Good Practice

Information Security 2023

DeNederlandscheBank
EUROSYSTEEM

Introduction

This Good Practice provides institutions under the supervision of DNB with tools and control measures with which they can comply with the legal provisions to ensure the continued availability, integrity, confidentiality and authenticity of (automated) data processing. In this document, ensuring the integrity, continuous availability and security of automated data processing is briefly referred to as "information security and cybersecurity".

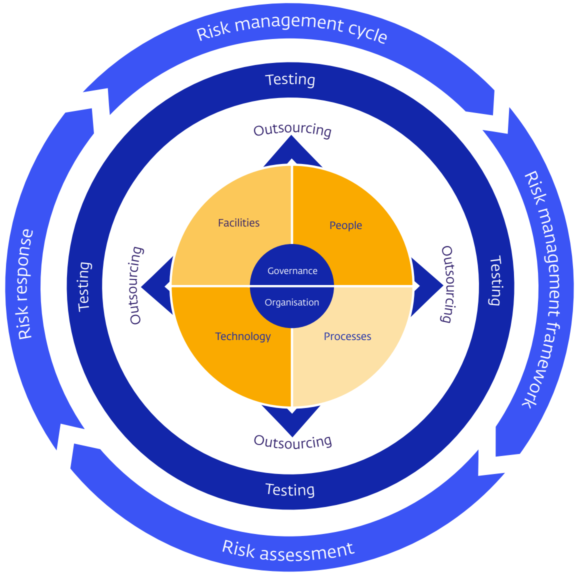
To manage risks in the field of information security and cybersecurity, institutions take control measures based on a risk analysis. These control measures are appropriate to the nature, size, complexity and evolution of the risks of the institution's activities and the complexity of its organizational structure. The control measures are not only aimed at technological solutions (*Technology*), they are also aimed at human actions (*People*), design of processes (*Processes*) and facilities (*Facilities*).

Institutions periodically and demonstrably evaluate the extent to which the control measures taken are effective in design, existence and operation to cope with the constantly changing risks in the field of information security and cybersecurity. They do this on the basis of a risk analysis – as part of their risk management process (*Risk Management Cycle*) and metrics that demonstrate the actual impact of the measures. Where necessary, control measures are improved or replaced by better control measures. The institutions set up their management (*Governance*) and organization (*Organisation*) to manage this. Institutions ensure, among other things, in line with the new corporate governance code 2022, the *DNB Q&A Key functions and adequate separation of functions* and the *DNB Q&A Key functions with operational independence and proportional set-up*, for an appropriate separation and independence of ICT risk management functions, control functions and internal audit functions[1]. Furthermore, the board has demonstrably followed training and education tailored to them to understand and address the most important ICT risks and control measures for its institution (*People*).

Institutions also ensure that they are 'in control' in the field of information security when outsourcing (*Outsourcing*). In addition, they test (*Testing*) to what extent they as an institution are resilient to cyber threats. This Good Practice includes a maturity model on the basis of which DNB assesses the management of risks in the field of information security and cybersecurity at the institutions under its supervision.

Reading Guide

This Good Practice is designed based on the following model, which consists of corresponding 'elements'.



[1] Nederlandse Corporate Governance Code 2022 pdf (overheid.nl)
Sleutelfuncties en adequate functiescheiding (dnb.nl)
Key functions with operational independence and proportional set-up (dnb.nl)

The Good Practice can be read from two perspectives:

1. **Summary** for directors, supervisory boards, key function holders and policymakers.
   For each element you will find a brief summary of the most important control measures with examples. The control measures are focused on the institution and the role of the board in implementing and supervising those control measures.
2. **Detailed** at the level of the control measures arising from market standards[2] with associated Good Practices.
   For each element you can click through to the control measures via a link. For readability, each control measure is included under one element of the model.
   Control measures can apply to different elements.

Under the *Contents* tab you can click on the different elements of the model. Tabs have been added for the Information Security Q&A and for the maturity model.

Reason for the update of the Good Practice Information Security (IS)

DNB structurally examines the quality of information security and cybersecurity within the financial sector.

In recent decades, DNB has seen an increase in potentially very harmful and professionalized cyber threats in the financial sector and beyond. DNB also sees a financial sector that, as a result of various forms of outsourcing and partnerships, operates more in chains, with the associated opportunities and risks for information security and cybersecurity.

The importance of knowledge and attention in the field of information security and cyber risks is endorsed at many boardroom tables. Administrative anchoring of this subject and organizing and maintaining knowledge among directors and internal supervision requires explicit attention.

Since the publication of the Good Practice Information Security 2019/2020, the European Supervisory Authorities, including EIOPA, have issued two relevant Guidelines in the field of information security and outsourcing[3]. In addition, the European Commission recently adopted the consolidated version of *Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations* (DORA)[4], which will apply from January 17, 2025.

In its supervisory investigations and the TIBER[5] program, DNB has come across many good examples of control measures that can mitigate risks in recent years.

Furthermore, various good examples and improvements of Good Practice Information Security have been provided by the various financial sectors. This was reason to update the 'Good Practice Information Security 2019/2020'. With this update, DNB conveys that information security and cybersecurity require permanent attention. This attention focuses on a strategic and administrative level to continue to ensure the improvement of the effectiveness of the control measures, which is in line with a constantly changing threat picture that institutions are confronted with.

What has changed compared to the Good Practice Information Security 2019/2020?

The Good Practice Information Security 2023 is as close as possible to the classification of 'Good Practice Information Security 2019/2020'[6].

The aforementioned guidelines from EIOPA have been incorporated into the management measures (controls) in the Good Practice Information Security 2023. The examples of the

[2] Relevant International Standards have been cited for the control measures in this Good Practice and associated Q&A, including EIOPA Guidelines on security and governance of information and communications technology and EIOPA Guidelines for outsourcing to cloud service providers, Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (DORA), Cobit (Control Objectives for Information and related Technology) of ISACA, ISO27000, the NIST Cybersecurity Framework SP 800-207, Zero Trust Architecture | CSRC (nist.gov) and The 18 CIS Critical Security Controls (cisecurity.org).

[3] EIOPA Guidelines on information and communication technology security and governance - European Union (europa.eu) and EIOPA Guidelines on outsourcing to cloud service providers - European Union (europa.eu)

[4] See EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu).

[5] Threat Intelligence Based Ethical Red-teaming TIBER: strengthening resilience against cybercrime (dnb.nl).

[6] For ease of recognition, the control measures are numbered in the same way.

controls have been updated. This involves market standards from the Zero Trust Architecture (NIST[7]) and the CIS Critical Security Controls[8], and DNB has collected practical examples from supervision.

In addition, this update contains the developments surrounding DORA[9] concerned; important aspects and principles of DORA have been incorporated. However, DORA's Regulatory technical standards (RTS)[10] had not yet been developed at a detailed level during the updating of this Good Practice Information Security 2023 and had therefore not yet been processed. The GP should therefore be seen as a supplement to the development around DORA and not as a (complete) replacement of DORA.

The most important changes are:

- a further deepening or tightening of the descriptions in relation to Good Practice information security 2019/2020.
- attention to a risk-based interpretation per control. This allows the institutions to apply increasingly far-reaching customization with regard to the design and implementation of their specific information security measures.
- attention to conducting a business impact analysis to assess the institution's exposure to serious business interruptions and their potential consequences.
- attention to digital operational resilience on short, medium and long term strategy that sets out how the Risk Management Framework is implemented.
- the role of the board of the institutions has been written down in a large part of the controls.
- attention to demonstrable follow-up tailored to them training and education by the board, supervisory board, supervisory board and key function holders to ensure the most important ICT risks and control measures for them institution to understand and address.
- attention to setting up an information security function by the institutions.
- additional examples for strengthening cooperation between institutions and other parties involved.
- attention to risks that may arise from 'Quantum Computing' and its possible control.
- clarification of the maturity levels.

A holistic approach

The Good Practice Information Security contains a system management measures for institutions to achieve a operational resilience framework in which the system of control measures an integrated approach with regard to the design and implementation of their specific information security measures is. In the Good Practice Information Security the various control measures depend of each other and strengthen each other. Risks can continue various control measures are mitigated and a control measure can cover various risks. The Good Information Security Practice ensures that the directors, supervisory boards, supervisory boards, the first, second and third lines, the chain partners and the service providers, to whom activities have been outsourced, work together. Various forms of assurance from external (ICT) Auditors with regard to Good Practice Information Security provide safeguards to directors, supervisory boards and councils of supervisory directors[11].

A *glossary* has been added for further clarification.

[7] SP 800-207, Zero Trust Architecture | CSRC (nist.gov).

[8] The 18 CIS Critical Security Controls (cisecurity.org)

[9] Digital Operational Resilience Act. EU requirements aimed at making ICT resilient to serious operational disruptions and cyber-attacks.

[10] Digital finance: Council adopts Digital Operational Resilience Act - Consilium (europa.eu).

[11] Examples include COS 3000 SOC2 reporting as well as a recently released standard from NOREA on the ICT report and the ICT Audit statement NOREA | Nieuw: de IT-Auditverklaring and Microsoft Word - NOREA Reporting on Management of ICT - v0.11 MASTER.docx

Scope

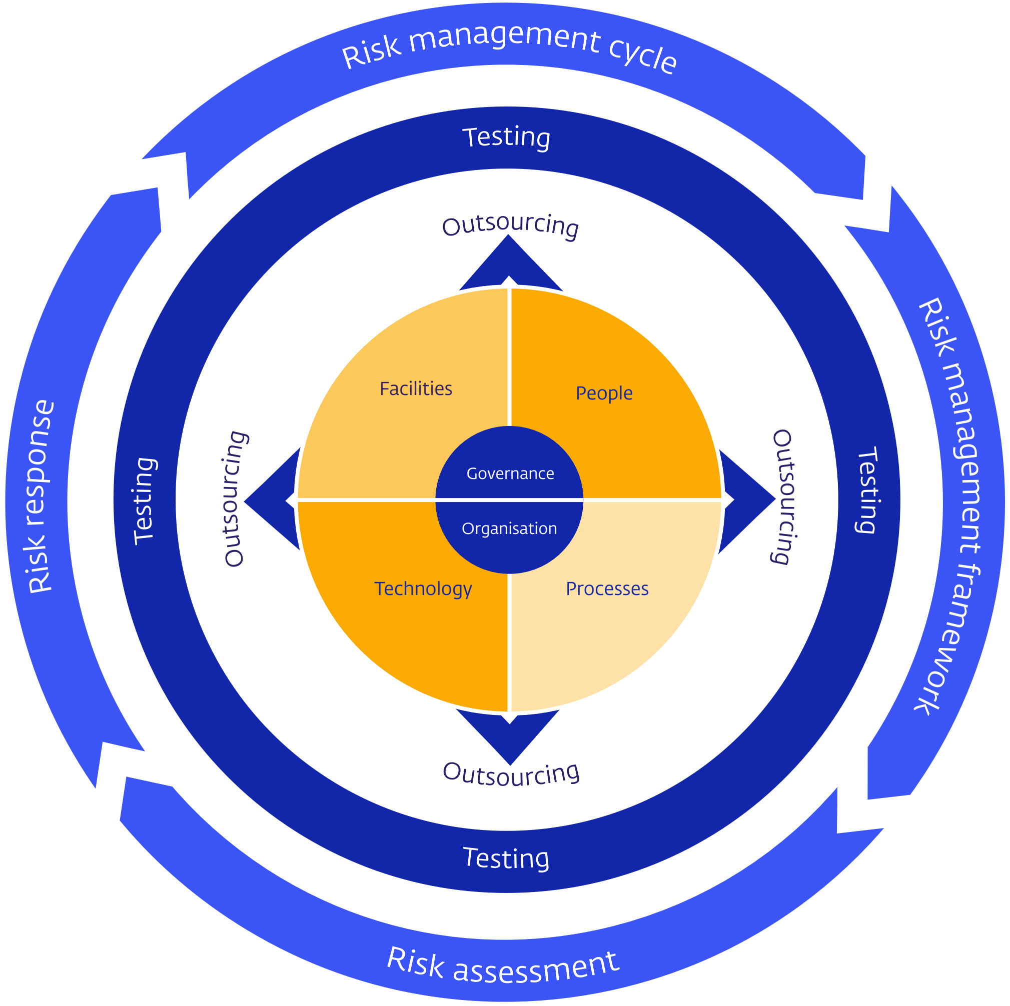
This Good Practice shows – without striving to be complete - what DNB means by a correct interpretation of the regulations in an honest and controlled manner of information security and cybersecurity. It's up to the institutions themselves for a control framework to implement that suits the nature, risk profile, size and complexity of the institution. This Good Practice does not rule out the possibility that an institution may require a different, possibly stricter application of the underlying rules, or that parts of the Good Practice are not relevant to an institution in question.

Disclaimer

For this Good Practice, these are non-mandatory recommendations. With the help of this Good Practice, DNB expresses its views on the observed or expected behavior in policy practice, which in our opinion constitutes a good application for information security and cybersecurity.

With this Good Practice, DNB aims to ensure that supervised institutions take into account what is stated therein, taking their own circumstances into account, without being obliged to do so. DNB Good Practices are indicative in nature and therefore do not rule out that institutions may require a different, stricter or otherwise, application of the underlying rules.

DNB Good Practice Information Security 2023



Q&A Information Security

Open Book Supervision

DNB structurally examines the quality of information security and cybersecurity within the financial sector. It does this, among other things, on the basis of periodic self-assessments of the institutions under its supervision. Until 2019, DNB indicated in the 'Q&A Information Security Assessment Framework for DNB research' what it pays attention to in its investigations as a guideline for completing these self-assessments. In 2019, the Q&A was replaced by the 'Q&A Information Security' and the 'Good Practice Information Security'. DNB has updated the Q&A and the Good Practice Information Security as of the end of 2023 (see under 'Downloads' on Open Book Supervision).

Question:

How do pension funds, premium pension institutions and insurers (hereinafter "institutions") meet the legal requirements under the supervision of DNB with regard to the continuous availability, integrity, confidentiality, authenticity, accountability, non-repudiation and reliability of automated data processing?

