Information security training

For operators

2025

Table of Contents

1. IT security basics

1.1. The basics of information security

What is security?

Even though often confused in the vernacular, data protection and data security are not synonymous. Data protection refers to the protection of personal data, while data security refers to the security of data stored, transmitted or processed on information systems.

IT security is the favourable state of IT systems in which the confidentiality, integrity and availability of the data handled are closed with respect to the elements of the system and are continuously assured (this is the so-called "CIA principle"):

- *confidentiality:* only those authorised have access to the information;
- *integrity:* the form and content of the information is as expected and the person who handles the information can be clearly identified;
- *availability:* the state when the services of an IT system are available to authorised users at a specified time, and the expected operation of the system is not temporarily or permanently impeded;

Information security is a much broader concept than IT security, as it includes all forms of information (not just electronic), as well as the security of services.

1.2. Legal basis

DORA Regulation

The Digital Operational Resilience Act (DORA) is an EU regulation that entered into force on 16 January 2023 and is applicable from 17 January 2025. It aims to strengthen the IT security of the financial sector to ensure that financial institutions remain resilient in the event of a major disruption.

The following pillars ensure the digital operational resilience of the financial sector:

1. **ICT risk management:** Financial institutions are required to develop a comprehensive framework for identifying, assessing, managing, and mitigating IT risks.
2. **Incident reporting**: Mechanisms must be put in place to report significant IT incidents to regulators in a timely manner, including detailed documentation and analysis of incidents.
3. **Digital operational resilience testing**: Regular testing must be carried out to ensure digital operational resilience, including basic and advanced tests.
4. **Third-party risk management**: Financial institutions need to manage the risks associated with third-party service providers, including key contractual provisions.
5. **Information sharing**: Exchange of information and intelligence on cyber threats between actors of the financial sector.

MNB Recommendation 1/2025 on information system security

The aim of the Recommendation is to provide practical guidance to members of the financial intermediary system on how to design the protection of their IT systems in a risk-proportionate

manner and to ensure a consistent interpretation of the application of the legal provisions on their protection. The Recommendation is applicable in conjunction with MNB Recommendation 2/2025 on the use of community and public cloud services, the Management Circular on written contracts and written declarations made electronically, MNB Recommendation 12/2022 (VIII. 11.) on the establishment and operation of internal security lines, on the management and control functions of financial institutions, and the MNB Recommendation on the use of external service providers.

1.3. Risk management

Information security risks and threats arising from operations can be identified. Knowing these, and taking into account the risk levels assumed by senior management, security professionals will set up a combination of protection mechanisms that is acceptable to the organisation.

A threat to the information system is any circumstance or event that compromises the security of data or information systems. This includes external incidents (e.g. natural disasters) or attacks from individuals (computer hacking).

Threat modelling

In risk analysis, it is important to be aware of the threats to the security of information systems. Threat modelling is a structural representation of all the information that could affect the security of the environment.

A threat model typically consists of the following elements:

- a description of the system to be modelled;
- assumptions about the system that can be checked or changed in the future;
- potential threats to the system;
- an action plan to reduce potential threats;
- validation of the model.

Threat modelling is the process of collecting, organising, and analysing these elements. There are several modelling techniques, such as STRIDE, which was adopted by Microsoft and works by breaking down potential threats to a system into six groups.

Threat	Nature of the threat	Definition
Spoofing	Identification	Identity fraud
Tampering	Integrity	Modification of information
Repudiation	Verifiability	Denial of an action
Disclosure of information	Confidentiality	Unauthorised access to data
Denial of service (DoS)	Availability	Denial of service, or withdrawal of service from the user
Elevation of user rights	Authorisation	Acquiring capabilities without proper authorisation

1.4. Managing information security incidents

A security incident is an unintended or unexpected event or series of events that causes an adverse change or a previously unknown situation in the electronic information system. As a result, the confidentiality, integrity, authenticity, functionality, and availability of the information processed in the system may be compromised or the risk of compromise may be increased.

The ability to identify, investigate, respond to, and recover from information security incidents must be planned, implemented, and managed to reduce the damage to the organisation.

