HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 153–165.
DOI: 10.32567/hm.2024.4.11

István Oláh,[1] Sándor Magyar[2]

Security and Operational Controls for a Public Cloud Service in a Financial Institution

Abstract

Today, cloud computing services are growing very fast. One of the main reasons for this is the increasing competition and innovation in the market, the increased demand for resources in IT systems and the demand for more complex knowledge-based solutions. Deploying a server and performing the associated tasks on your own infrastructure can often take weeks or months, while the same process takes only a few minutes with a cloud service provider. The use of cloud services has become commonplace for anyone using mobile devices, and for financial institutions, this technology is becoming inevitable in the short term. If an organisation carefully selects a service provider on the basis of legal, technical and information security criteria, and then monitors its operations on an ongoing basis, there is no reason why a financial institution should not use public cloud services, according to the criteria examined. It is important to stress, however, that our analysis did not cover all possible risk factors.

Keywords: public cloud services, information security, financial controls, audit method, physical controls, logical controls

Introduction

Today, IT services based on cloud technology are rapidly expanding. One of the reasons for this is the new demand for resources in IT ecosystems, systems with more complex knowledge, resulting from accelerating market competition and innovation. Getting a server up and running, and setting up the associated tasks, can take weeks or months on a dedicated infrastructure. The same in the cloud can be provided by

[1] E-mail: olah.istvan.gyorgy@uni-nke.hu
[2] E-mail: magyar.sandor@uni-nke.hu

a cloud service provider in minutes. For the processes and operations of a company, financial institution, or public administration, the IT systems must be available according to the SLAs[3] to access the services provided, and these can be delivered in the cloud. This expectation is reflected in the CER,[4] NIS2,[5] and DORA[6] specifications, which came into force in January 2023. Gartner's *The Cloud Strategy Cookbook*[7] outlines several key information security ideas:

- What are the security, governance, compliance, and data requirements?
- Does it contain personally identifiable information and security requirements?
- Is a vendor involved?
- Does it have special integration or location requirements?

In 2015, ENISA[8] published *Secure Use of Cloud Computing in the Finance Sector*.[9] In 2021, it has already clearly recommended the use of a specification in practice in its publication on healthcare systems,[10] based on NIST[11] and BSI[12] – C5.[13]

In many cases, the choice between a terrestrial and/or a cloud-based IT system is no longer a decision for the operations of financial institutions. The reason is that software vendors are developing new solutions in their own data centres less and less frequently, and are also migrating existing systems to cloud versions, resulting in the fact that in a few years, they will no longer support the non-cloud case.

The present study sets out the following research objectives:

RO1: Examination of the utilisation of public cloud services in a financial institution.

RO2: Analysis of physical security requirements from the perspective of a financial institution in the context of public cloud services.

Consequently, the research study has identified the following research questions to be addressed:

RQ1: Can a public cloud be audited in compliance with domestic regulations for a financial institution?

RQ2: Can a cloud service provider's data centre be considered part of a financial institution's operational environment? If so, how?

[3] SLA – Service Level Agreement.
[4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[5] Directive (EU) 2022/2555 OF the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).
[6] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 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) 2016/1011.
[7] Gartner 2021.
[8] ENISA – European Union Agency for Cybersecurity.
[9] Naydenov et al. 2015: 11.
[10] ENISA 2021.
[11] NIST – National Institute of Standards and Technology.
[12] BSI – Federal Office for Information Security in Germany.
[13] C5 – Cloud computing C5 criteria catalogue.

Cloud services

The cloud is a technology and the services associated with it. In practice, they are still often confused, because, for example, a "cloud" can be on the ground.