Answer:

Pursuant to art. 3.17 Financial Supervision Act, in conjunction with Article 20 of the Prudential Rules Decree and Article 143 of the Pension Act and Article 18 of the FTK Decree, institutions under the supervision of DNB have adequate procedures and measures to manage ICT risks. Managing ICT risks includes ensuring the integrity, continuous availability and security of automated data processing. In this context, adequate means that the procedures and control measures are based on the nature, scale and complexity of the risks of the institution's activities and the complexity of its organisational structure. This also includes procedures and control measures for those parts of automated data processing that have been (sub)outsourced. In this document, ensuring the integrity, continuous availability and security of automated data is briefly referred to as 'information security and cybersecurity'.

In order to comply with these provisions, institutions have taken control measures in the field of information security and cybersecurity based on a risk analysis. These control measures are not only aimed at technological solutions (*Technology*), they are also aimed at human actions (*People*), design of processes (*Processes*) and facilities (*Facilities*).

Institutions periodically and demonstrably evaluate the extent to which the control measures taken are effective in design, existence and operation to deal with the constantly changing risks in the field of information security and cybersecurity. They do this on the basis of a risk analysis – as part of their risk management process (*Risk Management Cycle*). Where necessary, control measures are improved or replaced by other control measures. The institutions set up their management (*Governance*) and organization (*Organisation*) to manage this. Institutions ensure, among other things, in line with the new corporate governance code 2022, the *DNB Q&A Key functions and adequate separation of functions* and *the DNB Q&A Key functions with operational independence and proportional set-up*, for an appropriate separation and independence of ICT risk management functions, control functions and internal audit functions. Furthermore, the board has demonstrably followed training and education tailored to them to understand the most important ICT risks and control measures for its institution (*People*).

Institutions also ensure that they are 'in control' in the field of information security when outsourcing (*Outsourcing*). In addition, they test (*Testing*) to what extent they as an institution are resilient to cyber threats.

In the Good Practice Information Security accompanying this Q&A, DNB offers tools with which institutions can practically implement the control measures in the areas of *Governance*, *Organization*, *People*, *Processes*, *Technology*, *Facilities*, *Outsourcing*, *Testing* and the *Risk Management Cycle*. This document contains various Good Practices (recommendations for control measures) that, in the opinion of DNB, properly fulfill the aforementioned requirements from Article 3.17 of the Financial Supervision Act, in conjunction with Article 20 of the Prudential Rules Decree and Article 143 of the Pension Act and Article 18 of the FTK Decree.

This Q&A was updated at the end of 2023. The answer has been expanded with passages about (sub)outsourcing, governance & key functions, training & education and a definition of information security & cybersecurity.

Should there be any discrepancies between the Dutch and the English version of this good practice document, the Dutch version shall prevail.

Relevant legislation and regulations

- Financial Supervision Act (Wft)
  - Article 1:1; definitions
  - Article 3:17 first paragraph; controlled and ethical business operations
  - Article 3:17 second paragraph; managing business processes and business risks.
- Prudential Rules Decree (Bpr)
  - Article 17; Financial institution means a payment company, clearing company, risk acceptance entity, credit company, premium pension company, insurer or branch
  - Article 20, second paragraph; have procedures and measures in place to ensure the integrity, continued availability and security of automated data.
- Pension Act
  - Article 143, first paragraph; safeguarding controlled and ethical business operations
- Compulsory Occupational Pension Scheme Act
  - Article 138, first paragraph; safeguarding controlled and ethical business operations*
- Decree on the Financial Assessment Framework for Pension Funds
  - Article 18; controlled business operations
- EIOPA
  - EIOPA Guidelines on Security and Governance of information and communication technology
  - EIOPA Guidelines for outsourcing to providers of cloud services
  - Regulation on Digital Operational Resilience
- Good practice for outsourcing by insurance companies published by De Nederlandsche Bank N.V. from August 2018
- Guidance on outsourcing by pension funds, publication of De Nederlandsche Bank N.V. of June 2014

* DNB is of the opinion that the corresponding applicability for these (professional pension funds) of the general standard regarding an organizational structure that ensures controlled and sound business operations, entails that these institutions also apply to the extent applicable - i.e. applied proportionately - must have procedures and measures in place to ensure the integrity, continued availability and security of automated data.

Glossary

Term	Definition
Cloud service provider	A service provider responsible for performing cloud services under an outsourcing agreement.
Application	A hardware/software system implemented to meet a particular set of requirements. The term application is generally used to refer to any part of software that can be executed. The terms application and software application are often used synonymously.
Availability	The property of accessibility and (timely) availability for use upon request for an authorized entity.
Management	The policy-making or administrative body of the institution.
Security incident	An individual event or a series of connected events that is not planned and that has or is likely to have an adverse effect on the continued availability, integrity, confidentiality and authenticity of ICT systems and services.
Security measure	A security measure or countermeasure designed to protect the continued availability, integrity, confidentiality and authenticity of information and to meet a set of defined security requirements.
Business Continuity Plan (BCP)	Documented information that guides an institution to respond to a disruption and continue, recover, and resume delivery of products and services in accordance with its business continuity objectives.
Cloud service	Services provided using cloud computing, i.e. a model for providing easy on-demand access via the network anywhere to a shared pool of configurable ICT resources (e.g. networks, servers, storage media, applications and services) that can be provided with minimal management effort or can be scaled up and down quickly through the intervention of service providers.
Cyber attack	An attack, via cyberspace, that targets the use of cyberspace by an institution for the purpose of disrupting, disabling, destroying or maliciously controlling a computer environment/infrastructure; or compromising the data or stealing information.
Cyber threat	Any form of malicious activity that attempts to collect, disrupt, degrade, or destroy information system resources or the information itself.
Cybersecurity	Preventing damage to, protecting and repairing computers, electronic communications systems, electronic communications services, wireless communications and electronic communications, including information contained therein, to ensure their continued availability, integrity, confidentiality, authenticity and non-repudiation.
Data breach	Access to or destruction, modification or release of (confidential) data at an institution, without this being the intention of that institution.
Service provider	A third party that provides a process, service or activity, or parts thereof, under an outsourcing agreement.
End User Computing	The ability for end users to design and implement their own information systems and thus view or edit data from the institution.
ICT asset	An ICT asset includes hardware, software systems or information and values of an organization.
ICT concentration risk	An exposure to individual or to multiple interconnected critical third-party providers of ICT services, which creates a certain degree of dependence on these providers such that the unavailability, failure or other type of shortcoming of the latter could affect the assets of a financial entity , and ultimately of the Union financial system as a whole, to fulfill crucial functions or to absorb other types of adverse effects, including large losses.
ICT infrastructure	All ICT facilities (hardware, middleware and software including applications, database, operating system, network, interface, etc.) that are required within an organization to support the various business processes.

Term	Definition
Information Security	Processes aimed at maintaining the continuous availability, integrity, confidentiality and authenticity of information and/or information systems. This may also involve other properties, such as accountability, irrefutability and reliability.
Integrity	The quality of accuracy, completeness and timeliness.
Critical or important system / process	If the relevant function, activity or system is essential for the business operations of the institution in the sense that without this function, activity or ICT system the institution would not be able to provide its services to its customers (policyholders, participants).
Crown Jewels analysis	A process for identifying those ICT assets that are most crucial for fulfilling an organization's mission or those assets that are seen as valuable by a criminal actor, such as specific Data, Applications, Assets and Services (DAAS).
Vulnerability	A weakness, sensitivity, or flaw in an active system, process, or control that can be exploited by a threat actor.
Legacy ICT system	An ICT system that has reached the end of its life cycle (end-of-life) and is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by the supplier or by an external ICT service provider, but that is still in use and supports the functions of the financial entity.
Metrics	Measuring instruments that, based on information collected from the company infrastructure and processes, can demonstrate whether the security measures are functioning as desired and mitigating the risk as expected.
Ransomware	Malicious software that encrypts the institution's data files, with the aim of later decrypting them in exchange for a ransom. Ransomware can also limit the availability or access to IT systems by encrypting system files that are essential for the proper functioning of the system.
Recovery Point Objective (RPO)	Recovery Point Objective. RPO is the aim to comply with the agreed maximum allowable amount of data loss after a disruption by the ICT department and/or a service provider. RPO is related to RTO, both are time intervals.
Recovery Time Objective (RTO)	Recovery Time Objective is the aim to meet the agreed recovery time after a disruption (e.g. a technical malfunction or cyber-attack) by the ICT department and/or an ICT service provider.
System / ICT system	Set of applications, services, ICT assets or other information handling components, including the operating environment.
Outsourcing	An agreement - in any form - between one institution and a service provider, whether supervised or not, on the basis of which this service provider, either directly or through sub-outsourcing, provides a process, a service or a carries out an activity that would otherwise be carried out by the institution itself.
Uncompromisable backup	A backup of your data that cannot be modified or deleted in any way, even by system administrators or by the users, applications or systems that created the data.
Confidentiality	The property that information is not provided to unauthorized persons, entities, processes or systems.

Points of attention for all controls

Risk based

Adequate management of information security means optimal effectiveness of the controls/management measures that an institution applies. This effectiveness is achieved, among other things, by having a good overview of one's own internal and external threat assessment. By analyzing the risks identified in the threat assessment[1], the institution periodically determines *its risk acceptance* and which control measures are effective for it and in what way. Responsibilities have been designated internally for monitoring sources of threat information by the institution and there are procedures in place for how threat information is received and shared internally for handling. The institution also periodically identifies which service providers are relevant to involve in monitoring and exchanging threat information and has made agreements with these parties for this purpose. This risk-based approach per control/management measure offers the institution the opportunity to apply increasingly far-reaching customization with regard to its information security and to adopt a proportionate approach. The focus on quality of control measures is preferred over quantity of control measures. Insight into the most important resources (*key assets*), the most important controls (*key controls*) and, where relevant, setting up metrics that can provide certainty to supervision that the most important control measures do indeed have the expected effect on risk reduction are essential.

Three lines Model

Financial institutions ensure appropriate separation and independence of ICT risk management functions, control functions and internal audit functions, in accordance with the rules of the 'three lines model' or a comparable internal risk management and control model.[2] For each control it is important to define the division of tasks and responsibility between the three lines: *How are the tasks and responsibilities divided between the first, second and third lines per control?*
The third line is positioned independently, reports and determines its own risk-based audit program.

Knowledge and competencies and Assurance

The importance of knowledge and attention in the field of information security and cyber risks is endorsed at many boardroom tables. Administrative anchoring of the entire system of controls and organizing and maintaining knowledge among directors and internal supervision requires explicit attention. The board, supervisory board, supervisory board and key function holders have demonstrably followed training and education tailored to them to understand and address the most important ICT risks and control measures for their institution.

Forms of assurance from external ICT Auditors of the individual controls and their context in the entire system of information security measures can also provide comfort with regard to the implementation of the Good Practice Information Security for outsourced activities to directors, supervisory boards and supervisory boards. Examples include Guideline 3000 reports, a SOC 2 report as well as a recently released standard from NOREA on the IT report and the ICT Audit statement[3].

Outsourcing

The institution is ultimately responsible for the control of the information security and cybersecurity risks of all its outsourced activities and functions in the outsourcing chain. This means that it is necessary for the institution to demonstrate the effective

[1] Risk = probability X impact, probability = threat X chance
[2] See: Key functions with operational independence and proportional set-up (dnb.nl) and Sleutelfuncties en adequate functiescheiding (dnb.nl)
[3] https://www.norea.nl/nieuws/nieuw-de-it-auditverklaring and Microsoft Word -NOREA Reporting on Management of ICT -v0.11 MASTER.docx

operation and implementation of all 58 controls monitors and checks, including where these partly or entirely take place at service providers or in the outsourcing chain.

Applicable to all 58 controls

When applying all 58 controls as described in this Good Practice Information Security, institutions explicitly address the following points.

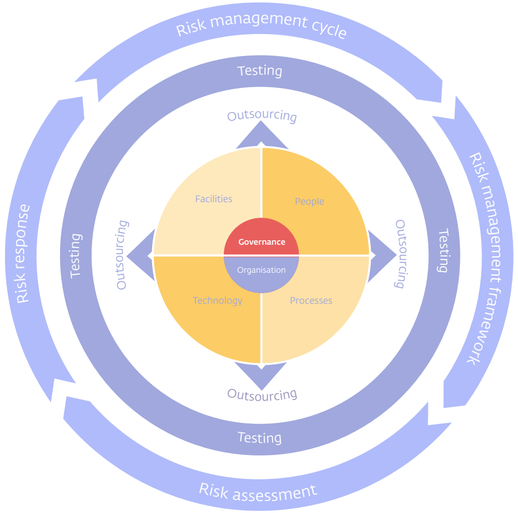
For **each** control:

- The effectiveness of the control is periodically optimized on the basis of the risk analysis from the internal and external threat assessment has emerged and metrics that demonstrate the effective operation of the controls. This also involved the experience gained with the relevant control and the placement of the control in the entire set of information security controls.
- Tasks, responsibilities and formal reporting lines of 1st, 2nd and 3rd line functions with regard to each control in the Good Practice have been assigned. This also includes outsourced activities.
- Makes the institution agreements with service providers, to whom activities have been outsourced, on a clear distribution of tasks and responsibilities. For each audit, the institution makes risk-based agreements with the service providers about the performance and level of internal control. These agreements also affect any subcontractors further down the chain.
- Does the institution demonstrably monitor and check compliance with the agreements made with and by its service providers with the correct scope and depth. It does this on the basis of reports or dashboards on compliance with the Service Level agreements and the level of internal control, including the effective operation in accordance with the set maturity levels (such as assurance and audit reports).
- When receiving assurance reports and/or audit reports, the institution determines that in terms of depth, scope and assurance level (such as Type I versus Type II; ISO certification versus ISAE/SOC) they correspond with those measures from the 58 named controls, of which part or all of the execution takes place at the service provider. If these reports do not cover the scope of the relevant measures, this may have consequences for the extent to which the institution can demonstrably demonstrate the effective operation (of at least 6 months) of one or more controls in the chain, with the result that the maturity level cannot be substantiated.
- The institution makes adjustments when its risk tolerances are exceeded by outsourcing, for example when deviations are visible in the reports or dashboards (see *Risk Management cycle*) or when the threat landscape requires this.