- An action plan for responding to information security incidents must be developed and kept up to date to ensure that the organisation is able to respond effectively and in a timely manner to any incident.
- A process for investigating and recording information security incidents should be established and maintained.
- A system for incident reporting and escalation must be developed and updated to ensure that the organisation can involve stakeholders in the definition and implementation of security incident responses.
- A team must be organised and trained to respond to information security incidents in a timely and effective manner.
- The incident management plan should be periodically tested and reviewed to ensure that the organisation responds effectively to information security incidents.
- A communication plan and process must be developed and kept up to date to manage communication with internal and external stakeholders.
- A review must be carried out once the emergency has been resolved. The cause of information security incidents must be identified. Remedial action should be reviewed and risks reassessed. The effectiveness of the response should also be reassessed and, if necessary, appropriate corrective measures taken.
- The integration of incident management plans, disaster recovery plans and business continuity plans should be developed and kept up to date.

Security log management

There are many names for the team that handles cyber security incidents, such as CIRT (Computer Incident Response Team), SOC (Security Operations Center), or CDC (Cyber Defense Center).

Cybersecurity incident management can be achieved by properly aligning the relevant human resources, processes, and technology levels. The technology layer should be integrated with other elements of the cybersecurity architecture, the basic incident management processes should be defined and aligned with related IT and non-IT processes, and the cybersecurity incident management team should be adequately trained to perform the processes.

To detect malicious activities, continuous monitoring of the organisation's systems is required. The aim is to provide real-time “visibility” of the protected data assets. A necessary precondition for this is that events with cyber security relevance are properly logged at each endpoint. Visibility is achieved by processing security logs, endpoint logs and network traffic. Once the necessary data has been collected, it needs to be aggregated, interpreted, indexed and analysed to identify harmful patterns and behaviours. This is usually provided by SIEM (Security Incident and Event Management) products at the technology level.

When a potential cybersecurity incident is detected, the first step is to make sure whether it is a real incident or a false alarm. Once it is confirmed that the incident is a real cybersecurity incident, the next step is to categorise and assess severity, which will determine the response actions and the timeframe for their completion (these tasks are collectively referred to as the triage step).

The next steps are to identify and take response actions to minimise the impact of the incident on business operations.

The next two steps, analysis and containment, are usually performed in parallel, in several iterations. The purpose of the analysis is to understand the details of the incident, on the basis of which an existing or individually defined response plan can be carried out. The purpose of containment is to isolate the incident and allow time for analysis. Since forensics and malware analyses usually take significant time, a proper containment strategy is essential to prevent further damage to business.

Once the appropriate response actions have been defined based on the results of the analysis, the incident must be eradicted and the systems must be remediated before the incident can be closed.

The sequence of the steps described above (continuous monitoring, detection, triage, containment, analysis, eradication, and remediation) is commonly referred to as the “incident response chain”.

SOAR

Today, incident management teams face similar challenges:

- the number and sophistication of cybersecurity attacks continues to grow;
- the complexity of the environment to be protected increases (new environments, such as IoT or the Cloud, are emerging alongside traditional IT systems).

As a result, SOC teams have to process a large number of alerts, with incident response chain steps to be performed in each case. They have to use a variety of different systems to perform their tasks. As each sub-task is carried out by different tools, it is difficult to effectively keep track of all the information related to a given incident in one central location.

The consequence of these is the so-called "alert fatigue", which can cause incidents to go unaddressed and increase the time it takes to deal with them.

Theoretically, these challenges could be easily addressed by scaling up the operation appropriately. However, scaling up to the desired level is not feasible in practice, even with an infinite budget – just think of the shortage of properly trained cybersecurity analysts.

At the technology level, it is the SOAR (Security Orchestration, Automation and Response) product that is designed to address these challenges. The main functions of SOAR products are orchestration and automation. Orchestration provides integration between SOAR and other products, while automation allows incident management without the need for human resources (e.g. identifying affected users in a phishing incident, checking whether someone has provided authentication information, disabling compromised user accounts, etc.)

SOAR provides a single interface for analysts to perform all incident management steps. Detection and response steps, vulnerability management and threat intelligence can be managed within the SOAR platform without the need to constantly switch between systems. In practice, this means that the

SOAR system “fetches” the alarms generated in the SIEM system, collects the information needed for triage, and supports the containment or even the remediation and recovery steps with automated actions. As all steps in the incident response chain are tracked within it, SOAR becomes the main tool for incident management teams. At the beginning of the shift, analysts enter this system and spend most of their time in it. Ideally, if the right integrations are in place, analysts will be able to find all the information they need to analyse the incident in SOAR and trigger the implementation of response actions from there (e.g. collection of other logs, isolation, collaboration with peer IT departments through opening error logs, etc.)

