The Architecture Guild

30.3.2026

Digital security

Contents

1 What is digital security? 2
1.1 Digital security architecture 3
2 Framework 3
2.1 Governance – How we manage digital security 5
2.2 Identification – What we have to protect 6
2.3 Protection – How we protect against threats 6
2.4 Detect – How we detect incidents 7
2.5 Response – How we manage incidents 7
2.6 Recovery – How we continue to operate 8
3 Digital security assessment 8
3.1 Information security audit methods 8
3.2 Frameworks and standards – what they fit into 9
4 More information 10

The Architecture Guild

30.3.2026

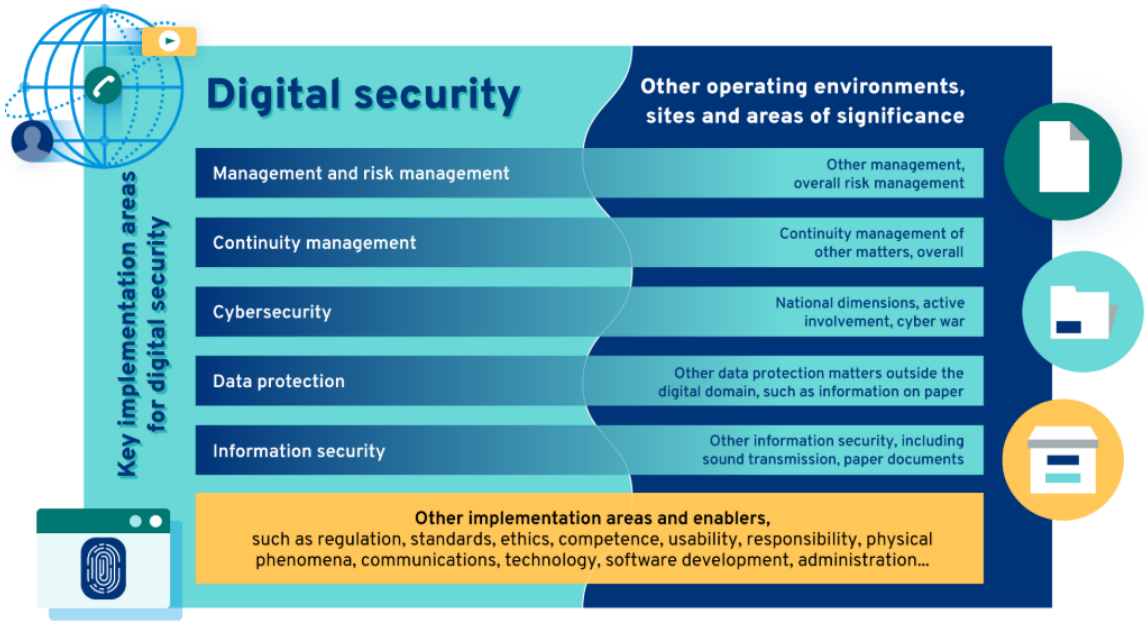
1 What is digital security?

Digital security aims to ensure that the digital operating environment is reliable, secure and accessible. This requires that different actors are able to prepare for threats to the digital operating environment, withstand disruptions and recover from them as effectively and as quickly as possible. Securing everyday functions also requires extensive cooperation, shared operating models and willingness to develop them.

Digital security implementation areas also extend beyond the digital world. In other words, digital security is not a separate entity from the rest of the organisation or society, but an integral part of all their activities.

Digital security in public administration has five focus areas that are shared by all actors and necessary for producing controlled digital security. These focus areas are management and risk management, continuity management, information security, data protection and cybersecurity.[1]

Figure 1 Digital security



[1] What is digital security? | Digital and Population Data Services Agency (dvv.fi)

The Architecture Guild 30.3.2026

1.1 Digital security architecture

The digital security architecture is first and foremost a planning and design tool to help with developing and structuring digital security. The architecture is an understanding of the organisation's assets and operating environment that need to be protected, as well as the threats and risks to them. In addition, it covers an understanding of the requirements and strategic policies that concern the organisation and the building blocks of digital security that they are implemented with.