When carrying out self-assessments and providing evidence for determining the maturity levels, the institution takes into account per control how it has implemented the points of attention with regard to the topics ‘Risk-based’ and the ‘Three lines model’ or a comparable internal risk management and control model.

With regard to the points of attention for outsourcing, you can choose to determine the impact of the outsourcing per control. On this basis, the service provider’s control measures can be taken into account in determining the maturity level of the control. Furthermore, it is good practice to demonstrate in a separate document for the most important service providers which maturity levels have been determined with regard to the controls on which the outsourced activities have an impact.

Governance



In this section you will find a brief summary of the control measures resulting from market standards that belong to the 'Governance' element with associated Good Practices.
At the end of this section there are 'links' on which you can click through to the control measures.

DNB understands this element as

Governance is about providing strategic, tactical and operational management of information security and cybersecurity, based on a risk analysis, in accordance with the institution's strategy, the goals of the ICT strategy, its risk appetite and legislation and regulations. The nature, size and complexity of the institution are taken into account.

Good examples of Governance control measures for the institution

In the *Governance* element, an institution creates a digital operational resilience strategy in the short, medium and long term based on a current risk analysis and threat assessment. In line with the digital operational resilience strategy, the information security policy is also periodically determined, implemented and monitored, including the resulting information security plan. The policy includes a description of the key roles, responsibilities and formal reporting lines for information security management. The policy sets out the budget, personnel, process and technology requirements related to information security, with employees at all levels responsible for ensuring the institution's information security.

The institution has paid explicit attention to resilience against cyber threats in its policy. The policy has been operationalized in preventive, detecting, corrective and repressive management measures. The institution monitors relevant developments in the field of information security and cybersecurity, including developments in the field of Quantum technology, AI, blockchain and technological knowledge. The institution ensures that business processes and ICT systems are set up according to an information architecture established by the institution. This Security Architecture provides insight into how the ICT systems and data collections support the strategy of the institution and its processes. All relevant ICT and security risks to which the institution is exposed have been identified and measured. The identified business processes and activities, business functions, roles and assets (such as information and ICT assets) are then classified according to how critical they are.

The institution uses a classification scheme[4] on the basis of which relevant control measures have been taken for, for example, access, encryption, storage and retention of data.

The institution works according to accepted (technical) standards in the field of information security and cybersecurity.

[4] ICT systems and data are divided into categories based on a risk analysis that indicates the degree of confidentiality, integrity and continuous availability (CIA).

Role of the board in the implementation of these control measures

The board of the institution is ultimately responsible for adequate governance and ensures that all elements of information security and cybersecurity have been controlled. For example, you can consider the following aspects:

- Based on a risk analysis and threat assessment, the board determines a digital operational resilience strategy for the short, medium and long term.
- The board has the ultimate responsibility to periodically determine the information security policy, including the resulting information security plan, in line with the digital operational resilience strategy.
- The board oversees and takes responsibility for ensuring that the established information security policy and information security plan are implemented, monitored and adjusted where necessary.
- Within the *Risk Management Cycle*, the board then ensures that the board periodically examines the extent to which the institution's information security and cybersecurity risks fit within the board's risk appetite. It can be considered to what extent an effective mix of control measures – *People, Processes, Technology and Facilities* – has been taken to manage the institution's risks.
- The board ensures that the institution's governance system, in particular the risk management and internal control system, adequately manages the institution's security risks.
- The board and risk management are familiar with the most important developments and take the risks and opportunities into account in their decision-making or risk assessment.
- The board ensures that the institution monitors that its service providers comply with agreements in accordance with the information security policy and - if applicable - the implementation of the information security plan.
- The board monitors the results of the relevant metrics that reflect the proper functioning of the control measures and responds adequately if they deviate with a possible material impact on the business risk.

Control measures:

> 1.1 Information Security plan

> 1.2 Information Security policies and procesmanagement

> 2.1 Information Security Architecture

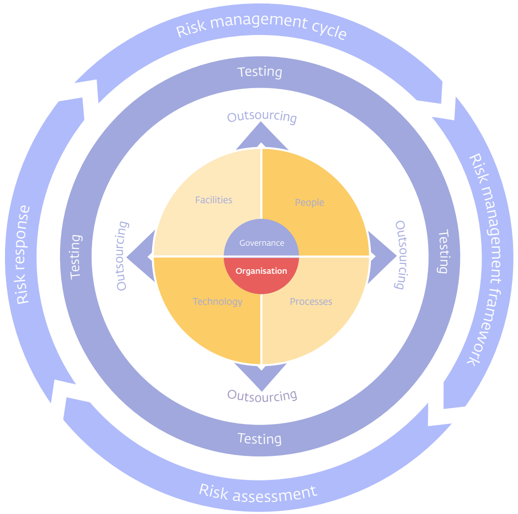
> 2.2 Data classification scheme

> 3.1 Risks and opportunities of future trends and regulations

> 3.2 Technical standards

← →

Organisation



In this section you will find a brief summary of the control measures resulting from market standards and Good Practices that belong to the 'Organisation' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

The tasks regarding information security and cybersecurity are clearly assigned within the institution and activities in this area are in accordance with the institution's strategy, its risk appetite and with legislation and regulations.

Good examples of Organisation control measures for the institution

In the *Organisation* element, the institution documents and formalizes the roles and responsibilities for the risk management and information security function. The institution has assigned tasks, responsibilities and authorities with regard to information security at all levels in the organization. For example, the institution has drawn up and communicated rules of conduct stating that employees handle information carefully (such as safely handling passwords, e-mail and a clean desk policy).

The institution shall, within its governance system and in accordance with the principle of proportionality, establish an information security function, with responsibilities assigned to a specific employee. The institution ensures that the independence and objectivity of this information security function is ensured by appropriately separating it from responsibilities regarding ICT activities and business operations. The information security function reports to the board.

The ownership of all data and information systems that the institution uses in its business operations are clearly assigned. The institution has controlled access to data and information systems through access rights. The principles of separation of duties are used here, based on the design of the administrative organization/ internal control of the institution.

For example, based on a risk-based approach, the institution has not only mapped out the desired separations of functions per application, but also emphatically per process if this process is supported by multiple applications. This prevents separations of functions at process level from being broken, even though they are set up in accordance with the requirements for each individual application in the process. At the same time, institutions are reducing high-privilege accounts to the minimum necessary number. With such an approach, unwanted mixtures of functions (toxic combinations) and the associated risks can be reduced.

Role of the board in the implementation of these control measures

The board of the institution is ultimately responsible for an adequate organization of tasks, responsibilities and authorities and ensures that all elements of information security and cybersecurity have been controlled. For example, you can consider the following aspects:

- The board has clearly assigned tasks and responsibilities in the field of setting up, managing and monitoring information security and cybersecurity.
- The board ensures that unwanted combinations of functions (toxic combinations) and the associated risks are reduced by the institution.
- Based on the risk profile of the institution and the risk appetite of the board, the organization may have sufficient capacity, knowledge and experience to fulfill these tasks and responsibilities.
- The board actively and visibly promotes the importance of information security and cybersecurity for the institution and its service providers.
- The board ensures that the institution monitors that its service providers comply with agreements regarding the allocation of tasks and responsibilities for information security and cybersecurity, ownership of data and information systems and separation of functions in their organizations.
- The board ensures that the CISO can act sufficiently autonomously, has sufficient resources and has direct lines of communication to the board.

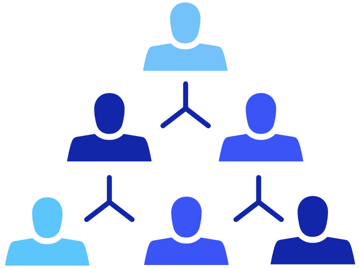
Control measures:

> 5.1 Responsibility for risk, security, compliance and Information Security function

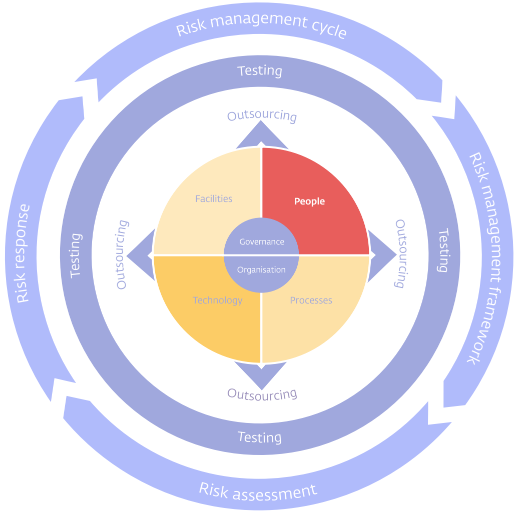
> 5.2 Management of information security and tasks of the information security function

> 6.1 Data and system ownership

> 7.1 Segregation of duties



People and Knowledge



In this section you will find a brief summary of the most important control measures resulting from market standards and Good Practices that belong to the ‘People’ element.
At the end of this element there are ‘links’ on which you can click through to the control measures.

DNB understands this element as

All employees, external hires and service providers are known with the institution’s information security policy, know their responsibilities and can work according to this policy and the institution’s risk tolerances.

Good examples of People control measures for the institution

The importance of knowledge and attention in the field of information security and cyber risks is endorsed at many boardroom tables. Administrative anchoring of the entire system of controls and organizing and maintaining knowledge among directors and internal supervision requires explicit attention.

The human factor is very decisive for the management of information security and cybersecurity risks. At *People* the institution appoints employees with knowledge of information security and cybersecurity that matches the ambition and risk profile of the institution and pays attention to maintaining this.

The institution invests in maintaining the knowledge level and competencies of its employees through education and training. Basic knowledge of information security and cyber threats is widely shared within the institution. In-depth knowledge is provided to IT managers and information security specialists. The institution pays explicit attention to cyber threats through security awareness programs. Attention is paid to the importance of (continuous) education in the field of cybersecurity.

The institution shares knowledge about cyber threats with other institutions and agencies. The institution participates, for example, in forums in which cyber threats and cyber-attacks are confidentially shared, such as the sectoral Information Sharing and Analysis Centers (ISACs).

The institution further determines on the basis of a risk analysis where its dependence on individuals with knowledge of information security and cybersecurity exceeds its risk tolerance. The institution takes control measures to limit excessive dependence on individuals (key person risk).

Prior to employment, the institution screens internal and external employees depending on the risk profile of the position of the employee. This screening is periodically repeated during the employment relationship or long-term hiring period. In the event of job changes, access rights that the employee or temporary worker may no longer have on account of the (new) job or upon termination of the (old) job are revoked as quickly as possible.

In the case of high-impact incidents, the institution uses root cause analyses to identify the extent to which the culture or behavior of certain employees (for example carelessness, dissatisfied (disgruntled) employees) within certain departments has contributed to the incident. Mitigating control measures are implemented based on this analysis.

Role of the board in the implementation of these control measures

The board of the institution is ultimately responsible for an adequate organization of tasks, responsibilities and authorities and ensures that all elements of information security and cybersecurity have been controlled. For example, you can consider the following aspects:

- The board, supervisory board and key function holders have demonstrably followed training and education tailored to them to understand and address the most important ICT risks and control measures for their institution.
- The board shows good exemplary behavior with regard to awareness of risks in the field of information security and cybersecurity and compliance with procedures that safeguard information security (tone-at-the-top).
- So-called 'management overrides' of existing processes and procedures by the board and senior management are avoided where possible.
- The board ensures that the institution monitors that its service providers comply with agreements regarding the personnel aspects of information security and cybersecurity as mentioned above.

Control measures:

> 8.1 Personnel recruitment and retention

> 8.2 Personnel competencies and culture

> 8.3 Dependence upon individuals

> 8.4 Personnel clearance procedures

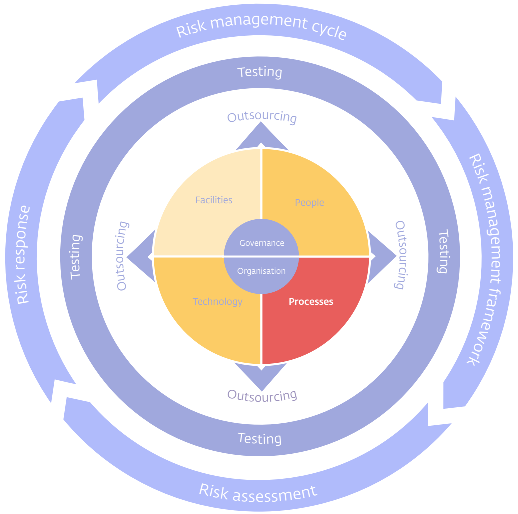
> 8.5 Job change and termination

> 9.1 Knowledge transfer to end users

> 9.2 Knowledge transfer to operations and support staff

> 9.3 Employee awareness

Processes



In this section you will find a brief summary of the most important control measures arising from market standards and Good Practices that belong to the 'Processes' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

Processes provide direction for controlled business operations and are necessary for managing risks in the field of information security and cybersecurity.

Good examples of Processes control measures for the institution

In the *Processes* section, it is important that the institution develops and maintains an ICT continuity plan, based on a series of different scenarios. The aim is to limit the impact of a major disruption on key business functions and processes and to promote the undisturbed continuation of information security functions during disruptions or cyber-attacks. The institution aims to limit the damage from security incidents, including cybersecurity incidents, as much as possible and to prevent recurrence. To this end, the institution has a formalized policy for incident management, which includes an escalation procedure and escalation criteria. The institution ensures that it takes effective crisis communication management measures. Cybersecurity incidents are reported to the authorities in accordance with applicable rules. Solutions for incidents are regularly analyzed to improve processes and IT systems. An example of this is setting up a Computer Security Incident Response Team (CSIRT) within the institution. As part of robust business continuity management, the institution conducts a business impact analysis to assess the institution's exposure to major business disruptions and their potential consequences, both quantitatively and qualitatively, using internal and/or external data and scenario analysis . The business impact analysis takes into account how critical the identified business processes and activities and their interdependencies are. The institution ensures that their ICT systems and ICT services are designed and tailored to their business impact analysis.

