security awareness.

22

Digital twin(s)

This chapter stands somewhat apart from the rest of the Whitepaper: as it contribute less directly to legal compliance or the promotion of compliance practices. Its purpose is to present a synthetic dataset designed for testing within a fictional IT environment of a non-existent manufacturer, rather than relying on real organisational data. The dataset includes a stimulated workforce and is particularly useful for assessing the capabilities of AI systems before applying them to „live" data within an exisiting organisation. The data was generated by the authors of the Whitepaper using various artificial intelligence-based systems and algorithms, such as generative language models and data simulation techniques.

22. Digital Twin(s)

Written by: Dr. Ágota Albert, Gergő Csarnai, Róbert Major

The concept covers, among other things:

- generating organisation-specific procedures, that take into account the organisational hierarchy, job descriptions, and requirements, including the responsibilities associated with each role (e.g., RACI);
- testing approaches for EIS grouping using a list of applications and infrastructure tools;
- employing the ITSM extracts to evaluate which tools an MI system would recommend for preventive maintenance and to detect potential indicators of security breaches.

Please note:

- The synthetic data does not represent actual events, persons, organisations, or assets. Any resemblance to real individuals, institutions, companies, locations, or events is purely coincidental and unintentional.
- The authors assume no responsibility for the accuracy, completeness, reliability or timeliness of the synthetic data, or for any direct or indirect consequences arising from its use. The dataset should not be relied upon as an authoritative source for real decision-making, business analysis, employment or other legal documentation, or for any practical application.
- The use of synthetic data is entirely at the user's own risk. It is strongly recommended not to base any decisions with real-world consequences on this data and to always consult verified, trustworthy sources.
- Synthetic data should not be used to identify individuals, misuse personal data, or otherwise infringe upon the rights, reputation, or interests of any natural or legal person.

The synthetic dataset of the digital twin comprises the following elements:

- a brief description of the organisation,
- employee headcount and organisational hierarchy,
- job descriptions of IT department personnel,
- applications andIT infrastructure,
- ITSM records.

Suggestions for further additions and comments on the completed documents can be sent to the following e-mail address: NIS 2wp.digitwin@gmail.com and can be accessed via this link: NIS 2 Whitepaper - „digital twin".

The digital twin includes a comprehensive list of all documents (strategies, regulations, other materials) cited in the MK Decree.This list can also serve as a starting point for preparing various materials, such as access agreements for employees in specific roles.

In addition, the digital twin contains 11 incident descriptions which allow users to explore both prevention (appropriate regulations, procedures, protocols, agreements, etc. as protective measures) and incident management scenarios, including response and action plans, thereby „learning from the mistakes of others". The incidents are based on real-life situations, and any penalties mentioned reflect those imposed on the organisations that committed the offences.

23. List of abbreviations

ACN – Agenzia per la Cybersicurezza Nazionale; in English: National Cybersecurity Agency

AI – Artificial Intelligence

AI Act – Artificial Intelligence Act

BCMS – Business Continuity Management System

BCP – Business Continuity Plan

BIA – Business Impact Analysis

BM OKF – Ministry of the Interior National Directorate General for Disaster Management

BMI – Bundesministerium für Inneres; in Hungarian: Federal Ministry of the Interior

BPM – Business Process Management

BPR - Business Process Reengineering

BQSA – Blockchain-based Quantum-Safe Architecture

BSI – Bundesamt für Sicherheit in der Informationstechnik; in English: Federal Office for Information Security

BYOD – Bring Your Own Device

CAQI – Common Assurance and Quality Indicator

CCB – Centre for Cybersecurity Belgium

CDN – Content Delivery Network

CER - Critical Entities Resilience Directive

CERT – Computer Emergency Response Team

CIA – Confidentiality, Integrity, Availability

CIP Security – Common Industrial Protocol Security

CMDB – Configuration Management Database

CyFun – CyberFundamentals Framework

CSA CAIQ – Cloud Security Alliance Consensus Assessments Initiative Questionnaire

CSA STAR – Cloud Security Alliance Security, Trust & Assurance Registry

CSIRT – Computer Security Incident Response Teams

DARPA – Defense Advanced Research Projects Agency

DEV environment – Development environment

DNP3 - Distributed Network Protocol 3

DNS service - Domain Name System service

DORA - Digital Operational Resilience Act

DPIA - Data Protection Impact Assessment

DRP - Disaster Recovery Plan

DSP – Digital Service Provider

ECC – Elliptic Curve Cryptography

EDR – Endpoint Detection and Response

eIDAS – electronic IDentification, Authentication and trust Services

EIS – electronic information system

EC - European Community

ENISA – European Union Agency for Cybersecurity

ENX – European Network Exchange

EU – European Union

EU-CyCLONe – European Cyber Crisis Liaison Organisation Network

EUR – euro

FALCON-1024 – Fast Fourier Lattice-based Compact Signatures over NTRU (parameter: 1024)