Cloud services are not defined in legislation. There are several arguments for and against the need for separate regulation, for example:

- NO, because the cloud (all components) or part of it can be in your machine room
- NO, because the primary concern for the data is consistent protection
- NO, because everything can be regulated in the related contracts
- YES, because it is in the public interest to regulate part of the mandatory content of contracts
- YES, because the immediacy of physical controls has been partially removed
- YES, because of the level of risk justified by the non-operational risk of larger cloud service providers
- YES, because the cloud has become the operational space for civil and military cyberspace

The authors' position on this is that no specific regulation is necessary, because it is irrelevant to the data where it can be located in an IT ecosystem,

- user, server on host
- on the network
- on storage
- the above on a virtual version
- on tape
- on disk
- on portable storage media
- on a mobile device
- anywhere
- in the cloud

because its protection must be consistent and proportionate to the risks.

In practice, the definitions provided in the National Institute of Standards and Technology (NIST) document 800-145 are utilised.[14] The common characteristics of services are:

- the ability to use the service as needed at that time, sometimes on a self-service basis
- access to the network is essential
- shared use of resources among users
- tracking of required operational capacities, payment of dynamic resources, and charges proportional to the services utilised

[14] Mell–Grance 2011.

Taking into consideration the ownership, the nature and content of the services provided, and the geographical location, the following cases may exist according to NIST:

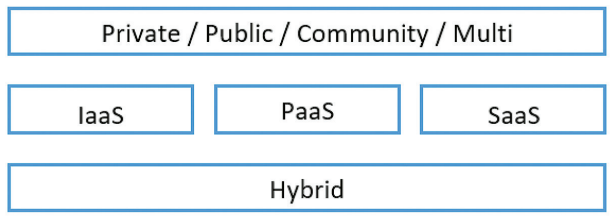

Figure 1: Categorisation of cloud services
Source: compiled by the authors

- Private is when an organisation uses the cloud as a technology in a private manner
- Public refers to service is typically available to everyone via the Internet, free of charge and/or for a service fee
- Community describes a service that is typically available to a specific group of people over the Internet, free of charge and/or for a fee
- IaaS[15] is when the basic infrastructure is utilised
- PaaS[16] when a service includes an operating system and/or running environment
- SaaS[17] when everything is provided by the service provider by outsourcing data and users
- Multi refers to the scenario where multiple service provider solutions are used in an integrated manner
- Hybrid describes a service provider's solution is deployed with some or all of the resources being hosted on the customer's infrastructure

Responsibility aspects

The management of information security risks in terms of services between the service provider and the service recipient should be clearly defined in terms of responsibilities at the IT ecosystem levels. The Hungarian National Bank Recommendation[18] guides a financial institution in this regard:

[15] IaaS –Infrastructure as a Service.
[16] PaaS – Platform as a Service.
[17] SaaS – Software as a Service.
[18] Recommendation No. 4/2019 (IV. 1.) of the National Bank of Hungary.

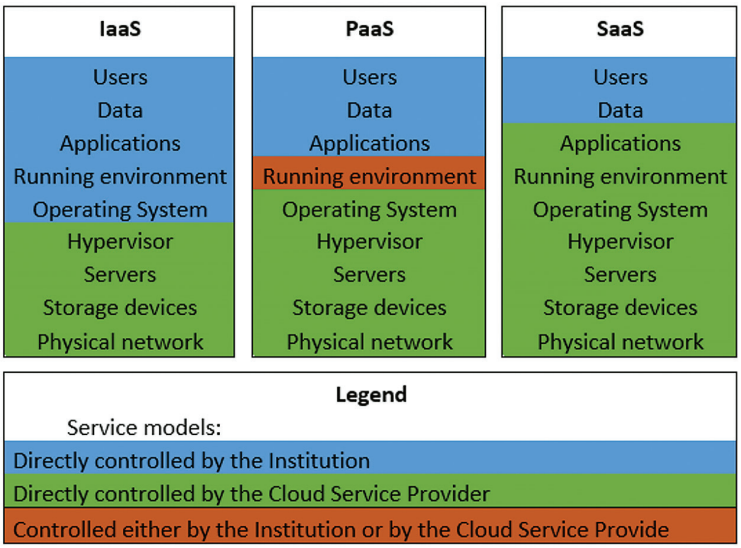

Figure 2: Service models and direct operators of controls over elements
Source: Recommendation No. 4/2019 (IV. 1.) of the National Bank of Hungary

It is important to emphasise that the client of the public cloud service, i.e. the financial institution, is always responsible for the handling of users and the confidentiality, integrity, and availability of data.