1.5. NIST Cybersecurity Framework

The NIST framework classifies all IT security capabilities, processes, and day-to-day activities into the following 5 main functions:

- *Identify*: the processes and assets that need protection.
- *Protect*: the application of appropriate security measures to safeguard the organisation's assets.
- *Detect*: the use of appropriate mechanisms to identify IT security incidents.
- *Respond*: the use of appropriate techniques to deal with IT security incidents.
- *Recover*: the application of appropriate processes to repair the damage caused by an IT security incident.
- Each of the main features includes an additional subcategory with corresponding recommendations.

NIST Recommendation SP-800-53 provides the control steps to successfully implement the security framework.

Category	Examples of controls
Access control	Account security and surveillance; least privilege; separation of duties
Awareness and training	User training on security threats; technical training for priority users
Audit and accountability	Content of audit records; analysis and reporting; record keeping
Assessment, authorisation, and monitoring	Connection to public networks and external systems; penetration testing
Configuration management	Checking approved software policies, configuration changes
Contingency planning	Alternative processing and storage sites; business continuity strategies; testing
Identification and authentication	Authentication policies for users, devices and services; credential management
Individual participation	Consent and privacy authorisation
Incident response	Incident response training, monitoring and reporting
Maintenance	System, staff and equipment maintenance

2. General attack techniques

A good starting point for learning about the anatomy of information security and cybersecurity attack techniques is the MITRE ATT&CK framework.

The framework documents the tactics, techniques and procedures (TTP-tactics and procedures) used by attackers based on attacks against real systems, thus providing insight into attacker behaviour.

MITRE ATT&CK provides a behavioural model consisting of the following elements:

- Tactics, which represent the attacker's short-term tactical objectives during the attack.
- Techniques, which describe the tools and procedures used by an attacker to achieve their goal.
- Sub-techniques, which describe in more specific detail the technique used to achieve the goal.
- Metadata, which is the documentation of the techniques and procedures used by the attacker, and other related information.

2.1. Attacking tactics and techniques

The tactical level describes the effect of an ATT&CK technique or sub-technique used. This is the tactical purpose of the attacker for which they are taking the action. For example, an attacker wants to gain user access to a system.

Name of the tactic	Description
Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
Resource Development	The adversary is trying to establish resources they can use to support operations.
Initial Access	The adversary is trying to get into your network.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Defence Evasion	The adversary is trying to avoid being detected.
Credential Access	The adversary is trying to steal account names and passwords.
Discovery	The adversary is trying to figure out your operational environment.
Lateral Movement	The adversary is trying to move through your environment and systems.
Collection	The adversary is trying to gather data of interest to their goal.
Command and Control	The adversary is trying to communicate with compromised systems to control them.
Exfiltration	The adversary is trying to steal data.
Impact	The attacker tries to manipulate, interrupt, or destroy the systems and the data.

Techniques show how attackers achieve their tactical goals through a certain action. For example, an attacker can collect login credentials to gain access to certain systems.

2.2. Example of techniques used in a network attack

The following figure summarises the techniques involved in the steps of an attack carried out through network access.

Initial Access

Technique used: Exploit Public-Facing Application

Attackers may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Execution

Technique used: Command and Scripting Interpreter

Adversaries may abuse command and script interpreters accessible through the Internet to execute commands, scripts, or binaries. The malicious code can be embedded in the payload used in the previous step, or in a variety of other ways to reach the vulnerable shell of the target system.

Persistence

Technique used: Modify Authentication Process

Services that manage the authentication process, such as Local Security Authentication Server (LSASS) and Security Accounts Manager (SAM), are responsible for collecting, storing, and validating credentials in a Windows environment. The attacker exploits their vulnerabilities to gain access to authentication information, allowing them to gain long-term access to target systems.

Technique used: Pre-OS Boot

Using the access gained, the attacker modifies the boot process to maintain remote access to the device. This is particularly difficult to detect, because it circumvents software protection technologies.

Technique used: Traffic Signaling

An adversary can install services to remotely send commands to the compromised device. This may take the form of a series of network packets that have particular characteristics.