In other words, digital security architecture aims to plan and perceive digital security, which is an extensive and constantly changing entity, paying particular attention to how the changing environment and its requirements affect digital security choices and solutions made.

Digital security architecture is used to achieve the following objectives:

- Understand the needs related to the organisation's activities and set objectives for the digital security practices and technical solutions based on them.
- Prepare a description of the organisation's digital security structures as part of the organisation's enterprise architecture.
- Adapt digital security solutions to the organisation's other activities by, for example, considering them in the organisation's enterprise architecture.
- Set a target state for digital security, towards which we work with determined development.

In other words, the framework as such is not a set of criteria or a catalogue of safety controls – it contains concrete measures and examples for improving digital security.

Who?

The framework is intended for all public administration actors as a tool for holistic planning and conceptualising of digital security.

The framework does not establish which instrument or tool an organisation should use to describe or document digital security, as the effectiveness of description methods vary from organisation to organisation. An organisation should utilise the framework in a manner that it deems to be best. However, creating visual and structural descriptions makes it considerably easier to conceptualise large entities.

2 Framework

The framework for digital security architecture is based on the internationally recognised Cybersecurity Framework developed by the American National Institute of Standards and Technology (NIST). The framework brings together practices from a variety of standards

and consists of six key functions: governance, identification, protection, observation, response and recovery.

The framework enables systematic planning and documentation of digital security requirements, principles and the capabilities serving them in accordance with the organisation's goals. The key functions of the framework and their objectives are briefly described in this document. The actual measures are divided under six key functions into categories that form the structure of the framework.

Cybersecurity Framework

The framework for digital security architecture is based on the internationally recognised *Cybersecurity Framework* developed by the American *National Institute of Standards and Technology (NIST)*. The framework compiles practices from several standards and it consists of six key functions: **governance**, **identification**, **protection**, **observation**, **response** and **recovery**. In the framework, the functions are divided into several categories. Each category consists of detailed measures and **capabilities**.

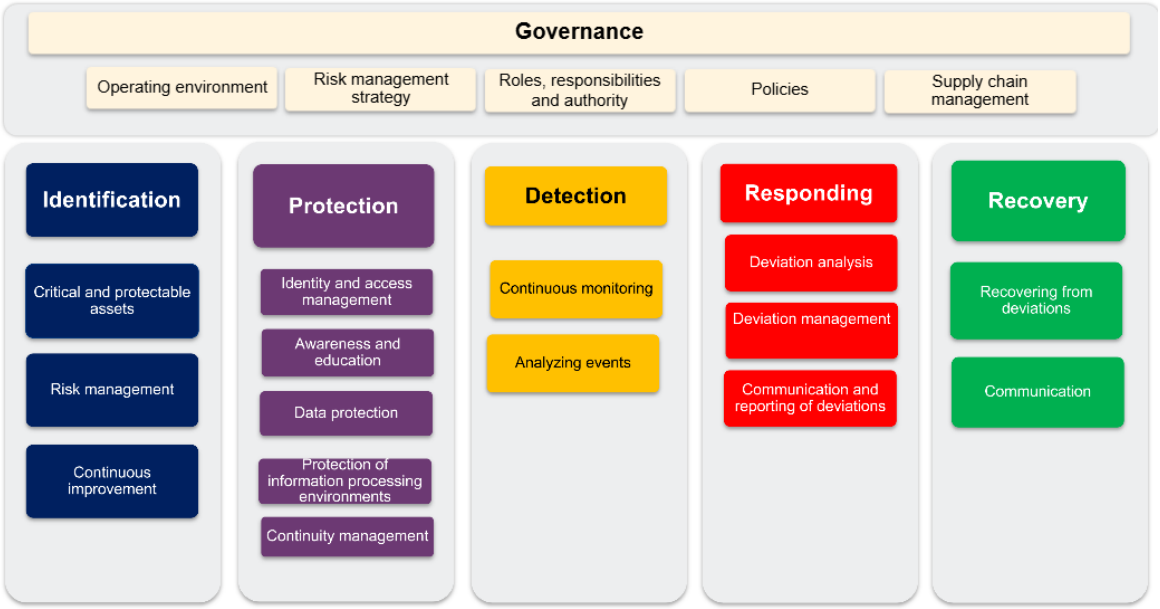
Figure 2 Cybersecurity Framework | NIST

The NIST Cybersecurity Framework (CSF) 2.0

Presentation of the framework

The development of a digital security architecture begins by identifying factors related to one's own operating environment, such as the digital elements to be protected, the infrastructure, regulations and other requirements. Once factors and requirements related to digital security have been identified, it becomes possible to plan the solutions used for protection and observation with this information. The main steps of the guidelines aim to help with building comprehensive structures for responding to incidents, recovering from them and using accumulated lessons and experiences for further development.