A service used can now be practically anything. Cloud technology can be used for wrong purposes without significant expertise, for example by cybercriminals.

Matching the control logic of a public cloud service to its legal logic in five steps

In our country, several financial institutions are covered by the Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities (hereinafter: LRTV),[19] because finance is one of the sectors listed in its annex. In this context, the Act L of 2013 on the information security of state and municipal bodies (hereinafter: IBTV)[20] is applicable to these organisations under Section 2(c). The information security requirements of the IBTV are established in an implementing decree of the Ministry of the Interior; in 2024, the MK decree on the new security classification and information security conventions in the context of NIS2 was published.[21]

At the time of writing, both regulations were in force. The Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter: HPT)[22] is one of the foundational pieces of legislation relating to financial activities. According to Article 67/A

[19] Act CLXVI of 2012.
[20] Act L of 2013.
[21] Decree No. 7 of 2024 (VI. 24.) of the Cabinet Office of the Prime Minister.
[22] Act CCXXXVII of 2013.

of the HPT, IT systems in operation must possess a continuous certificate of secrecy. The Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter: DÁPTV),[23] a financial institution is also an organisation obliged to provide digital services. In this context, Section 81(1)(d) of the Act establishes the basis for the requirements regarding information security compliance. Both the HPT and the DÁPTV require compliance with the same government regulation.[24] It has been stated in several analyses, and conference presentations, that financial institutions to which the DORA requirements apply are not subject to NIS2. This correlation exists as long as a credit institution provides its services to an entity subject to DORA under a law of a country's jurisdiction that is founded on NIS2.

Based on the provisions of the NIS2, the Cybersecurity Act, the Act also defines several services, such as data centre services and cloud services, which are included in the Digital Infrastructure sector. A credit institution may have customers that DORA does not cover, and therefore the Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision (hereinafter: Cyber-certification Act).[25] For this reason, the implementing regulation will also apply to a credit institution if it is a financial institution. The controls in the new regulation are defined based on NIST-800-53 Rev. 5.[26]

Audit of legal logic requirements

In the light of international and national laws and regulations, the question arises as to whether a credit institution's IT systems can be audited against the required logical controls.

This question has been posed to the audience and co-presenters at several professional conferences in the recent past. The typical answer received back was no. We believe the answer to this question is yes, but in several steps. The steps can be taken for any public cloud provider, an example is given for Microsoft Azure.

Selecting and assembling a test control

As a first step, it is necessary to select a logical control based on BM Decree 41/2015 (15. VII.)[27] (hereinafter: BM Decree) and MK Decree 7/2024 (24. VI.) (hereinafter: MK Decree), for example, the lock of the work section, which must be aligned with the NIST identifier.

[23] Act CIII of 2023.
[24] Government Decree 42/2015 (III. 12.).
[25] Act XXIII of 2023.
[26] NIST Computer Security Resource Center 2020.
[27] Decree 41/2015. (VII.15.) of the Minister of Interior.

Table 1: NIST assembly of regulatory control

BM Decree			
Locking the session	3.3.10.10	3.3.10.10.2 Covering the screen: When locking a session, the information previously visible on the screen should be obscured by a publicly visible image (or blank screen) or by the login interface, which may include the name of the person locking the session.	
MK Decree			**NIST**
Lock device, Screen lock	2.83	The organisation concerned shall hide the information on the display when locking the device. The organisation shall display static or dynamic images on the device display during the lock period. During device locking, the organisation shall ensure that the information on the display is not visible. In this way, the organisation prevents access by unauthorised persons.	AC- 11 (1)

Source: compiled by the authors

NIST control documentation

The second step is to identify the control in the audit documents published by the cloud service provider.