Defence Evasion

Technique used: Impair Defenses

The adversary disables preventive (such as firewall or antivirus software) and detective (such as logging) protection controls on the device in order to minimise the detection of its presence or a subsequent attack technique.

Technique used: Modify System Image

Adversaries may make changes to the operating system of embedded network devices to weaken defenses and gain new capabilities.

Technique used: Network Boundary Bridging

An adversary establishes interoperability between segregated networks, such as by changing the settings of a compromised network or perimeter device, or by changing the settings of an endpoint device with multiple network interfaces. This opens up the possibility to access additional internal network segments.

Technique used: Weaken Encryption

The adversary modifies or disables the requirement to encrypt network connections on the compromised device. They also gain access to the keys used for encryption, which can be used to access stored data that is encrypted with the key or transmitted over the network.

Credential Access

Technique used: Input Capture

The adversary captures input streams containing user credentials and use them to extract and decrypt the credentials.

Discovery

Technique used: Network Sniffing

The attacker captures network traffic, which will be used for identifying additional vulnerable devices that can be targeted, or for obtaining data.

Collection

Technique used: Data from Configuration Repository

The adversary collects data from various configuration repositories, which helps to gain remote or even administrative access.

Command and Control

Technique used: Non-Application Layer Protocol

The adversary uses network connection level communication protocols to remotely control the compromised device.

Technique used: Proxy

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure.

Exfiltration

Technique used: Automated Exfiltration

Adversaries may exfiltrate data or sensitive information from the compromised system through communication channels created earlier.

3. Preventing hacker attacks

To prevent hacker attacks, organisations have a number of process and technology controls in place. In this chapter, we are going to discuss the most important techniques.

Access management

Access management refers to a set of security mechanisms that determine what users can do on the system, i.e. the resources they can access and the operations they can perform. Includes security measures that control

- the authorisation of a user to access the system;
- the applications a user can run;
- the information a user can read, create, add, or delete.

It generally includes the steps of identification, authentication, access approval, and audit, but, in some cases, it is also considered to include accountability.

The main principles used in access control:

- Separation of Duties

  The goal is to assign different people to different steps in a process. To do this, the process must be designed to prevent one person from controlling and manipulating the entire process (for example, the same person in an accounting department cannot receive invoices and initiate their payment).

- Least Privilege

  By respecting this principle, the system restricts access to resources for users and applications to only those that are necessary. This requires defining the minimum set of privileges required for users to work.

Access control is also important because if a user account has been accessed by attackers during an attack, the damage can be minimised (if it is not a privileged account). To prevent incidents, it is recommended to set passwords for user accounts to the appropriate strength and to change them regularly.

Network separation

The network must be designed so that each device can communicate only with those devices that are absolutely necessary to perform its function. One technological way to achieve separation is to use firewalls.

3.1. Basics of vulnerability management

Vulnerability management aims to identify vulnerabilities affecting the organisation and reduce the risks they pose by eliminating the vulnerability or applying compensatory controls.

3.2. Vulnerability analysis

Vulnerabilities affecting the organisation must be uncovered so that appropriate measures can be taken to reduce the associated risks. Ongoing vulnerability assessment is one of the first steps in the vulnerability management process, as it is used for comparing information about new vulnerabilities with information available about internal assets in order to identify the assets affected.

During the vulnerability assessment, analysts collect the affected assets and notify the asset owners or operations teams of the vulnerability. The effectiveness of vulnerability assessment largely depends on how up-to-date and accurate the asset information database of the organisation is.

In large corporate environments, using vulnerability scans can be difficult for a number of reasons, such as:

- before the scan itself takes place, careful planning is needed to determine the appropriate timing of the test to minimise potential business impacts, as even passive scans can negatively affect the operation of systems;
- in a large corporate environment, it can take a long time (weeks or even months) to run a full scan due to the large size of the infrastructure. If the vulnerability scans are not complemented by vulnerability analysis, many vulnerabilities will go unnoticed for a long time between two scan cycles;
- in highly or even completely isolated environments, network scanning can be complicated, while the use of locally installed scanners increases the time and resources required for scanning;
- In certain environments using critical or unique technologies, design and implementation requires additional care.

3.3. Prioritisation and classification of vulnerabilities

If a vulnerability is found to affect an information asset of the organisation, the related risks must be determined to allow the prioritisation of response and the implementation of compensating controls.