The business impact analysis and the ICT continuity plan include various scenarios that take into account the continuity of security measures and the undisturbed continuation of information security functions during disruptions and cyber-attacks. Crisis management has been set up, including the associated communication protocols. Alternative processing and recovery options for all critical ICT services are available in the ICT continuity plan. In the event of a disruption or emergency, and during the implementation of business continuity plans, the institution ensures that it takes effective crisis communication measures whereby all relevant internal and external stakeholders, including relevant supervisory authorities, are informed in a timely manner.

The institution implements changes in a controlled manner with the aim of preventing these changes (intentionally or unintentionally) from leading to a lower information security level, leading to disruptions in business processes and/or negatively affecting data integrity. Changes, including security patches, in ICT applications, ICT infrastructure, ICT processes and critical system settings follow a standardized and controlled path, whereby changes are registered (audit trail), approved and evaluated. This also applies to ICT systems that are developed and managed by end users. The institution maintains a register of end user computing applications that support critical business functions or processes.

The institution establishes and maintains criteria for protecting test data. Test and production data are properly separated from each other. Changes are tested according to a test plan that includes acceptance criteria; also for security and ICT performance.

The institution safeguards the quality of the ICT management processes. The institution implements and maintains procedures with regard to, among others:

- configuration (keeping track of the ICT systems that the institution uses and the various parameters therein),
- back-up and restore from systems and data,
- availability of (back-up) data at an external location,
- the storage, archiving and destruction of data in accordance with laws and regulations,
- the deletion, transfer, processing and provision of sensitive data,
- compliance with current laws and regulations,
- access to the institution's information systems and data.

The institution periodically obtains independent assurance about the functioning of the control measures. For example, in the form of a report from the internal or external auditor in which an opinion is given on the design, existence and operation of control measures during a certain period.

The institution has procedures for logical access control or logical security (identity and access management). Access (remote or otherwise) to critical ICT systems is only granted according to the need for information and when strong means of authentication are used.

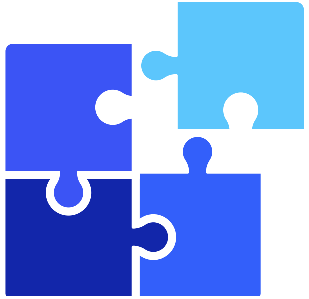
Role of the board in the implementation of these control measures

The board of the institution is ultimately responsible for ensuring and/or checking that the strategy and the overall ICT security plan are in line with the guidelines of the board and other company procedures. For example, you can consider the following aspects:

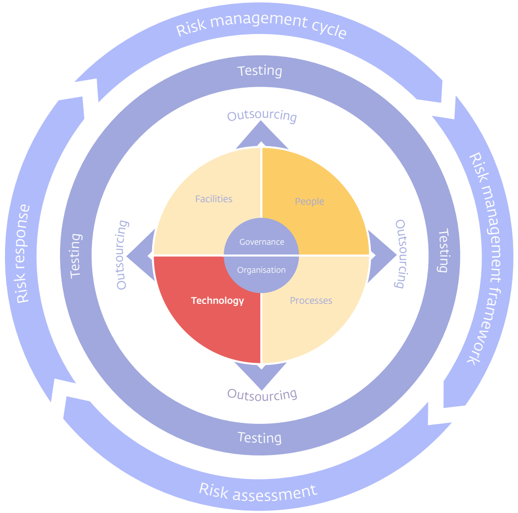
- The board is responsible for establishing and approving a business impact analysis and a resulting continuity plan to limit the impact of a major disruption on key business functions and processes.
- The board checks annually whether the business impact analysis and the continuity plan are up to date. The board ensures that important changes in ICT systems or services are immediately incorporated into the continuity plan.
- The board is involved in drawing up the continuity plans and actively participates in testing the ICT continuity plan.
- Security monitoring reporting provides the institution with insight into the nature of both operational and security incidents to enable management to make appropriate decisions.
- The board facilitates independent supervision and periodically approves internal (ICT) audit plans, ICT audits and material changes thereto.
- The institution provides the board with insight into the proper functioning of the control measures by generating metrics where relevant that are fed with data from the infrastructure and processes.

Control measures:

- > 10.1 Change standards and procedures
- > 10.2 Impact assessment, prioritisation and authorisation
- > 10.3 Test environment
- > 10.4 Testing of changes
- > 10.5 Promotion to Production
- > 11.1 ICT Business impact analysis and ICT Continuity plans
- > 11.2 Testing of the ICT Continuity plan
- > 11.3 Uncompromisable backup storage
- > 11.4 Restoration
- > 12.1 Storage and retention arrangements
- > 12.2 Disposal
- > 12.3 Security requirements for data management
- > 13.1 Configuration repository and baseline
- > 13.2 Identification and maintenance of configuration items
- > 15.1 Security incident policy and definition
- > 15.2 Incident escalation
- > 16.1 Security testing, surveillance and monitoring
- > 16.2 Monitoring of internal control framework
- > 16.4 Evaluation of compliance with external requirements
- > 16.5 Independent assurance
- > 17.1 Identity & Access Management
- > 17.2 User account management



Technology



In this section you will find a brief summary of the most important control measures resulting from market standards and Good Practices that belong to the 'Technology' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

Information security and cybersecurity are partly shaped by taking technical control measures.

Good examples of Technology control measures for the institution

In the *Technology* element, technical control measures are designed in such a way that they ensure a high level of continuous availability, integrity, confidentiality and authenticity. The institution's risk analyzes take current cyber threats into account. Examples include the CIS[5] Top 18, threat analyses from the NCSC[6] and ENISA[7], and the results of penetration testing and ethical hacking. The institution ensures that the maintenance of the ICT infrastructure and ICT applications is planned and structured, in line with the change management procedures and the life cycle management process of the institution.

For example, the institution ensures that the technological obsolescence of its ICT infrastructure and ICT applications remains within its risk tolerance limits and that security updates are applied. DNB also ensures that institutions have an idea of which ICT infrastructure and ICT applications their business processes depend on and to what extent the ICT systems are vulnerable to cyber-attacks. An analysis is made of the network to see where far-reaching network segmentation of the network is useful, such as around the 'crown jewels' of the institution.

The institution has implemented preventive, detective and corrective control measures to protect ICT systems against cyber-attacks, such as viruses, malware, ransomware, spyware and DDoS attacks. With regard to preventive control measures, DNB ensures that the institution applies up-to-date technical security measures (such as firewalls, network segmentation and intrusion detection) and has set up associated management procedures to limit access to the ICT infrastructure to authorized persons. For example, the institution applies modern firewall technology that is in line with standards such as GovCert[7] and ISO/IEC[8].

The institution has further formulated policy regarding the sharing of confidential information. A risk analysis has been made so that the security measures are applied proportionately. Examples are that confidential data is recorded encrypted on laptops and that the Data Loss Prevention institution applies software to control

[5] Center for Internet Security. See https://www.cisecurity.org/controls/cis-controls-list.
[6] Nationaal cybersecurity Centrum. See https://ncsc.nl
[7] European Union Agency for Network and Information Security. See https://www.enisa.europa.eu/
[8] International Standards Organisation. See https://www.iso.org

outgoing messages. The institution ensures that the management of cryptographic keys takes place in a controlled manner, also with regard to outsourced activities.

The risks arising from outdated or unsupported ICT assets are identified, assessed and mitigated. Decommissioned ICT assets are processed and disposed safely. To this end, a plan is drawn up that is coordinated with all business units involved.

The institution ensures that an increased focus on customer experience and time-to-market does not lead to the implementation of infrastructural (security) measures and investments in technological developments being postponed (too) long.

Role of the board in the implementation of these control measures

The board of the institution is ultimately responsible for developing and implementing the ICT strategy. For example, you can consider the following aspects:

- The board ensures that it is periodically informed about the risks in the field of information security and cybersecurity and about new technological developments (which may entail both opportunities and risks in the field of information security and cybersecurity).
- As a director, you can take these risks into account within the Risk Management Cycle, see also the relevant element in the model.

Control measures:

> 18.1 Infrastructure resource protection and availability

> 18.2 Infrastructure maintenance

> 18.3 Cryptography and Cryptographic key management

> 18.4 Network Security

> 18.5 Protection of sensitive data

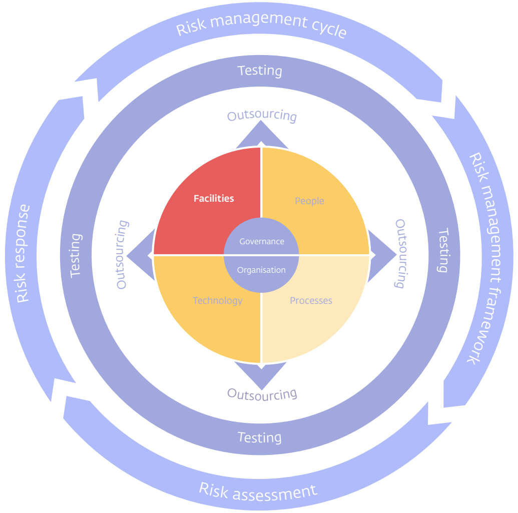
> 19.1 Malicious software prevention, detection and correction

> 19.2 Vulnerability Management

> 19.3 Application Maintenance

> 20.1 Protection of security technology

Facilities



In this section you will find a brief summary of the most important control measures resulting from market standards and Good Practices that belong to the 'Facilities' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

DNB understands this element as, among others, that access to information is also physically secured, such as control measures that protect access to sensitive locations such as the site, office buildings, data centers, cabling and remote work locations and limit (environmental) threats (such as power outages, fire and water damage).

Good examples of Facilities control measures for the institution

In the *Facilities* section, the institution has established, documented and implemented physical security measures in line with its risk profile with regard to:

1. the physical security of office buildings, sites and critical ICT infrastructure locations, such as data centers and server rooms against environmental hazards.
2. gaining access to buildings and sites that are important for carrying out business processes.

This includes appropriate management measures to protect against threats in proportion to the importance of the buildings and the critical nature of the activities or ICT systems located in these buildings.

An example here is that the institution also takes control measures to protect the security systems themselves. This could include additional physical access security. The institution regularly monitors the effectiveness of physical access security measures and reports on the results to senior management. An example of this is that the institution has the physical access security measures checked by a "Mystery Guest".

Role of the board in the implementation of these control measures

The role of the director is particularly important in determining, implementing and monitoring policy. For example, you can consider the following aspects:

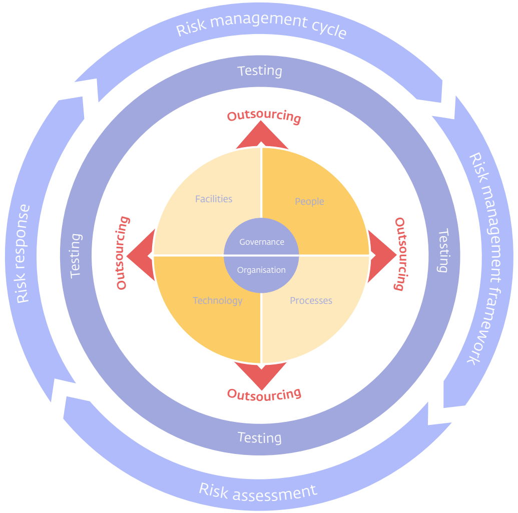
- The board shows that it attaches importance to adequate physical access security and implements the necessary control measures based on the risk profile of each location.
- The board is informed about this and calls the organization to account if there are gaps (tone at the top).

Control measures:

> 21.1 Physical security measures

> 21.2 Physical access

Outsourcing



In this section you will find a brief summary of the most important control measures resulting from market standards and Good Practices that belong to the 'Outscourcing' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

DNB sees that institutions are increasingly outsourcing critical or important business processes such as ICT, asset management, customer, pension, policy and financial administrations (*Outsourcing*). The benefits of outsourcing are also offset by risks that an institution exposes itself to. In the context of information security and cybersecurity, this is, for example, the undesirable handling of the service provider with confidential data of the institution. There is also a risk that the security and continuity of confidential data and systems is not in accordance with internal policy as a result of under-outsourcing by the service provider.

Good examples of Outscourcing control measures for the institution

For all control measures in this Good Practice, when activities/systems are outsourced, the institution remains ultimately responsible for information security and cybersecurity. This means that the institution has set up a process for each control measure that safeguards at least the following:

- the institution makes agreements with service providers to whom activities have been outsourced about a clear division of tasks and responsibilities. **For each control measure**, the institution makes risk-based agreements with the service providers about the performance and level of internal control. These agreements also affect any subcontractors further down the chain.
- the institution periodically and demonstrably monitors and checks compliance with the agreements made with the correct periodicity, scope and depth. It does this on the basis of reports or dashboards on compliance with the Service Level agreements and the level of internal control (such as assurance and audit reports) and, if necessary, decides to conduct its own audits or inspections at the service providers.
- the institution makes adjustments when deviations are visible in the reports or dashboards (see Risk Management Cycle) and, if necessary, decides to conduct its own audits or inspections of the service providers.

These three control measures show as a good example that the institution agrees on specific performance and risk criteria with its service providers, that these agreements are monitored and that they are reported to stakeholders. Accountability reports from service providers are analyzed by the institution to identify trends and developments and, if necessary, adjust services.

During the contract preparation phase, the institution pays attention to how the service provider will continue to comply with contractual obligations, legislation and regulations and that the outsourcing does not hinder supervision. During the contract preparation phase, the institution also prepares a risk analysis together with its service providers and determines how it will deal with any residual risks. This analysis included risks at parties to which services have been outsourced and an exit plan was agreed with agreements on a controlled termination of the services. This includes determining how the institution's (backup) data will be deleted after exit. Sub-outsourcing is in scope here.