Table 2: AC-11 (1) control

NIST			
AC-11 (1)	Device Lock, Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colours, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Source: NIST Special Publication 800-53

Examining the possibility of control

In a third step, it is suggested to examine the possibility of establishing control AC-11 (1) in the example, based on several compliance documents audited by third parties. It is very important to note that control as an option does not imply the implementation of control as required by the organisation.

This is stated in the documentation:

"AC-11 Session Lock. The information system:

(a) Prevents further access to the system by initiating a session lock after [FedRAMP Assignment: fifteen (15) minutes] of inactivity or upon receiving a request from a user; and

(b) Retains the session lock until the user re-establishes access using established identification and authentication procedures."

Definition of control parameters at the organisational level

In the fourth step, it is necessary to define the control parameters of the organisation. This can be done in a related policy or an Information System, Information Security System Plan. In the case of a session lock control, it is the time parameter that must be specified. This can be any value, which may be as long as 15 minutes, set by the cloud service provider. The principle of proportionality of risk should be applied to this definition. Accordingly, several values may be prescribed for a single cloud service provider based on the risk level of the IT system. In the practical examples examined, this conscious value setting is often not performed and the time parameter set by the service provider is typically used. In any case, it is recommended that the parameters of the controls for service users should be defined, if possible, based on a risk analysis. The defined values can and should be recorded in the system security system plan, for example, in an OVI[28] table. If necessary, the table can be extended with additional controls specific to the cloud service.

Validation of the required control parameters

In the fifth step, the parameters required by the security domains in the design of a cloud service need to be set according to the related and approved documentation. This can also be accomplished through individually accessible administrator service web interfaces. For an IT system, many information security controls must be established in a public cloud service. This may require thousands of parameters to be configured. To facilitate this, service providers typically offer an API.[29] A simple script can be created to set the required security parameters in an automated manner. In this case, it is recommended that a six-eyes check is integrated into the organisation's internal processes before executing the settings, as the use of this procedure in itself poses a significant information security risk.

Continuous monitoring of controls

APIs provided by service providers also allow an organisation to export the parameters of the services it uses. Building on this capability, simple scripts can be created to

[28] See: https://nki.gov.hu/hatosag/hirek/ovi-urlap-4-60/
[29] API – application programming interface.

provide an automated way to continuously monitor the information security control parameters of IT ecosystem elements in the cloud. One example of this is to compare the read parameter with the required parameter and reporting discrepancies. Another possibility is to monitor the deviation from the previously read value. Many more examples of verification could be described, but the emphasis is on treating any discrepancy found during verification as an information security incident. These incidents are always investigated in a documented manner by the organisations according to their respective procedures, thus creating secondary control over the cloud service providers. It is recommended that the logs of a cloud service provider's administrative activities be reviewed before engaging a service. It is necessary to determine for which activities and which log entries should be generated by the organisation. In practice, it is advisable to do this before the contract is concluded because, in this case the specification can be taken into account when choosing a service provider. The logs generated by operational systems in a public cloud should be continuously scanned by an analytical SIEM,[30] SOAR[31] or any analytical system, thus reducing the risk of exposure to the cloud service provider.

Mapping a public cloud service to regulatory-based physical controls

When using a public cloud service, except in the hybrid case, the user must accept, in fully or in part, that the server rooms or data centres will be located outside the physical space under their direct control. It does not follow that it is not necessary to analyse the physical controls. It is recommended that a public cloud service provider's data centre is subject to the physical controls of the relying organisation, even though the data centres are not located in its facilities.