Prioritisation should not be based solely on the severity of the vulnerability, but also take into account the criticality of the asset within the organisation. Therefore, the way the organisation prioritises vulnerability should take both into account.

So-called 0-day vulnerabilities, for which no patches exist yet, but have already been targeted by malicious codes (exploits), require special prioritisation because they sometimes receive too much attention compared to their real impact and risk exposure. By default, 0-day vulnerabilities should be treated with the highest severity, but it is of paramount importance to follow the usual prioritisation process to ensure that they are treated in a way that is proportionate to the real risk.

The purpose of vulnerability triage is to determine the timeframe for response.

When a vulnerability is identified during a vulnerability assessment or scan, vulnerability triage ensures that the priority assigned to the vulnerability is checked and, if necessary, fine-tuned, depending on how the affected system component is used within the organisation.

3.4. Reducing the impact of vulnerabilities

If an information asset is confirmed to be vulnerable, and the vulnerability is exploitable, it must be determined how the impact of the vulnerability can be mitigated.

If a security update is available, the patch should be managed in accordance with the established priority. Otherwise, some form of compensatory control must be defined. If there is publicly available information on vulnerability mitigation (e.g. from the manufacturer of the vulnerable system), this can be used as a basis, but, in any case, its applicability within the organisation should be checked.

If, for any reason, it is not possible to apply an update or compensating control, the associated risk should be monitored in line with the organisation's general risk management processes.

4. Patch management

The following concepts are most commonly used in relation to patch management:

patch	A *patch* is a small piece of code that is released to fix one or more bugs discovered after the programme has been published.
hotfix	A *hotfix* is a type of patch that, as the name suggests, usually provides an urgent and vital correction to the programme and that should be installed as soon as possible.
official patch	Official patches and updates are issued by the product manufacturer. Manufacturers have different support policies, but security patches to fix vulnerabilities are usually provided until the end of the standard support period.
unofficial patch	When a software product reaches the end of its lifecycle and the manufacturer no longer supports it or discontinues the product, no more official patches are released. However, there are cases where enthusiastic developers use their own time and resources to develop and publish patches to keep the software alive. Such patches are called unofficial patches.

A significant share of cybersecurity incidents are the result of exploiting vulnerabilities for which patches have been in place for weeks or months at the time of the attack.

One of the most famous ransomware, WannaCry, exploited a vulnerability that was patched two months before the first successful attack, yet the attack affected more than 200,000 computers in over 150 countries, causing disruption or outages in critical services such as healthcare in the UK, local government in Sweden or rail transport in Germany. Ransomware attackers, probably dissatisfied with the willingness of their victims to pay, have changed their attack method over time. Nowadays, some ransomware attacks are not only about taking data hostage, but also about getting it. In many cases,

data is first stolen, and then encrypted. This way, the blackmail operation is no longer just about restoring the data, but also about the risk of disclosing damaging information if the victim fails to pay, such as intellectual property or sensitive emails, as in the Sony hacking. Moreover, if personal data is stolen, the company could even face a significant fine from the authorities.

As a consequence, improving vulnerabilities is of paramount importance to ensure outage-free operation and to avoid losses. In most cases, vulnerabilities are fixed by installing a patch. Patches can fix not only security flaws, but also operational flaws, as well as those that add new functionality to systems.

In addition to solving these challenges, patch management can be improved and made more efficient by not trying to install all patches on all our devices. The installation of patches should be prioritised to ensure that those patches are installed first that address the most pressing issues, and that patches for less immediate dangers are scheduled for a later time or even completely disregarded.

In practice, of course, scheduling, testing, and deployment also present their own challenges.

In many cases, the last step in the patch installation process is a reboot, which results in the device being temporarily unavailable. In the case of a workstation, if the user has saved all open files, the reboot is a minor inconvenience. However, restarting a server, a network device or a similarly critical piece of infrastructure that operates 24/7 can result in a service outage, which, if timed badly, can not only hinder internal users, but – in the case of an internet bank, for example – can also affect customer satisfaction or business result. Therefore, the timing should also take into account the needs of the business and preferably be done at a time to keep the negative impact at minimum.