The institution also has a thorough and well-documented incident management process, including the responsibilities of all parties involved, for example by establishing a cooperation model in the event of actual or suspected incidents.

Role of the board in the implementation of these control measures

The institution's board is ultimately responsible for the effective management of outsourced activities by making contractual agreements, monitoring the extent to which those agreements are complied with and making timely adjustments when the agreements are deviated from. For example, you can consider the following aspects:

- The board approves and periodically reviews the outsourcing policy and also discusses the outsourcing strategy from the perspective of information security. Based on the evaluation, you can adjust the outsourcing policy if necessary or you can direct the adjustment or termination of existing outsourcing contracts.
- When making choices in the outsourcing strategy, the board takes into account the associated risks in the field of information security and the way in which these risks are continuously managed.
- Through an analysis, the institution has an up-to-date picture of the inherent information security risk of all outsourcing and/or outsourcing chains. The institution monitors which control measures have been taken in accordance with the information policy and which demonstrably work. The board has been and will be informed of this.

Control measures:

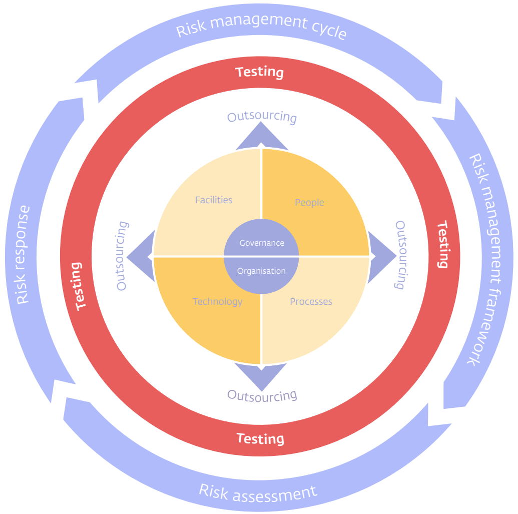
> 14.1 Third party and supplier services management

> 14.2 Third party and supplier risk management

> 16.3 Internal control at third parties

← →

Testing



In this section you will find a brief summary of the most important control measures resulting from market standards and Good Practices that belong to the 'Testing' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

Research shows that conducting Security testing is effective for continuously improving information security and cyber resilience of institutions. Security Testing can focus on various elements from the model of this Q&A. For example, a test can focus on weaknesses in the infrastructure (*Technology*), but also on human behavior and actions (*People*) or on weaknesses in access to buildings (*Facilities*). The scope of Security testing can focus on the internal organization, but can also include critical or important outsourcing.

Good examples of Testing control measures for the institution

The institution implements a testing program linked to the risk management framework, involving a variety of different information security evaluations, assessments and tests to ensure effective identification of vulnerabilities in the ICT systems and services. Based on a risk analysis and current cyber threats, it is determined which types of security tests are carried out as well as the scope and depth of those tests. The risk analysis takes into account current cyber threats, the changing landscape of ICT risks, any specific risks to which the institution is or could be exposed and how critical the information assets and services provided are.

The nature and frequency of these tests depends on the risk profile of the institution, with testing of critical ICT systems and vulnerability scans being carried out annually. Furthermore, security testing is performed in the event of changes to infrastructure, processes or procedures, and if changes are implemented due to major operational or security incidents, or due to the release of new or significantly modified critical applications.

An example is that the institution can or has various types of security tests carried out, including pen tests aimed at the security of infrastructure and applications, red teaming, testing physical security and testing human actions in relation to information security and cybersecurity. These tests can be carried out by internal or external hired parties.

The institution verifies that the party carrying out the security tests is sufficiently equipped to carry out such tests (do they have the correct experience, certifications and references?). An example here is that the institution draws up *an annual plan* based on a risk analysis for the types of security tests to be carried out.

Role of the board in the implementation of these control measures

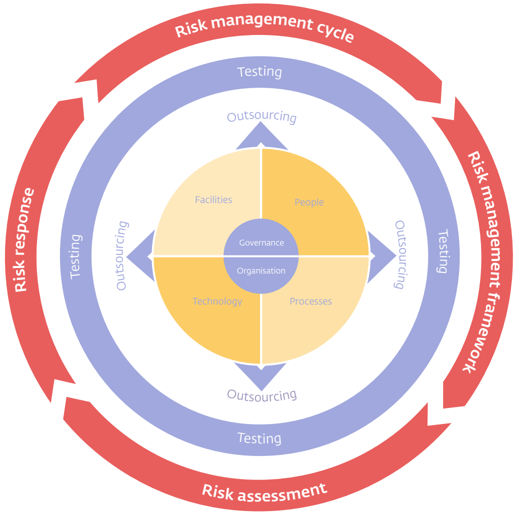
The board of the institution is ultimately responsible for directing, monitoring and carrying out Security testing. For example, you can consider the following aspects:

- The board makes sufficient resources available to carry out the test program, discusses the most important outcomes of the test program and ensures that procedures are in place to ensure that security test results are monitored, evaluated and prioritized.
- The board ensures that any identified vulnerabilities are mitigated without delay with clear deadlines, taking into account how critical the vulnerabilities and/or the affected ICT system are.

Control measures:

> 22.1 Penetration testing and ethical hacking

Risk management cycle



In this section you will find a brief summary of the most important control measures resulting from market standards and Good Practices that belong to the 'Risk Management Cycle' element.
At the end of this element there are 'links' on which you can click through to the control measures.

DNB understands this element as

The *Risk Management Cycle* applies to all elements of the model. It is important that the institution regularly identifies and analyzes the risks relevant to it in the field of information security and cybersecurity. Based on this risk analysis, the institution determines its response, takes control measures to limit risks and (temporarily) accepts any residual risks. Accepted residual risks are periodically reevaluated and offered for acceptance again.

Good examples of Risk Management Cycle control measures for the institution

In the Risk Management Cycle element, the institution has safeguarded the management of risks with regard to information security and cybersecurity by implementing an ICT Risk Management Framework that is in line with its own digital operational resilience strategy. This framework is based on a Plan-Do-Check-Act cycle, which is regularly reported to the board. The institution uses clear definitions for information security and cybersecurity in its *ICT Risk Management Framework*, which are derived from market standards such as NIST, ISO and Cobit. The definitions are applied consistently within all documents and reports. An example is that current cyber threats such as malware, ransomware, DDoS attacks and phishing are part of the institution's ICT Risk Management Framework.

The institution regularly and at least once a year and with every major change in the infrastructure or relevant processes, carries out a risk analysis based on qualitative and quantitative methods, in which current cyber threats are analyzed and prioritized. To this end, the institution maps out and regularly updates its business processes and activities, business functions, roles and assets (such as information and ICT assets) to determine their importance for ICT and security risks and to determine their mutual dependencies. She also explicitly takes her legacy systems into account.

As important input for the risk analysis, the institution's specified threat assessment is first mapped or updated.

Where necessary, the institution takes additional control measures. In addition, the institution makes explicit which risks are formally accepted. Control measures that no longer work effectively are adjusted, replaced by other control measures or phased out.

The institution draws up a 'risk action plan' for unacceptable risks that details the risk response. The risk action plan is approved by the management level that is appropriate to the nature and extent of the residual risks. An example here is that the institution has made explicit for current cyber threats which risks are formally accepted and for which residual risks additional control measures are necessary.

The institution ensures that the 1st, 2nd and 3rd lines are actively involved in the creation, implementation, maintenance and evaluation of the Risk Management Cycle.

Assurance by (ICT) Auditors with regard to the individual controls and their context in the entire system of Information Security Measures can provide assurance with regard to the Good Practice Information Security to directors and supervisory boards.

Role of the board in the implementation of these control measures

The board of the institution is ultimately responsible for directing, implementing and eliminating the control measures resulting from the Risk Management Cycle. For example, you can consider the following aspects:

- The board has overall responsibility for establishing and approving a short, medium and long-term digital operational resilience strategy that sets out how the Risk Management Framework is implemented.
- The board has had a risk management cycle set up for this purpose and is regularly informed about information security risks and cyber threats.
- The board evaluates the result of the ICT Risk Management Framework annually and in the event of major ICT-related incidents via a written report. Current developments and risks are taken into account. The ICT Risk Management Framework is regularly subject to (internal) audits. Insurers process risks in the ORSA, pension funds in the ERB and banks in the ICAAP.
- The board makes sufficient resources available to take effective control measures based on the risk profile of the institution and the risk appetite of the board. The board periodically checks to what extent the risks that the institution faces in the field of information security and cybersecurity are within the board's risk tolerances. Also in the event that critical or important work has been outsourced to service providers.
- The board periodically considers the extent to which an effective 'mix' of control measures - people, processes, technology and facilities - has been taken to mitigate the institution's risks in the field of information security and cybersecurity (from a comprehensive approach).

Control measures:

> 4.1 ICT Risk Management framework

> 4.2 Risk assessment

> 4.3 Maintenance and monitoring of a risk action plan

Maturity Model

An institution can use a self-assessment to determine to what extent the management of information security and cybersecurity is at the required level. To determine this level, DNB uses a maturity model based on definitions of standards known in the market such as COBIT[9].

Financial institutions are demonstrably 'in control'. In the model used by DNB with 58 control measures, this corresponds to at least a maturity level of '3': demonstrable effectiveness for a minimum of 6 months for 55 control measures. For the Risk Management Cycle controls, concerning controls #4.1, #4.2 and #4.3, this corresponds to a maturity level of '4'.

When completing the *self-assessment*, the institution takes into account the definitions in the table below when assigning the maturity levels. The first column contains the maturity levels from 0 to 5. The second column contains the definitions of the maturity levels that DNB uses in its supervisory investigations. The third column contains criteria to further clarify the maturity level.

The criteria mentioned at levels up to and including 3 'defined' (design, existence and operation) mainly concern the demonstrability and effectiveness of the control itself. The criteria for levels 4 and 5 relate in particular to the demonstrability and effectiveness of the system of controls and the role that specific control plays in it.

The criteria for the maturity levels also apply to the control measures that are implemented in the outsourcing chain.

To determine the maturity level, the institution has determined the tasks and responsibilities of the first, second and third lines.

[9] In the old GP Information Security, DNB followed as closely as possible the definitions that DNB has been using since 2014 and which are derived from "CobiT 4.1 Research, 2007, Appendix III—Maturity Model for Internal Control, page 175".

←
→

Level:	Defenition of the maturity level:	Criteria for clarification:
0	**Non-existent –** No attention has been paid to this control measure.	
1	**Initial -** The control measure is (partially) defined, but is implemented inconsistently. There is a great deal of dependence on individuals in the implementation of the control measure.	■ No or limited control measure implemented. ■ The control measure was implemented on an ad hoc basis. ■ The control measure is not documented. ■ The method of implementation depends on an individual and is not standardized. ■ The tasks and responsibilities, including the necessary separation of functions, are described for this control, but in practice they are often not carried out in accordance with the description. ■ Testing of the effectiveness of this control takes place occasionally. ■ The effect of the control measure is not assessed.
2	**Repeatable but informal –** The control measure is in place and is implemented in a consistent and structured, but informal manner.	■ There is limited evidence of design and existence. ■ The control measure is only partly determined, partly recorded in writing and partly embedded in the organization. ■ The tasks and responsibilities, including the necessary separation of functions, are described for this control measure and are implemented in practice. ■ The effect of the control cannot be demonstrated and/or has not been recorded. ■ The effectiveness of the control measure is periodically tested and recorded for less than 6 months **or** the effectiveness cannot be demonstrated for 6 months.
3	**Defined (design, existence and operation) –** The design of the control measure is documented and implemented in a structured and formalized manner. The required effectiveness of the control measure is demonstrable and is tested. Where necessary, the control measure is improved.	■ Design, existence and effective operation are demonstrable. ■ The control measure is defined on the basis of a risk assessment. ■ The control measure has been determined, recorded in writing and embedded in the organization. ■ Tasks and responsibilities, including the necessary separation of functions, have been written down, implemented and tested for effectiveness and are being evaluated. ■ The effective operation has been risk-based tested, demonstrated and recorded over a period of at least 6 months. ■ The implementation of the control measure is reported to management.
4	**Effective and measurable system of control measures -** In addition to the effectiveness of individual control measures, the effectiveness of the coherence of all information security measures is also periodically evaluated. This evaluation of the system of control measures is recorded and reported to management.	Criteria for level 3 plus the following distinguishing criteria: ■ The evaluation of the control measure takes place in the context of the system of information security measures. ■ The evaluation is documented. ■ The tasks and responsibilities for evaluating have been formalized. ■ The frequency of evaluation is based on the risk profile of the institution and takes place at least annually. ■ During the periodic testing of the effective functioning of the control, KCIs (metrics) are used, (operational) incidents are included and benchmarking takes place with peers. ■ The outcome of the evaluation is reported to management.
5	**Continuous improvement and future-oriented system of control measures -** Continuous efforts are made to improve the effectiveness of the system of control measures by taking future risks into account. External data and benchmarking are used for this. Employees are proactively involved in the future-oriented improvement of the effectiveness of the coherence of information security measures.	Criteria for level 4 plus the following distinguishing criteria: ■ The control measure is continuously updated. Evaluation is focused on the future and includes benchmarking with peers. ■ When designing the control measure, results from self-assessments, gap and root cause analysis were used. ■ The control measures taken have been benchmarked based on external data and are 'Best Practice' compared to other organizations. ■ The effectiveness of the control measure is tested on the basis of KCIs (metrics). ■ Employees are demonstrably continuously and proactively involved in improving the control measures.