GAP analysis – gap analysis

GDPR – General Data Protection Regulation HR – Human Resources

HSM – Hardware Security Module

HVAC - Heating, Ventilation, and Air Conditioning

IAM – Identity and Access Management

IB – Information Security

IBF – Information Security Officer

IBSZ – Information Security Policy

ICS - Industrial Control Systems

IDS – Intrusion Detection System

IEC - International Electrotechnical Commission

IIoT – Industrial Internet of Things

ICT – Information and Communication Technology

IPS - Intrusion Prevention System

ISO - International Organisation for Standardization

IT - Information Technology

ITSM system - IT Service Management system

R&D – research and development

Cybersecurity Act – Act LXIX of 2024 on Cyber Security in Hungary

Cyber Act – Act on cyber security certification and cyber security supervision

SME – Small and medium-sized enterprises

Government Decree – Government Decree No. 418/2024 (X. 30.)

KPI – Key Performance Indicator

KSH – Central Statistical Office

MFA - Multi-Factor Authentication

AI – Artificial Intelligence

MK Decree - 7/2024. (XI. 15.) MK Decree

MKKR - Hungarian Qualifications Framework

NAIH – National Authority for Data Protection and Freedom of Information

NBSZ - National Security Service

NCSC/CERT.LV – National Cyber Security Centre / Computer Emergency Response Team Latvia

NDR – Network Detection and Response

NIS1 – Network and Information Systems Directive (first version)

NIS2 – Network and Information Security Directive (version 2)

NISG – Netz- und Informationssystemsicherheitsgesetz; in English: Network and Information Security Act

NIST CSF – National Institute of Standards and Technology Cybersecurity Framework

NIST SP – National Institute of Standards and Technology Special Publication

NKI – National Cyber Security Institute

NMHH - National Media and Infocommunications Authority

OAuth – Open Authorization; Hungarian: Nyílt jogosultságkezelési protokoll

OECD – Organisation for Economic Co-operation and Development

OES – Operator of Essential Services

OLA - Operational Level Agreement

OPC UA - Open Platform Communications Unified Architecture

OSCAL – Open Security Controls Assessment Language

OT – Operational Technology

PAM – Privileged Access Management

PCI DSS – Payment Card Industry Data Security Standard

PDCA – Plan – Do – Check – Act

PPT – People, Process, Technology

PQC – Post-Quantum Cryptography

QCC – Quantum Communication Channel

RACI – Responsible, Accountable, Consulted, Informed

RBT – System Security Plan

RDSI – Réseau Numérique à Intégration de Services (Integrated Services Digital Network, ISDN)

RPO – Recovery Point Objective

RSA – Rivest–Shamir–Adleman; public key encryption algorithm

RTO - Recovery Time Objective

SaaS – Software as a Service

SAB – Satversmes aizsardzības birojs; in English: Latvian Constitution Protection Bureau

SAML - Security Assertion Markup Language

SIEM - Security Information and Event Management

SIG-Full – Standardized Information Gathering Questionnaire (Full); in Hungarian: Standardized Information Gathering Questionnaire (full version)

SIS - Safety Instrumented System

SL2 - Security Level 2

SLA - Service Level Agreement

SMART - Specific, Measurable, Achievable, Relevant, Time-bound

SMS - Safety Management System

SOC - Security Operation Center

SOC 2 – System and Organisation Controls 2; Hungarian: System and Organisation Controls Type 2 report

SPHINCS+ – Stateless Practical Hash-based Incredibly Nice Cryptographic Signature Plus

SPOC – Single Point of Contact

SSH-Q – Secure Shell – Quantum-safe

SWIFT – Society for Worldwide Interbank Financial Telecommunication

SZTFH – Supervisory Authority for Regulatory Affairs

SZTFH Decree – 1/2025. (I. 31.) SZTFH Decree.

TCP/IP – Transmission Control Protocol / Internet Protocol; Hungarian: transmission control protocol / internet protocol, internet protocol suite

TISAX – Trusted Information Security Assessment Exchange

TLD – Top-Level Domain

TOM – Technical and Organisational Measures

TQNI – Trusted Quantum Network Infrastructure

UAT environment – User Acceptance Testing environment

USA – United States of America

VBA – Visual Basic for Applications; no translation available, a programming language built into Microsoft Office applications

VDA – Verband der Automobilindustrie; English: German Association of the Automotive Industry

VDA ISA – VDA Information Security Assessment

VLAN - Virtual Local Area Network

24. Disclaimer

This document was created as part of a non-profit professional collaboration and is published under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) license.
The document may be freely distributed, quoted, and used for internal preparation, training, and customer support purposes. However, it may not be sold or presented as a proprietary work.
Modification, independent republication of any part, and incorporation into any commercial product or service only permitted with the prior written consent of the coordinator (Dr. Dániel Váczi). In all cases of use, the authorship and the origin of the document must be clearly acknowledged.