Patch management can also be facilitated by standardising tools. It is advisable to minimise the number of tool types used in the IT environment as much as possible, not only to simplify the process, but also to reduce the time needed for testing. As far as possible, use the same configurations for test systems as for live systems, but use separate systems. An important part of the patch management process is exception handling. It may not be possible to deploy a patch for reasons such as compatibility issues. For example, the installation of a patch may cause a system crash, or, in the case of a third-party device, the configuration cannot be changed without the manufacturer's approval. The process should also address the treatment of these exceptions and manage them accordingly, not forgetting the approval, monitoring and regular review of exceptions.

5. Cloud security

Cloud computing, as defined by NIST, is a model that enables access to a common pool of configurable computing resources (such as networks, servers, storage, applications and services) on demand, from anywhere, conveniently. They should be rapidly deployable, scalable and terminable with minimal user resources and service provider interaction.

5.1. Cloud application security

Securing cloud applications means using rules, tools, and controls to protect the software running in the cloud.

Cloud applications are vulnerable to various cyber threats, such as:

- unauthorised access to application features or data;
- application services vulnerable to threats from incorrect configurations;
- account hijacking due to poor encryption and identity management;
- data leakage due to insecure APIs or infrastructure endpoints;
- Distributed Denial of Service (DDos) attacks due to mismanaged resources.

The 5 best practices for implementing effective security steps for cloud applications:

- *Identity and Access Management*
  IAM ensures that all users can only access data and application functions that require authentication.

- *Encryption*
  Implementing encryption in the appropriate parts of the application optimises application performance while protecting sensitive data. In general, the encryption of data during storage, transmission and use should be addressed.

- *Threat monitoring*
  Once an application is deployed in the cloud, it is essential to continuously monitor threats in real-time.

- *Data privacy & compliance*
  In addition to application security, data protection and compliance are essential to protect the end users of cloud applications.

- *Automated security testing*
  A key part of making cloud applications secure is integrating automated security testing directly into the development process. Shifting left testing reduces the cost of detecting and fixing vulnerabilities, while ensuring that developers can continue to release code quickly.

5.2. Cloud infrastructure and platform security

IaaS and Paas providers treat applications inside users' virtual instances as black boxes, as they are not responsible for running and managing users' applications. Therefore, it is important to note that it is the user's responsibility to secure applications running in such a cloud, as follows:

- When designing an application to run in the cloud, threat modelling of the application should also be performed and the results fed back into the design process.
- Remediation processes should be defined and implemented to reduce the impact of web vulnerabilities.
- It is the user's responsibility to keep their applications up to date and it is recommended to ensure a security patching strategy that provides protection against malware and exploits. This also helps ensure the confidentiality and integrity of their data.

6. Best practices related to system hardening

Hardening procedures aim to establish minimum levels of system security in order to reduce the attack surface and thus information security risks.

6.1. CIS Benchmarks

CIS has developed different reference settings for specific systems, such as Microsoft and Linux products. The standards cover two levels of configuration:

- The first level focuses on attack surface reduction.
- The second level aims to create defence-in-depth.

The benchmark categories defined by CIS are as follows:

- Desktop and web browsers
- Mobile devices
- Network devices
- Virtualisation platforms
- Cloud environments

6.2. System hardening best practices

Use of Standard Operating Environments (SOE)

SOE is the standardised installation and configuration of operating systems and applications, designed to provide consistent and secure baseline settings and values.

When SOE comes from third parties or service providers, additional supply chain risks should be considered, such as the accidental or intentional transfer of malicious content or configurations. To reduce the likelihood of such events, organisations should not only obtain operating environments from trusted sources, but also perform vulnerability and configuration scans before using them to ensure their integrity.

Use of operating system releases and versions

Newer releases of operating systems often result in improved security features compared to older releases. This can make it more difficult for attackers to create a working exploit (code or technique to exploit a vulnerability) for the vulnerabilities they have discovered.

Recommended security controls:

- Use the latest releases and updates of operating systems for workstations, servers, and network devices.

Operating system configuration

If operating systems are installed by default, this can easily lead to an insecure operating environment, which attackers can use as an initial entry point to the network.

Recommended security controls:

- Adhere to the hardening guidelines provided by the manufacturers for the secure configuration of the operating system.
- Disable, rename, or change passwords for default operating system accounts.
- Disable or remove unnecessary operating system accounts, software, components, services, and features.
- Enable procedures that make it impossible to change, disable, or bypass security features of operating systems.
- Prevent non-priority users from using scripting engines and applications in a Microsoft Windows environment.