1.1 Information Security Plan

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Based on a risk analysis and threat assessment, the administrative or policy-making body (hereinafter: “the board”) determines a digital operational resilience strategy in the short, medium and long term.
- The board has the ultimate responsibility to periodically determine the information security policy, including the resulting information security plan, in line with the digital operational resilience strategy.
- The board oversees and takes responsibility for ensuring that the established information security policy and information security plan are implemented and monitored.
- The information security plan defines the key information security management roles and responsibilities and sets out the budget, personnel, process and technology requirements related to information security, with employees at all levels responsible for ensuring the institution’s information security.
- The information security policy and plan are related to the business strategy and the nature and size of the institution (proportionality) and support the goals of the ICT strategy.
- The institution informs employees and service providers of the current information security policy. This applies to all employees and relevant service providers.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has drawn up an information security policy in line with internationally accepted standards such as ISO27001/2 and the NIST cybersecurity framework.
- The information security policy contains preventive, detecting, corrective and repressive control measures. In the NIST cybersecurity framework, for example, this is further expressed in the *Identify*, *Protect*, *Detect*, *Respond* and *Recover* phases.
- The institution’s information security policy describes both (ICT) technical control measures and procedural control measures in the business processes.
- The institution updates the information security policy at a fixed periodicity that suits the nature, size and complexity of the institution (for example twice annually) and at a higher frequency when there is reason to do so, for example in the event of mergers and acquisitions, major outsourcing or new cyber threats.
- Employees of the institution are familiar with the policies in the field of information security through awareness programs and know their roles and responsibilities in that regard.

1.2 Information Security policies and procesmanagement

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Control measures that arise from the information security policy and plan are part of standardized and predictable (ICT) work processes (controlled and ethical business operations) and are consistent with the risk analysis and threat assessment.
- The board ensures that the institution's governance system, in particular the risk management and internal control system, adequately manages the institution's security risks.
- (ICT) work processes and procedures ensure controlled IT system development, acquisition of secure hardware and software from an undisputed source, processing and storage of data, ICT system maintenance and ICT support.
- The information security policy ensures that the institution maintains log files and monitors critical IT activities so that errors can be detected, analyzed and corrected.
- Emergency procedures have been drawn up for situations not covered by standard procedures.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has described and/or set up (ICT) work processes and procedures in workflow tooling that ensures controlled implementation of those (ICT) work processes and procedures. For example, the workflow tooling enforces the 4-eye principle when adjusting critical ICT systems, system parameters or data and that all activities are traceable (logging).
- The procedures are based on internationally accepted standards, such as ITIL, BISL and PRINCE II.
- The institution updates the implemented control measures in relation to the (recalibrated) risks. In doing so, it adjusts the (design of) (ICT) work processes and procedures at a fixed periodicity (for example annually) and with a higher frequency when there is reason to do so, for example in the event of mergers and acquisitions, outsourcing of the (ICT) work processes or incidents in the execution. In the event of new or increasing forms of cyber threats, the institution examines whether (ICT) work processes and procedures need to be tightened. The institution determines the extent to which its employees, temporary workers and service providers adhere to the established (ICT) working methods and are aware that a controlled performance of their work contributes to information security and resilience against cyber threats.

←

→

2.1 Information Security Architecture

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Business processes and ICT systems are set up according to an information architecture established by the institution, which addresses, among other things:
  - Vision on information provision;
  - Target architecture of ICT systems and processes;
  - Cybersecurity and privacy requirements;
  - System and data classification;
  - Rationalization of current ICT systems; phasing out legacy ICT systems and ICT systems that are vulnerable to cyber threats;
  - The ICT architecture is in line with the ICT strategy.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution works according to an Information Security Architecture that provides insight into how the ICT systems and data collections support the business strategy and business processes.
- The information architecture is based on internationally accepted standards such as TOGAF and DYA, whereby the areas of attention developed therein have also been viewed from a security perspective.
- The institution has developed a vision showing how the ICT systems and organizational structure will evolve to support the business strategy in the medium/long term; critical or important dependencies on third parties/partners have been identified.
- This vision involves elements of NIST ZERO Trust architecture such as creating a separation (logical or possibly physical) of 1. The communication flows used to control and configure the network and the application/service (control plane) and 2. The communication flows used to perform the actual work of the organization (data plane).
- The institution uses architectural principles that are aimed at making information available to authorized employees, customers and third parties as simply, flexibly, reliably and securely as possible.

2.2 Data classification scheme

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Ownership of systems and data has been determined by the organization's board.
- The institution has established a data classification policy, whereby all relevant information security risks to which it is exposed are identified, classified and measured.
- The measurement of ICT and security risks is carried out based on the established ICT and security risk criteria, taking into account how critical the business processes and activities, business functions, roles and assets (such as information and ICT assets), the extent of known vulnerabilities and previous incidents that have affected the institution.
- The methods used to determine criticality ensure that protection requirements are consistent and comprehensive.
- Based on the above classification policy, relevant security measures are taken regarding access, encryption, storage, retention, cleaning, etc.
- The institution periodically checks whether employees comply with the classification policy.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has drawn up a data classification scheme based on the risks on the basis of which all ICT systems and data are classified into, for example: Confidentiality, Integrity, Availability (CIA), High/Medium/Low and Public/Confidential/Secret.
- Based on the classification, the institution takes control measures, such as encrypted storage of all data in the Secret category.
- The institution has insight into the data center location(s) where its business-critical information is stored. This institution periodically determines that the locations are in accordance with its information security policy.
- The institution actively monitors, using DLP tooling, the extent to which sensitive data is sent outwards from the corporate network and whether this is in accordance with the data classification.

3.1 Risks and opportunities of future trends and regulations

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board and risk are aware of the most important applications of technological developments and threats and include the risks and opportunities in their decision-making.
- Developments in the sector are mapped, including in the field of cybersecurity, which also includes topics such as 'technology' and 'risk management'.
- The potential impact of all these developments/threats is weighed and, if applicable, appropriate control measures are taken to mitigate risks.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Employees are active on internet forums and/or subscribed to cybersecurity newsletters.
- The institution purchases a service from an external party that provides targeted security intelligence.
- The institution is a member of professional and/or trade associations or other sectoral organizations that exchange knowledge and experience in the field of cybersecurity, such as ISACs.
- The institution maintains close contacts with government agencies that focus on cybersecurity, such as the NCSC or the Digital Trust Center.
- The institution has made contractual agreements with critical or important outsourcing partners on cooperation and information exchange in the field of information security and cybersecurity.
- Developments in the field of Quantum technology are mapped, both for practical applications of Quantum in the field of security and for risks arising from Quantum technology, such as risks in the field of cryptography.
- The institution monitors the applications of new technologies, such as Artificial Intelligence and blockchain, and pays attention to both opportunities and risks.

←

→

3.2 Technical standards

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution works according to accepted (technical) standards in the field of information security and cybersecurity. These are focused on the nature, size and complexity of the institution.
- Working according to standards has been communicated to employees; they are familiar with the standards relevant to their work.
- New ICT systems and changes to ICT systems comply with the established standards.
- The institution verifies that work is being done in accordance with the established standards.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution works according to internationally accepted standards for information security and cybersecurity, such as the MITRE Att@CK framework, ISO27001/2, NIST cybersecurity framework, NCSC Guidelines and/or CIS Baselines.
- The standards have been communicated and known to internal and contracted personnel, such as ICT security officers, ICT architects, project managers, software developers, functional and technical managers, ICT risk managers and ICT auditors.
- The follow-up of deviations from security baselines is determined based on the security risk.
- The institution's ICT security officer assesses new standards in the field of information security and cybersecurity and makes proposals on how they can strengthen the institution's information security and cybersecurity control measures.
- The ICT architecture and standards formalized by the institution have been declared applicable to the institution's service providers. It is periodically determined to what extent the service providers have organized their ICT environment in accordance with these standards.
- The ICT infrastructure and the ICT application landscape are tested annually against the most current security baselines and market standards.

4.1 ICT-Risk Management Framework

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board has set up a risk management cycle and is regularly informed about information security risks and cyber threats.
- The institution addresses risks and control measures in the field of information security and cybersecurity in the ICT Risk Management framework in line with its own digital operational resilience strategy.
- The ICT Risk Management Framework is part of the institution's overall Risk Management framework.
- The risk tolerances with regard to information security and cybersecurity have been determined and recorded.
- The board makes sufficient resources available to take effective control measures based on the risk profile of the institution and the risk appetite of the board. The board periodically considers, and actively involves risk, the extent to which an effective 'mix' of control measures - people, processes, technology and facilities - has been taken to mitigate the risks of the institutions in the field of information security and cybersecurity (from a comprehensive approximation).
- The board annually evaluates the desired/required level of maturity of the 58 control measures on a risk-based basis.
- The board evaluates annually, and in the event of major ICT-related incidents, via a written report on the result of the ICT Risk Management framework. Current developments and risks are taken into account.
- The ICT Risk Management framework is regularly subject to (internal) audits.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution uses clear definitions for information security and cybersecurity in its ICT Risk Management Framework; these are derived from market standards such as NIST CF, ISO 27000 and CobiT and are used consistently within all documents and reports in the ICT Risk Management Framework.
- Insurers process risks in the ORSA, pension funds in the ERB and banks in the ICAAP. The digital operational resilience strategy includes the following elements;
  - explanation of how the ICT Risk Management Framework supports the institution's business strategy and objectives;
  - determination of the risk tolerance limit for ICT risk (in accordance with the risk appetite) and an analysis of the impact tolerance for ICT disruptions;
  - clear information security objectives, including key achievements, indicators and key risk metrics;
  - explanation of the ICT reference architecture;
  - an outline of the various control measures that have been or will be introduced to detect, protect and prevent the effects of ICT-related incidents and to gain insight into how they are related to each other;
  - demonstrating current digital operational resilience based on the number of reported major ICT-related incidents and the effectiveness of preventive control measures;
  - developing a communication strategy in the event of ICT-related incidents. Current cyber threats such as malware, ransomware, DDoS attacks and phishing are part of the Risk Management framework.
- Parties in the chain of outsourced services work in accordance with the institution's ICT Risk Management Framework.

- The institution periodically assesses the extent to which parties to whom activities/systems have been outsourced work in accordance with the institution's ICT Risk Management Framework.
- The institution obtains an integrated picture of the management of risks in the chain in the field of information security and cybersecurity based on internal reports and reports from service providers.
- The tasks of checking compliance with ICT risk management requirements can be outsourced to intra-group or external companies. With such outsourcing, the institution remains ultimately responsible for the integral risk picture.

4.2 Risk assessment

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board periodically checks to what extent the risks that the institution faces in the field of information security and cybersecurity are within the risk tolerances established by the board. Also in the event that critical or important work has been outsourced to service providers.
- The institution regularly or at least once a year, and with every major change in the infrastructure or relevant processes, carries out ICT risk analyses based on qualitative and quantitative methods. She also explicitly takes her outdated and legacy systems into account. As important input for the risk analysis, the institution's specified threat assessment is first mapped or updated.
- The likelihood and impact of inherent risks in the field of information security and residual risks are identified.
- The institution includes the risks associated with the applications of new technologies in ICT risk analyses and the threat assessment.
- Based on its risk assessment, among other things, the institution determines and implements control measures, where relevant measures their effectiveness with KCIs (metrics) and periodically tests their effectiveness to manage the identified ICT and security risks and protect the information assets in accordance with their classification.
- Residual risks are submitted for (temporary) acceptance at the management level that is appropriate to the nature and extent of the residual risk.
- Accepted residual risks are periodically reevaluated and resubmitted for acceptance when they fall outside the institution's risk tolerance.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution annually carries out an ICT risk analysis with all stakeholders within the institution that are relevant to the analysis. On this basis, current cyber threats are weighed and prioritized.
- To this end, the institution maps and regularly updates its business processes and activities, business functions, roles and assets (such as information and ICT assets) in order to determine their importance for ICT and security risks and to determine the mutual dependencies.
- The institution also regularly and at least annually carries out a specific ICT risk assessment on all legacy ICT systems.
- To map out its own threat assessment, the institution uses various external and internal sources and threat intelligence, such as the One Financial Threat Landscape for the Netherlands (1FTL-NL).
- The institution maps out its 'crown jewels', evaluates them periodically and relates them to current cyber threats and control measures taken. Where necessary, the institution takes additional control measures. Control measures that no longer work effectively are adjusted, replaced by other control measures, or phased out.
- The institution periodically assesses the risk analysis of parties in the chain for relevance and determines the extent to which they meet the institution's requirements.
- The weighted and prioritized risks in the field of information security and cyber threats are addressed by the institution and limited to an acceptable level that matches the institution's risk tolerance.

- The institution analyzes the risks associated with the applications of cryptographic technology to support its business processes in the short (1 year), medium (1-5 years) and long (>5 years) term. In doing so, it takes into account the development of Quantum computing and the possible resulting threats to the institution.
- The institution makes an annual update of this analysis.
- The institution discusses the inventory in the context of the Risk Management Cycle at board level.

4.3 Maintenance and monitoring of a risk action plan

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution draws up a 'risk action plan' for unacceptable risks that further elaborates the risk response.
- This 'risk action plan' includes residual risks and the necessary compensatory control measures. These control measures are weighed and prioritized in conjunction with the other information security measures to be taken.
- Residual risks in the field of cybersecurity are part of the institution's risk action plan.
- The risk action plan is approved by the management level that is appropriate for the nature, size and complexity of the residual risks.
- The risk action plan is up to date; follow-up of the actions is monitored.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- For current cyber threats, the institution has made explicit which risks are formally accepted and for which residual risks additional control measures are necessary.
- Intended actions in the field of cybersecurity and the status of implementation are described in the risk action plan. Deviations from the original planning are periodically reported to the responsible management level that is appropriate to the nature, size and complexity of these residual risks. The institution has line management draw up an 'in control' statement (ICS) annually.
- The institution periodically determines the (re)prioritization of the information security measures and approves the use of the resources. This sets out the decision as to why which prioritization was made.
- The institution periodically assesses the risk action plans of service providers in the chain for relevance and determines that they meet the institution's requirements. In the event of deviations, the institution makes agreements with those parties to limit the risk to an acceptable level that fits within the institution's risk tolerance.
- The institution periodically includes in its risk action plans those controls whereby the service providers cannot meet the information security requirements of the institution. The institution takes additional control measures if necessary.