Figure 3 The architecture of digital security



2.1 Governance – How we manage digital security

The goal of management is that the organisation has established administrative structures and processes to manage digital security.

The end result is that the following matters related to the organisation's digital security are in line with the organisation's operations and are regularly developed.

- Strategies
- Policies
- Processes
- Resources

This guides the organisation in what it should do to achieve and prioritise the objectives and expectations of the other five key functions of the framework. Management-related functions play a key role in integrating cybersecurity and digital security into the organisation's broader comprehensive risk management strategy.

Management covers understanding the organisation's operations; defining the cybersecurity strategy and supply chain risk management; setting roles, responsibilities and authorisations; policy creation; and supply chain management.

It is essential that the organisation's cybersecurity and digital security risk management strategy, expectations and policy are defined, communicated and monitored.

2.2 Identification – What we have to protect

The purpose of the identification stage is that the organisation has identified its operating environment and the critical protected objects and assets that enable it to continue operating. Furthermore, the organisation has identified the threats and risks to the above and potential impact of the risks on its operations.

The identification of an organisation's own operating environment and protected subjects is the first part of forming a digital security architecture. Measures, such as the protection of targets or detection of incidents, can only be carried out if you know your own environment well enough.

Identification creates a description of the digital environment of your organisation, including

- its systems, information pools, devices, and data contained therein
- its operating environment and factors that guide its operation, such as legislation
- its digital security management model, such as practices and plans
- the threats and risks of the digital environment and their controls

It is essential for the architecture of digital security that, during the identification phase, the targets requiring special protection, observation, response or recovery measures can be determined.

2.3 Protection – How we protect against threats

The purpose of the protection stage is for the organisation to protect identified targets, such as information systems, information resources and data from identified threats and risks by means of risk management. In practice, this means, among other things, identity and access management, information network security, information security, planning and implementation of information security technology appropriate of the identified risks, and the documentation and description of these measures.

From the perspective of protection, it is essential to take into account different requirements and information security solutions at all stages of the lifecycle of information systems, services and supporting infrastructure, from development to maintenance and decommissioning.

As the information security and data protection requirements of the protected objects vary according to the data to be processed and the operating environment, it is particularly important to identify the requirements concerning the operations and data of your organisation in the identification section of the framework.

The protection measures presented in the framework are measures derived from international information security, cybersecurity and digital security standards that enable the organisation to build its protection as a whole instead of separate solutions.

2.4 Detect – How we detect incidents

The objective of the observation phase is for the organisation to develop the ability to observe incidents affecting digital security. In practice, this means defining and implementing the incident management process in a way that the organisation has defined the base level of digital security and has introduced a process and methods to detect events that affect digital security and to improve detection capability.

It is important to note that in terms of digital security, mere protection against identified risks and threats is not enough. In addition, we need an understanding of what is normal activity and what is abnormal activity in digital environments. Observation of abnormal activities can be carried out efficiently if the targets to be protected and their intended use and operating environment are sufficiently well known.

There are several technical solutions to implement detection capabilities, but relying on them alone is insufficient, as it is also necessary to have processes and operating models for processing and correcting observed incidents in place.

Digital security observation is also supported by notifications made by users. Therefore, it is essential that the organisation has an operating model for reporting and receiving notifications.

The following sections guide you to systematically build your power of observation so that the operating models and selected technical solutions would support each other as well as possible.

2.5 Response – How we manage incidents

The aim of the response stage is for the organisation to have the capability to respond to detected digital security incidents as quickly as possible according to the incident management process. In practice, this means implementing an incident management process in which the personnel and stakeholders are aware of their tasks and roles in response measures, communication, coordination and reporting practices have been defined, and digital security disruptions are managed and their impact mitigated.