Managing local administrator accounts

If local administrator accounts are used with common account names and passwords, this can allow an attacker who wishes to compromise a workstation or server to easily transfer authentication credentials across the network to other workstations or servers.

Recommended security controls:

- Disable local administrator accounts or use random and unique passwords for the local administrator account of each device
- Use individual local administrator accounts for workstations and servers, without domain administrator privileges

Application management

The right to install applications may be a real business need for users, but it can be exploited by an attacker.

Recommended security controls:

- Deny users the right to install unapproved software.
- Deny users the right to remove approved software.

Application control

Application control can be highly effective not only in preventing malicious code from running, but also in ensuring that only approved applications are installed.

Recommended security controls:

- Implementing application control on endpoint devices

Exploit protection

An attacker can effectively exploit vulnerabilities in operating systems by creating and deploying a targeted exploit if the operating system's prevention features are not enabled.

Recommended security control:

- Implement exploit protection features on workstations and servers

PowerShell

PowerShell is easy to use for full control of Microsoft Windows environments, even by an attacker.

Recommended security controls:

- Disable or remove Windows PowerShell 2.0.
- Restrict the use of the PowerShell language (Constrained Language Mode).
- Centrally store PowerShell event logs in a protected location, monitor them continuously, and take incident management action in the event of a compromise alert.

SSH

SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh or rcp. It is strongly recommended that older, text-only login protocols are abandoned in the different environments.

Recommended security controls:

- Set the permissions of /etc/ssh/sshd_config correctly.
- Set SSH private and public key permissions correctly.
- Use SSH Protocol 2.
- Disable SSH HostbasedAuthentication.
- Disable SSH root login.

Set SSH LogLevel to the appropriate level. **Host-based Intrusion Prevention System (HIPS)** Many endpoint security solutions rely on signatures to detect malicious code. This approach is only effective if the malicious code has already been profiled and the signature databases are up to date. The host-side intrusion prevention system uses behavioural detection schemes to identify and block anomalous behaviour such as malicious process injection, keyloggers, or malicious code that is unknown to antivirus vendors.

Recommended security controls:

- Install and run HIPS on workstations.
- Install and run HIPS on critical servers, such as authentication servers, DNS servers, web servers, file servers or email servers.

Software firewall

Often, traditional network firewalls fail to prevent malicious code from spreading across the network or an attacker from leaking sensitive data, as they usually only control the selection of ports and protocols to use between different network segments. Software firewalls are more effective than network firewalls in that they can control which applications and services can communicate with workstations and servers.

Recommended security controls:

- Install and run software firewalls on workstations and servers to control inbound and outbound application-level network connections and communications

Endpoint protection software

Attackers often invest considerable time and effort in developing exploits that work well and are reliable. Although known exploits can be profiled by antivirus vendors, they can still remain an effective method of intrusion in organisations that lack the technologies and processes to detect them.

Recommended security controls:

- Implement and run endpoint protection software on workstations and servers.
- Set signature-based detection to a high level of detection.
- Set heuristic detection to a high level.
- Set up measures against ransomware.
- Update signature databases at least daily.
- Set up automatic and regular scanning for all fixed and removable media.

Device access control software (DAC)

Using device access control software makes it possible to prevent unauthorised devices (e.g. unapproved smartphones, tablets, Bluetooth devices, wireless devices, 4G/5G hardware keys) from connecting to workstations and servers via external interfaces such as USB ports, contributing to the deep protection of workstations and servers.

Recommended security controls:

- Install and run device access control software on workstations and servers to prevent unauthorised devices from connecting.
- Disable external interfaces on DMA-enabled workstations and servers.

7. SWIFT security basics & security requirements

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions worldwide to send and receive financial transaction information in a secure, standardised, and reliable environment.

SWIFT's Customer Security Programme (CSP) helps these institutions to ensure their protection against cyber-attacks is up-to-date and effective, protecting the integrity of the wider financial network.

Mandatory security controls set a security baseline for the entire organisation using SWIFT. They must be applied by all SWIFT users on the local SWIFT infrastructure. SWIFT prioritises these mandatory controls to set a realistic short-term target for tangible security improvements and risk mitigation.