The legislation described for the examination of logical controls includes the IBTV. The second paragraph of the third section typically applies to a financial institution. According to this, IT systems may have components within the European Union. This is a geolocation constraint that should be tested for compliance at the outset of a cloud service provider selection process and non-compliant providers should be excluded. Typically, the leading cloud providers in Europe and the U.S. can meet this requirement. It is recommended that cloud service contracts should specify the countries and localities in which the service provider will deliver services to the customer. It is also advisable to stipulate in the contracts that the customer has the right to control the physical facilities directly or indirectly. If these are included in the contracts, a significant step will be taken to ensure that a cloud service user can view the service provider's premises as they would as a private facility.

[30] Security Information and Event Management.
[31] Security Orchestration, Automation, and Response.

Audit of legal physical requirements

Most physical controls can be checked similarly using the five-step method described in the previous chapter. For completeness, a specific procedure and/or additional control is recommended. An example of each is provided.

Continuous monitoring of controls with specific additions

A public cloud service operating area is usually not managed or controlled by the user. It is recommended that specific additions beyond the five steps outlined in the case of logical controls are included in the related contracts.

Chapter 3.1.5 of the BM Decree provides for the management of security incidents. According to 3.1.5.6.1.1, "everyone who is in contact with the electronic information system or the object in which it is located is required to report the occurrence of a security incident or if an indication or emergency is detected".

Chapter 3.2.1 of the BM Decree prescribes controls for physical and environmental protection, for example: "3.2.1.4.1 The covered entity: 3.2.1.4.1.1. Shall ensure physical access to authorized personnel only at entry and exit points defined by the covered entity."

The technical, human, and other skills needed to do this are covered in the five-step methodology already described for logic checks. This does not imply that the user organisation meets the requirements in Sections 3.1.5 and 3.2.1, as the information on the controls is available from the cloud service provider in the course of day-to-day operations. For this reason, specific clauses for such cases need to be included in the service contracts, as they are usually not included in the service providers' blanket contract designs. In our case, the physical locations of the services used:

- access rules
- for the management of rights in the monitoring systems
- the incident reporting process and contact details
- the means of monitoring the above

be specified in the service contract.

It is also included as a control requirement in the MK Decree in point 11.6:

"The organization shall ensure that digital and analog media are protected and controlled by appropriate security measures during transportation outside the controlled area." Examples of digital media include floppy disks, magnetic tapes, external/removable hard disks, flash drives, CDs, and DVDs. Examples of analog media include paper and microfilm.

"The organization must ensure accountability of the media during transport outside controlled areas." This may include restricting transport activities to authorised persons and monitoring transport activities.

"The organization should document activities related to the transport of media." The organisation concerned should have the flexibility to define the methods of

record-keeping for different types of media transfers, based on the risk assessment of the EIR.

Additional physical controls

If you use a cloud service, you may need to implement additional controls, as data centres are not directly supervised. An example of this are the requirements found in BM Decree 3.3.8.5.2, and in MK Decree 11.6, which can be used as a logical control to facilitate activities in the physical space.

Table 3: NIST assembly of regulatory control

BM Decree			NIST
Cryptographic protection	3.3.8.5.2	Cryptographic mechanisms should be in place to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas.	MP-5
MK Decree			
Transport of data media	11.6	1. The organisation must ensure that digital and analogue media are protected and controlled by appropriate security measures during transportation outside the controlled area. Examples of digital media include floppy disks, magnetic tapes, external/removable hard disks, flash drives, CDs, and DVDs. Examples of analogue media include paper and microfilm. 2. The organisation must ensure accountability of the media during transport outside controlled areas. This may include restricting transport activities to authorised persons and monitoring transport activities. 3. The organisation should document activities related to the transport of media. The organisation concerned should have the flexibility to determine the methods of record-keeping for different types of media transfers, based on the EIR risk assessment.	