5.1 Responsibility for risk, security, compliance and Information Security function

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board has assigned tasks and responsibilities in the field of setting up, managing and monitoring information security and cybersecurity.
- The board actively and visibly promotes the importance of information security and cybersecurity for the institution and its service providers.
- There is a culture of awareness within the institution regarding the responsibility of employees to comply with and maintain security processes and procedures.
- The institution shall, within its governance system and in accordance with the principle of proportionality, establish an information security function, with responsibilities assigned to a specific employee.
- The institution ensures that the independence and objectivity of this information security function is safeguarded by appropriately separating it from responsibilities for processes regarding ICT activities and business operations.
- The information security function reports to the board.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The board of the institution visibly and actively promotes the importance of information security and cybersecurity.
- The institution has assigned tasks, responsibilities and authorities with regard to information security at all organizational levels.
- The institution has appointed a Chief Information Security Officer (CISO) who reports directly to the board.
- Specific responsibilities in the field of information security and cybersecurity control measures have been assigned to a Computer Security Incident Response Team (CSIRT) or Security Operations Center (SOC).
- When entering into critical or important outsourcing relationships and when monitoring those relationships, the institution checks that the above points apply to its chain partners.

5.2 Management of information security and tasks of the information security function

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has set up an information security function.
- The tasks of the information security function include at least:
  - a) supporting the board in drawing up and maintaining the information security policy, monitoring its rollout and implementation;
  - b) reporting regularly and on an ad hoc basis to the board and providing advice on the status of information security and its developments;
  - c) monitoring and assessing the implementation of information security measures;
  - d) ensuring that information security requirements are met where work has been outsourced to service providers;
  - e) ensuring that all employees and service providers who have access to information and systems are appropriately informed of information security policies;
  - f) coordinating investigations into operational or security incidents and reporting the relevant incidents to the board.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Rolling out training and awareness sessions on information security for employees.
- The institution uses internationally accepted standards, such as the ISO 27000 series, to organize information security and cybersecurity.
- Information security (including cybersecurity) is part of the tasks of the 1st, 2nd and 3rd lines. This is reflected in organizational charts and job descriptions.
- The institution regularly consults with its service providers at various levels about the management of risks in the field of information security and cybersecurity. The institution makes a record of this.
- This examines at which points in the chain improvements and/or actions are necessary (PDCA cycle). The follow-up of these actions is monitored.
- Input is given to this periodic discussion from the 1st, 2nd and 3rd lines (at the institution and at the service providers).
- The information security function regularly reports to the board/management of the institution on the management of risks in the field of information security and cybersecurity.

6.1 Data and system ownership

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The ownership of all data and information systems that the institution uses in its business operations is clearly allocated.
- Data and information systems are classified by the system owner. Control measures have been determined in accordance with this classification. See control measure 2.2.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has formulated principles in a policy document with regard to ownership, storage locations, retention periods and applicable legislation and regulations.
- The institution maintains an overview of all information systems and data and the owners responsible for them.
- The institution has entered into agreements with cloud service providers for outsourced ICT systems and cloud services. This determines who owns the data and information systems and where they are located.
- The institution has drawn up and communicated rules of conduct stating that employees handle data carefully (safe handling of e-mail and clean desk policy). Compliance with the rules of conduct is monitored.
- The institution has restricted access to customer files based on whitelisting at the file/customer level. Specific data elements are protected, such as special personal data and income data. Consulting files is logged; the logging is periodically reviewed and exceptions are resolved with the data owner.

7.1 Segregation of duties

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board ensures that unwanted mixing of functions (toxic combinations) and the associated risks are reduced by the institution, even in the event that critical or important activities have been outsourced.
- Segregations of duties are based on the structure of the institution's AO/IC.
- Segregations of duties have been further elaborated on the basis of a risk analysis, implemented and approved by senior management.
- When defining and implementing separation of duties, the principles of "need-to-know" and "least privilege" were used as a starting point and the concept that critical tasks and functions are divided among more than 1 person was taken into account.
- The implementation of relevant procedures regarding segregation of duties is periodically assessed and revised if necessary.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has drawn up a formally established standard for separation of duties in the form of an authorization matrix.
- Using the authorization matrix (soll), the institution periodically checks whether authorizations have been enforced in accordance with the requirements of segregation of duties in the ICT systems (ist) (soll-ist comparison).
- The implementation of separations of duties in ICT systems is periodically assessed. After major changes have been made to ICT systems, an interim assessment takes place.
- Based on a risk-based approach, the institution has not only mapped out the desired separations of functions per application, but also emphatically per process if this process is supported by multiple applications. This prevents separations of functions at process level from being broken, even though they are set up in accordance with the requirements for each individual application in the process.
- The institution minimizes the number of accounts with high privileges. With such an approach, unwanted mixtures of functions (toxic combinations) and the associated risks can be reduced.
- The institution is alert to prevent roles of project employees from conflicting with their role in the performance of their line tasks. Exceptions are detected and submitted to management for (temporary) acceptance.
- For accounts with high privileges (for example, administrator accounts), the setting applies two-factor authentication.
- The institution does not allow the use of generic and shared accounts; Senior management signs off on exceptions to this rule.
- The separation of duties is supported by an adequate Identity and Access Management system (IAM), see also controls 17.1 and 17.2.

8.1 Personnel recruitment and retention

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution attracts sufficient employees with experience and knowledge of information security and cybersecurity that matches the ambition and risk profile of the institution.
- The institution invests in maintaining the knowledge level of employees through education and training in the field of information security and cybersecurity.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has entered into agreements with specialized parties to keep the knowledge of its employees and policymakers in the field of information security and cybersecurity up to date.
- The institution has drawn up a gap analysis that shows how it will keep the knowledge level of its employees in the field of information security and cybersecurity up to date in the future.
- The board is sufficiently aware and acts accordingly that they themselves could be the target of an attack.

8.2 Personnel competencies and culture

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board, supervisory board and key function holders have demonstrably followed training and education to understand the most important ICT risks and control measures for their institution.
- The board shows good exemplary behavior with regard to awareness of risks in the field of information security and cybersecurity and compliance with procedures that safeguard information security (tone-at-the-top).
- So-called ‘management overrides’ of existing processes and procedures by the board and senior management are avoided where possible.
- The knowledge and competencies of employees and policymakers in the field of information security and cybersecurity are in line with the (digital) ambitions of the institution.
- The institution periodically checks to what extent the knowledge and competencies of employees and policymakers in the field of information security and cybersecurity are (still) in line with the (digital) ambitions of the institution.
- In the event of high-impact incidents, the institution uses root cause analyses to identify the extent to which the culture or behavior of certain employees contributed to the incident. Mitigating control measures are implemented based on this analysis.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Budgets for permanent education in the field of information security and cybersecurity have been determined and are sufficient.
- Policymakers within the institution have at least basic knowledge of information security and cybersecurity. They have demonstrably followed training and education to understand the most important ICT risks and control measures for their institution.
- Job descriptions include the knowledge and competencies expected of employees with regard to information security and cybersecurity.
- The institution has developed a training plan on the basis of which the knowledge of cybersecurity experts keeps up with current developments surrounding cyber threats. The realization of this plan is monitored.
- The institution includes cultural aspects (e.g. carelessness, dissatisfied employees) in root cause analyses of incidents.

8.3 Dependence upon individuals

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has identified which processes/activities that are critical to the operation of its business and which it depends on a limited number of employees.
- Based on a risk analysis, the institution determines where the dependence on individuals exceeds its risk tolerance.
- The institution takes control measures to limit over-dependence on individuals within its risk tolerance limits.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has made an inventory that shows the key person risk.
- Elaborated training programs are aimed, among other things, at spreading knowledge and experience more widely in the field of information security and cybersecurity.
- The institution demonstrably applies job rotation and succession planning for critical functions.

8.4 Personnel clearance procedures

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Prior to commencement of employment, personnel are screened in relation to the risk profile of the position.
- The screening is repeated periodically during the employment relationship.
- The above applies to both institution's own employees and hired employees.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has drawn up job profiles that distinguish between positions with a high, medium and low risk profile.
- The pre-employment screening requirements have been recorded, ratified and are used within the recruitment and selection process.
- The institution has demonstrably requested certificates of conduct (Verklaring Omtrent het Gedrag, VOG) for positions with an average or high risk profile and checks references.
- Risk-based in-employment screening is carried out periodically for medium and high risk positions.

8.5 Job change and termination

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- In the event of job changes, rights in ICT systems and processes are adjusted as quickly as possible. Access rights that the employee is no longer allowed to have due to the new position will be revoked immediately.
- Upon termination of employment, the institution immediately revokes rights in systems and processes. Attention is also paid to access rights to systems / services that fall outside the management of the institution, such as internet portals or cloud applications to which the (former) employee is subscribed on behalf of the institution.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution uses User Provisioning, whereby access rights in ICT systems are automatically created, changed, blocked and deleted from the HR system.
- Identity Access Management pays specific attention to *joiners*, *leavers* and *movers*. See also control measures 17.1 and 17.2.
- The institution maintains (manually or automatically) a register of tools, portals and/or cloud applications that its employees have access to by virtue of their position. In the event of termination of employment or change of position, the access rights of the employee in question are transferred to another employee.

9.1 Knowledge transfer to end users

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Employees have the knowledge and skills to correctly use ICT applications and ICT systems in accordance with the institution's procedures and work instructions.
- Employees know how information technology supports their critical business processes and are aware of the risks associated with that technology with regard to information security and cybersecurity. Employees apply that knowledge in their daily operational work.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Employees periodically receive functional training on the correct use of ICT applications and ICT infrastructure, whereby attention is also paid to information security and cybersecurity aspects.
- Work instructions for the correct use of ICT applications and ICT infrastructure are available in the form of internal wikis, intranet and help functions in the applications and systems.
- In (SLR) discussions with service providers, the institution is alert to ensure that knowledge development and knowledge sharing by employees also receive sufficient attention from the service provider.

9.2 Knowledge transfer to operations and support staff

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- ICT employees have the knowledge and skills to develop, purchase, implement and manage applications and systems in accordance with the institution's procedures and work instructions.
- ICT employees know how information technology supports their critical business processes and know the risks associated with that technology with regard to information security and cybersecurity. ICT employees apply that knowledge in their daily operational work.
- ICT employees actively use their specialist knowledge to recognize information security risks and cyber threats and to manage them with appropriate control measures. Attention is paid to the importance of (continuous) education in the field of cybersecurity (in addition to monitoring developments).

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Targeted security training for specific target groups, such as ICT system developers, helpdesk employees, ICT managers and employees with a role in information security and cybersecurity.
- In (SLR) discussions with service providers, the institution is alert to ensure that knowledge development and knowledge sharing by employees also receive sufficient attention from the service provider.

9.3 Employee awareness

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board has demonstrably followed training and education tailored to them to understand and address the most important ICT risks and control measures for its institution.
- The board shows good exemplary behavior with regard to awareness of risks in the field of information security and cybersecurity and compliance with procedures that safeguard information security (tone-at-the-top). Established guidelines and codes of conduct regarding information security and cybersecurity. These are known to employees at all levels of the institution.
- Increasing security awareness is part of the information security policy, in which a security awareness (training) program has been implemented. Explicit attention is paid to cybersecurity risks.
- The institution ensures that the training program provides regular training for all staff members.
- Employees know how to act when they suspect or identify risks in the field of information security and cybersecurity.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- In the context of *security awareness*, a training program has been established for all employees to ensure that they are trained to perform their tasks and responsibilities in accordance with relevant information security policies and procedures to reduce human error, theft, fraud, misuse or loss .
- The institution uses a mix of resources to maintain and improve security awareness among its own employees and external parties. Security coordinators have been appointed within the institution for this purpose.
- Presentations, phishing campaigns, mystery guests and e-learning are used to further improve security awareness. Participation in e-learning courses has been made mandatory by the institution; results are measured and monitored.
- The institution uses appealing examples from its own practice in the *security awareness* program, such as security incidents that have occurred. Attention was paid to, among other things, CEO fraud, ransomware and spear phishing in periods when the institution may be more vulnerable due to (end of the year) crowds, holidays or understaffing.
- So-called 'management overrides' of existing processes and procedures by the board and senior management are avoided.
- The institution takes initiatives to increase awareness in the field of cybersecurity together with outsourcing partners.

10.1 Change standards and procedures

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Changes, including security patches in ICT applications, ICT infrastructure, ICT processes and critical system settings follow a standardized and controlled path, are prioritized and evaluated.
- Tasks and responsibilities regarding checking and approving change requests have been assigned.
- Technical objectives and functional and non-functional requirements, including those related to information security, are defined and recorded before initiating development activities or system operations.
- Control measures have been taken to prevent unintentional changes or intentional manipulation of the ICT systems during development.
- Changes to critical systems and infrastructure are not requested, approved and implemented by one and the same person (separation of duties).
- The development, implementation, operation and/or configuration of the ICT systems take place in separate systems and are documented (audit trail).
- The ICT systems developed or managed by end users also follow a standardized and controlled path that provides appropriate control in the areas of prioritization, registration and evaluation.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution ensures that requests for system development are recorded and handled in a structured manner, for example in a central registration system.
- The change management process is based on international standards and practices, such as ITIL, Agile, Scrum, Devops.
- The institution works according to the shift left principle, which assumes that Agile, Scrum, Devops teams include application security in the earliest stages of system development.
- The institution also uses a workflow system for Agile, Scrum and Devops that supports the entire process from change request to implementation, including logging and documentation.
- The institution has applied separation of duties in its Agile, Scrum, Devops system development with regard to, for example, operations and control or development and security.
- Control measures have been taken to protect the integrity of the source code of ICT systems.
- Secure Coding guidelines are used by internal developers or service providers who offer application services through which development activities are carried out.
- Automated scans/review of code take place in accordance with these Secure Coding Guidelines, as well as automated scans/review of code and configuration for vulnerabilities (such as OWASP in web development).
- When open source libraries are used in the code, they are automated and checked for vulnerabilities before production.
- The impact analysis of a change takes into account a fallback scenario in case the change is not successful.
- The institution has set up a Change Advisory Board (CAB) in which various disciplines such as business, ICT and ICT Risk/ICT Security make decisions about changes.
- Various disciplines such as business, ICT and ICT Risk/ICT Security are sufficiently and timely involved in decisions about changes.
- The institution reassesses the change management procedure annually.