Changes in 2021

The 2021 version of the CSCF introduced two significant changes. These are aimed at improving and adapting the framework to changing threats and at implementing tighter security controls. A

recommended control has been made mandatory and the scope of another existing control has been extended:

- New Mandatory Control: Control 1.4, Restriction of Internet Access, has become mandatory. This control focuses on limiting Internet access to the minimum necessary extent required to perform business functions, both in the secure zone and in operator PCs that interface with SWIFT.
- Change in scope: The scope of Control 4.2, Multi-factor Authentication, has been extended. It now requires the use of multi-factor authentication before access to SWIFT-related applications or components operated by third-party service providers that process transactions.

8. Security guidelines in CIS and NIST recommendations for operators

8.1. CIS

The CIS (Center for Information Security) framework was developed in 2008 to meet the complex IT security needs of organisations.

Prioritisation is one of the main advantages of CIS controls. They are designed to help organisations quickly identify the starting point for their defences, directing scarce resources towards immediate and high-value-added activities. The CIS 8.1 version distinguishes 18 controls.

Inventory and control of company assets	Audit log management	Managing suppliers & service providers
Inventory and monitoring of software assets	Email and web browser protection	Software security
Data protection	Anti-malware protection	Incident management
Secure configuration of enterprise tools and software	Data recovery	Penetration testing (Pentest)
Account management	Network infrastructure management	
Access rights management	Network monitoring and protection	
Continuous vulnerability management	Security awareness and skills training	

8.2. NIST

What is NIST 800-53?

NIST 800-53 is a security compliance standard created by the U.S. Department of Commerce and the National Institute of Standards in Technology (NIST) in response to rapidly growing technological

advances by national adversaries. It summarises the controls proposed by the Information Technology Laboratory (ITL).

The standard was developed to integrate privacy and security controls and to facilitate integration with other IT security and risk management approaches.

What is the purpose of NIST 800-53?

The purpose of the security and privacy standard is threefold:

- Providing comprehensive and flexible controls that ensure the security of IT today and in the future, in an ever-changing world of technology and threats.
- Developing methodological bases to increase the effectiveness of the control of processes and techniques.
- Developing a common communication scheme to improve the discussion of risk-taking concepts between organisations.

NIST 800-53 security controls

The NIST framework classifies all IT security capabilities, processes and day-to-day activities into the following 5 main functions:

- *Identify*: the processes and assets that need protection.
- *Protect:* the application of appropriate security measures to safeguard the organisation's assets.
- *Detect:* the use of appropriate mechanisms to identify IT security incidents.
- *Respond:* using appropriate techniques to deal with IT security incidents.
- *Recover:* the application of appropriate processes to repair the damage caused by IT security incidents.

NIST 800-53 provides security and privacy controls and guidance. They are assigned to the following 20 themes, which correspond to one of the 5 categories mentioned above.

Identify	Protect	Detect	Respond	Recover
Asset management	Access control	Anomalies and events	Response planning	Recovery planning
Business environment	Awareness and training	Continuous security monitoring	Communication	Implementing improvements
Governance program	Data security	Detection processes	Analysis	Communication
Risk assessment	Information protection processes and procedures		Mitigation activities	

Risk management strategy	Maintenance of protection systems		Implementing improvements	
Supply chain risk management	Managing protective technology			

9. Declaration on the learning outcomes of the course

Please send a declaration that you have successfully completed this course by e-mail to dora_oktatas@otpbank.hu with the following text:

"The training material developed by OTP Bank Plc. for the Contracting Partners who are ICT service providers in accordance with the requirements of the DORA Regulation has been read and understood by, and is accepted as binding on, all persons employed by [name of Partner company] in relation to the service provided to OTP Bank Plc. [Name of Partner company] undertakes to ensure that its employees and subcontractors involved in the provision of the service are familiarised with the training material throughout the life cycle of the service and to expect its employees and subcontractors to comply with the terms of the training material."service

10. Declaration on the learning outcomes of the course for sole traders

If you are a sole trader, please complete the following form and send it to dora_oktatas@otpbank.hu: "By completing this declaration, I declare that I have read and accept the contents of the General Privacy Notice (https://www.otpbank.hu/portal/hu/adatvedelem) of OTP Plc."

Please also be informed that OTP Bank, as the controller, processes the name and e-mail address of, and the fact of completion of the training by, the sole trader in the context of the declaration in order to comply with the requirements of the DORA Regulation on the basis of a legitimate interest pursuant to Article 6(1)(f) of the General Data Protection Regulation.