Source: compiled by the authors

Microsoft's premises are considered to be an area not controlled by the user. Digital media for backup and archiving purposes are also produced here and handled during transport. According to the documentation available for the five-step methodology described in the Logical controls test, the service provider platform is capable of encryption. It does this by default using a self-generated and self-managed cryptographic procedure. For a financial institution, it is necessary to consider whether these are sufficient to adequately manage industry secrets, GDPR,[32] and corporate confidentiality. We think not, because in this case all data is still available to a cloud service provider in an interpretable manner, so additional controls need to be applied. To this end, it is proposed to develop a separate HSM[33] solution used and managed

[32] GDPR – General Data Protection Regulation.
[33] HSM – Hardware Security Module.

exclusively by the user organisation. To enhance the information security for use, the following is proposed:

- If possible, do not generate keys on the service provider's devices, because residual information must be considered.
- Key management should be controlled and restricted.
- All activities in the key management processes should be performed by the user organisation.
- Stored keys should not be directly accessible by the cloud service provider.

There are several options for setting up an HSM with cloud service providers on a software-based solution, which can be interpreted as a SaaS. Its development can be completed quickly with the associated process flows without integration issues. In our experience, this solution is suitable for a financial institution. If required, it is also possible to develop a custom hardware-based HSM, but then all external and internal APIs must be developed and kept up to date by the customer organisation, which can be managed by a specially trained staff.

Discussion

Cloud services are now commonplace for anyone using a mobile device. In the case of financial institutions, it will become unavoidable in the short term. If an organisation selects a service provider based on legal, technical, and information security criteria and continuously monitors its operations, there is no obstacle for a financial institution to use a public cloud service based on the criteria examined in this article.

It is also important to emphasise that not all possible risks have been considered in this analysis. For this reason, we recommend that all organisations should draw up a list of information security controls for analysis in proportion to the risks associated with other aspects. Based on the criteria you have compiled, analyse the use of any public cloud service, the outcome of which may be that you do not use the service or use it differently.

Drawing on the conducted studies, our results are as follows:

R1: We have determined that by applying our five-step examination method proportionally to risk, a financial institution can audit a public cloud service, except for certain physical controls.

R2: We have found that, from the perspective of protected data, security must be implemented uniformly regardless of storage and processing location. Therefore, a public cloud provider's data centre must be subject to at least the same controls as a financial institution's own data centre. Given that a financial institution cannot directly control the physical space of a public cloud provider, compensatory controls, such as data encryption, ensure adequate protection.

This article is an excerpt from a presentation given at the II. Alverad-Bánki International Cybersecurity Conference on October 15, 2024.

References

European Union Agency for Cybersecurity (ENISA) (2021): *Cloud Security for Healthcare Services.* Online: www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cloud%20Security%20for%20Healthcare%20Services.pdf

Gartner (2021): *The Cloud Strategy Cookbook.* Online: www.gartner.com/smarterwithgartner/the-cloud-strategy-cookbook

Mell, Peter – Grance, Tim (2011): NIST SP 800-145, *The NIST Definition of Cloud Computing.* Gaithersburg, MD, USA: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-145

Naydenov, Rossen – Liveri, Dimitra – Dupre, Lionel – Chalvatzi, Eftychia (2015): *Secure Use of Cloud Computing in the Finance Sector.* ENISA. Online: https://doi.org/10.2824/199301

NIST Computer Security Resource Center (2020): *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.* Online: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Recommendation No. 4/2019 (IV. 1.) of the National Bank of Hungary on the use of community and public cloud services. Online: www.mnb.hu/letoltes/4-2019-felho.pdf

Legal sources

Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities

Act L of 2013 on the Information Security of State and Municipal Bodies

Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises

Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision

Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services

Decree No. 7 of 2024 (VI. 24.) of the Cabinet Office of the Prime Minister on the requirements for security classification and the specific security measures to be applied for each security class

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Government Decree 42/2015 (III. 12.) on the protection of IT systems of financial institutions, insurance and reinsurance undertakings, investment ventures and commodity exchange service providers

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 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) 2016/1011

Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)