In most cases, responses to digital security incidents occur either as a result of an incident that is detected using technical tools or through user reports.

For response, it is important that possible incidents have already been considered beforehand. Related plans for communication, recovery and continuity must also be up-to-date and known by the necessary persons.

One part of an incident response is analysis and investigation of the reasons for the incident and taking the necessary corrective measures.

It is therefore advisable to practise incident response at regular intervals either by holding internal targeted exercises or by participating in an exercise organised by an external party.

2.6 Recovery – How we continue to operate

The objective of the recovery phase is for the organisation to be able to recover from a disruption caused by digital security back to its normal operating state. In practice, this means creating and developing recovery plans for critical protected systems based on incident recovery experiences and planning to correct any reputation damage caused by a digital security disruption.

Actions related to functional recovery also serve as input for continuous improvement, i.e., **identification** of new requirements, needs and capabilities (Step 1).

3 Digital security assessment

3.1 Information security audit methods

This document compiles the most common frameworks and methods of information security auditing and provides practical instructions on how to select a suitable combination for verifying administrative and technical information security. The focus is on auditing practices: what is actually checked, what evidence is used and what tools are used.

What does information security audit mean in practice?

Auditing can mean a wide variety of things. In practice, it is divided into three questions:

1) Is the required management and control system in place? (administrative information security)

2) Are the controls implemented in everyday life and are they demonstrably effective? (operational activity)

3) Is the technical implementation and configuration in line with the requirements? (technical security)

A good audit combines both administrative and technical information security (e.g., configurations, logs, test results, vulnerabilities, code checks).

Administrative vs. technical security

Administrative security means:

- Management, different policies, responsibilities, risk management, incident handling, continuity, supplier management, roles, instructions, minutes, supplier agreements, continuity plans, audit reports

Technical security means:

- Configurations, vulnerability management, identity management, network solution and segmentation, logging, adequate hardening, application security, backups, vulnerability scans, penetration testing reports

3.2 Frameworks and standards – what they fit into

Below is a description of the key audit methods and the role in which they are usually used. The best result is almost always achieved by combining the management system (e.g., ISO 27001) and the technical control catalogue (e.g., CIS Controls) with the application security requirements list (OWASP ASVS).

ISO 27001

ISO 27001 is a management system and requires processes for risk-based information security management. Ideal for external certification and demonstrates that security is managed in a controlled manner and when an organisation wants a systematic management model (roles, risks, improvements) and/or certification.

ISO/IEC 27002 is an annex to ISO 27001 and can be used to verify that the information security controls (organisational, personnel, physical, technological) are adequate and are particularly suitable as an audit criterion.

CIS (Critical Security Controls)

The CIS is a prioritised technical control catalogue for practical cyberdefence (18 controls) and it is suitable for ensuring whether “the configuration is correct”. It includes an implementation and action list for basic technical security and also includes configuration hardening standards (operating system, cloud services, databases, network devices).

OWASP ASVS (Application Security Verification Standard)

OWASP ASVS is an application security requirement and audit standard that defines the security requirements to be measured and verified for applications according to their criticality (levels L1–L3).

In practice, it is used as a common set of criteria for development, testing and auditing, for example, as a procurement requirement, as a basis for penetration testing and as an acceptance criterion for DevSecOps.

NIST SP 800-53

NIST SP 800-53 is a comprehensive and detailed framework for data security and data protection controls, covering administrative, technical and operational controls, in particular for high assurance and government environments.

It is used in practice to define, audit and continuously monitor system security requirements, often in conjunction with risk classification and baseline thinking.

The Architecture Guild

30.3.2026

4 More information

If you would like to familiarise yourself with the digital security architecture framework in more detail, please refer to the public Confluence workspace and the eOppiva course on digital security architecture and its utilisation in the organisation prepared by the Digital and Population Data Services Agency.

Workspace: Digitaalisen turvallisuuden arkkitehtuuri - Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio - DVV external Confluence

The course is available on eOppiva: What is digital security architecture?- Organising digital security through architecture (eoppiva.fi)