10.2 Impact assessment, prioritisation and authorisation

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution examines the extent to which proposed changes in the operational environment will affect the existing security measures and whether additional control measures are necessary to reduce the risks in question. In this assessment, the interests of all relevant stakeholders are taken into account in decision-making on change requests.
- The institution prioritizes changes resulting from the impact assessment.
- Urgent or short-term necessary ICT changes are traceable and are reported to the relevant owner of the ICT asset for subsequent analyses.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The information security role / officer within the institution is involved in assessing the impact of change requests on the control measures taken in the context of information security and cybersecurity.
- The institution explicitly considers the information security aspects of the changes when determining the impact and priority of change requests.
- The institution prioritizes the results of an impact assessment by means of a classification of the change (for example: standard, normal, urgent, immediate).

10.3 Test environment

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Criteria for protecting test data have been established and are maintained.
- Access to test and production ICT systems is strictly separated. This is checked before and after for all environments.
- The institution has an environment available in which it tests the effectiveness of security control measures.
- The institution pays attention to version management when the software version of the test environment is the same as the production environment.
- Test and production data are not mixed.
- The institution does not use uncleaned production data in the test environment.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The User ID and password or other authentication of administrators in the test environment are never the same as those of the production environment.
- The institution tests exclusively with anonymized representative test data in a test environment separate from production.
- The institution uses specific software for cleaning and anonymizing data.
- Test and production systems are logically or physically separated. The institution uses the DTAP models and checks compliance with the separation between environments using random samples.
- The institution has a representative environment to test the effectiveness of new and changed (security) infrastructure such as IDS, SIEM, Web Application Firewall (WAF), routers, etc.

10.4 Testing of changes

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Changes in the ICT infrastructure and ICT applications are tested before they are put into use (production).
- The tests are carried out according to a test plan that also includes acceptance criteria for information security and ICT performance.
- The institution has defined an authorization flow that states which persons are authorized to test.
- Security testing is part of the development and testing process before changes are implemented.
- The institution scans changed ICT systems for vulnerabilities to cyber threats on the basis of a risk assessment before they are put into production.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution carries out various tests (such as a system test, user acceptance test, regression test and integration test) to determine the effectiveness of security measures in changed applications and infrastructure. In an agile working method, software is tested based on acceptance criteria (definition of done).
- The acceptance criteria include that the following elements are met: access security functions, authorizations work in accordance with specifications, confidential data is encrypted, critical actions are logged and the system performance meets the set requirements.
- When testing changes, information security and cybersecurity control measures are explicitly included, for example through security & vulnerability scanning and source code reviews.
- Where ICT applications have been outsourced, the institution determines on a risk-based basis that the most important functionality and security measures work in accordance with specifications.

10.5 Promotion to production

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Controlled transfer of changes in production systems takes place.
- Key stakeholders in system changes, such as users, system owner, functional and technical administrators, are involved in the change transfer and approval process.
- Logs are kept and subsequently checked whether changes have been made in accordance with the agreements by authorized persons.
- Based on a risk analysis, the institution determines whether a new or adapted ICT system will be used in parallel with the old system. For risky adjustments, the institution has provided a fall-back plan.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution establishes transfer procedures for putting into use changes in the ICT infrastructure and ICT applications.
- The authorizations to implement changes in production are not granted to employees on a permanent basis but are granted on a temporary basis.
- The institution uses a workflow system for the controlled transfer and registration of changes in the production environment.
- The institution uses privileged access management tools that issue and track temporary authorizations.
- Changes to business-critical systems and changes to security parameters take place under the 4-eyes principle.
- The setting logs all changes in the production environment. On this basis, it is periodically checked that no unauthorized changes have taken place.
- The institution pays, for a predetermined period, closer attention to security issues after major or critical changes have been put into production.

11.1 ICT Business impact analysis and ICT Continuity plans

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board is responsible for establishing and approving a business impact analysis and a resulting continuity plan to limit the impact of a major disruption on key business functions and processes.
- The board checks annually whether the business impact analysis and the continuity plan are up to date. The board ensures that important changes in ICT systems or services are immediately incorporated into the continuity plan.
- The institution conducts the business impact analysis to assess exposure to serious business disruptions, both quantitatively and qualitatively, using internal and/or external data and scenario analyses.
- The institution ensures that the availability of critical ICT systems and ICT services are designed and aligned with their business impact analysis.
- The business impact analysis and ICT continuity plan include various scenarios that take into account the continuity of cybersecurity control measures and the undisturbed continuation of information security functions during disruptions and cyber-attacks.
- Crisis management has been set up, including the associated communication protocols.
- Alternative processing and recovery options for all critical ICT services are available in the ICT continuity plan.
- In the event of a disruption or emergency, and during the implementation of the business continuity plans, the institution ensures that it takes effective crisis communication measures.
- All relevant internal and external stakeholders, including relevant supervisory authorities, were informed in a timely manner.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has a crisis management function that, among other things, establishes clear procedures in the event that ICT Business Continuity plans are activated. This also includes internal and external crisis communication.
- The institution has communicated its ICT continuity policies appropriately within the institution, for example via an internal website to all relevant staff and, where applicable, also to external service providers.
- The institution has hard copies of the continuity plans at a location that is known and accessible to the employees directly involved. A list of important telephone numbers and e-mail addresses is part of this.
- The institution has identified per department which processes are critical and which people are directly involved.
- When implementing a new system or application, the institution includes it in an updated version of the ICT continuity plan and associated test cycle.
- The institution uses service providers to prevent inconvenience from DDoS attacks, for example NaWas: the national car wash of the National Management Organization of Internet Providers, NBIP.

11.2 Testing of the ICT Continuity plan

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board is involved in drawing up the continuity plans and actively participates in testing the ICT continuity plan.
- Test scenarios are mapped out from which a test calendar/ planning is drawn up for testing the ICT continuity plans.
- Testing the ICT continuity plan demonstrates that the institution can function at a predetermined minimum essential service level until full operations are restored.
- Resilience against cyber-attacks that impact availability is included and tested in the scenarios.
- Testing the continuity measures covers the entire chain of systems and applications that support critical business processes.
- Test results are documented and identified shortcomings are analyzed, monitored and reported to the board.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution carefully prepares the testing of the ICT continuity plan, reports on the test results and ensures follow-up of action points. In the event of major findings or shortcomings, the institution carries out a retest to determine that the addressed findings and shortcomings actually lead to the desired result.
- The institution structurally plans capacity for both business and IT staff for testing business continuity or contingency testing.
- The institution includes chain partners in testing continuity measures. Results of the tests are discussed with the chain partners and, if applicable, improvement actions are determined.
- When implementing a new system or application, the institution includes it in an updated version of the ICT continuity plan and associated test cycle.
- The institution explicitly includes cybersecurity threats such as (D)DoS and Advanced Persistent Threats (APTs) in its test scenarios. To set up continuity tests, the institution uses experiences from testing within the sector and incidents with an impact on business continuity, for example via the ISAC sector.

11.3 Uncompromisable back-up storage

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has more than one location for the storage of data required for controlled business operations.
- Based on the business impact analysis, the institution determines which back-up data must remain unalterable, complete and correct and takes appropriate control measures.
- The locations are secure, at a sufficient distance from each other and accessible to authorized persons to ensure the continuity of critical or important functions in the event that the primary processing location is no longer available. Catastrophic scenarios are taken into account.
- The risk profile of the locations is such that a disaster cannot affect all locations at the same time.
- The contents of the back-up are determined periodically by the business process owners and ICT staff.
- The availability of the data at the different locations (back-up / data mirroring) is in accordance with the data classification policy of the institution.
- Compatibility of hardware and software to restore archived data and periodically restore archived data is assured.
- The institution has taken control measures to prevent, detect and mitigate cyber threats aimed at damaging back-ups.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- Based on a risk analysis, the institution has determined at which external location the back-ups will be kept.
- The institution periodically checks whether the offsite backup is usable by restoring it to a test environment. The users are closely involved in this.
- The institution periodically checks that back-ups are available and usable for repairing damage resulting from a cyber-attack (offline/air-gapped backup).

←

→

11.4 Restoration

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Based on the business impact analysis, the institution has implemented procedures in the ICT continuity plan for the recovery of ICT systems, ICT applications, data and documentation for both the short term and, if necessary, also for the medium and long term.
- The institution can respond appropriately within the target of their own Recovery Time Objectives and their own Recovery Point Objectives (RPOs, the maximum time within which a system or process must be recovered after an incident). The procedures and plans are documented, widely available and easily accessible in case of emergency, including a clear definition of roles and responsibilities.
- The procedures and plans are continuously updated in accordance with the lessons learned from incidents, tests, new risks and threats, this also applies to the RTOs and RPOs.
- Creating and restoring backups complies with institution policies for the continued availability, integrity, confidentiality, and authenticity of systems and data. The content and frequency of backups are determined in accordance with business recovery requirements. The back-up and recovery procedures are tested and evaluated on a regular basis.
- When recovering from an ICT-related incident, the necessary checks are carried out to ensure the integrity of the data. Attention is paid to consistency between systems.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has made agreements with its service providers and also internally between business and ICT about Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) and their testing.
- The procedures and plans for back-up and recovery of ICT systems specify which circumstances can trigger activation of the plans, and which actions are taken to ensure the availability, integrity, continuity and recovery of at least the critical ICT systems , ICT services and data. The plans aim to achieve the recovery objectives related to the institution's activities.
- After a disruption or major system failure, the institution can use back-ups or "snapshots" to restore its data and ICT systems within the set time limit so that its critical business processes can continue with sound data and correctly functioning systems.
- The institution periodically tests whether the back-up and restore works correctly.
- The institution has determined a maximum downtime and maximum data loss of its critical processes and determined, based on realistic tests, that recovery activities (for example: restoring backups) are feasible within this maximum downtime.
- The institution has drawn up a recovery scenario in case cybersecurity incidents occur.
- The institution has taken various control measures to monitor access to back-ups: offline back-up, network zoning, detection of anomalous back-up/restore activities.
- It is continuously checked whether there is sufficient capacity for back-up so that critical data can always be fully restored.

←
→

12.1 Storage and retention arrangements

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has a policy regarding data storage, retention and archiving of data. This is periodically updated and checked.
- The institution has defined and implemented procedures for data storage, retention and archiving of data in line with business objectives.
- Critical data storage and the environment where the data storage is hosted are protected against Ransomware attacks (such as air gap handling, Write Once-Read Many (WORM) etc).
- When storing data, legal requirements regarding retention periods are taken into account.
- It is periodically checked whether there is sufficient capacity for the backup so that critical data can always be fully restored.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution maintains an expiration calendar of stored data on the basis of which data is destroyed.
- The institution has made agreements with the service providers regarding the retention period of data in accordance with the institution's policy. These work through to any subcontractors.
- The institution periodically checks to what extent service providers adhere to the agreed retention periods, for example by means of SLR and/or assurance reports.
- The institution periodically assesses whether service providers and subcontractors meet the institution's requirements for data storage, archiving and retention.

12.2 Disposal

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has defined and implemented procedures to ensure that business requirements for the protection of sensitive data and software are met when data and hardware are deleted or transferred.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution uses destruction protocols for cleaning and destroying documents and electronic data carriers such as laptops, mobile phones, hard drives, SSD storage media and USB sticks.
- The institution has made agreements with service providers about the secure deletion and destruction of data. The institution periodically checks whether service providers still comply with these agreements.

12.3 Security requirements for data management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has defined and implemented policies and procedures regarding the secure receipt, processing, storage and provision of data in accordance with the institution's policy.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution includes in its information security policy how employees handle sensitive information based on its data classification policy (see control measure 2.2).
- The institution provides the right resources that enable its employees to send and receive data securely, such as encrypted USB sticks, encrypted internet connections, secure e-mail, document vaults, etc.
- The institution periodically checks whether it still complies with laws and regulations regarding data storage. Where necessary, it adjusts its policies and procedures.
- The institution periodically assesses whether service providers in the chain meet the institution's requirements in the field of data management.

13.1 Configuration repository and baseline

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution manages, inventories, tracks, corrects and removes unauthorized and unmanaged ICT assets on which its business processes depend, both internally and in its outsourcing chain.
- The ICT asset inventory is sufficiently detailed to allow rapid identification of an ICT asset, its location, relationship to other ICT assets, its security classification and its owner.
- The institution maintains a register of end user computing applications that support critical business functions or processes.
- The institution has insight into the configuration (parameters) of those ICT assets.
- The institution evaluates recommendations from suppliers and external parties for the secure design of ICT infrastructure and ICT applications and records how it configures its ICT assets 'securely' (baselines).
- The responsibility for the configuration (baselines) of the various ICT assets has been assigned to the relevant parts within the institution and has been recorded.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution determines the (security) baselines based on various sources such as suppliers, best practices in the market and guidelines.
- The institution has inventoried its ICT assets and recorded them in a central repository such as a Configuration Management Database (CMDB).
- The institution uses the CMDB to verify the actual ICT assets present. Differences are analyzed and followed up.
- The institution uses the CMDB to determine to what extent ICT assets are outdated and to what extent they are supported with security updates.

←

→

13.2 Identification and Maintenance of Configuration Items

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Changes to the configuration management database (see control measure 13.1) are made in a controlled manner. This means that changes have been approved and are logged. The institution has established the configuration management procedure.
- The configuration management procedure is integrated with procedures for change management, incident management and problem management.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The configuration management procedures are based on international standards such as ITIL.
- The institution periodically carries out automated scans (inventory) of the ICT infrastructure. The outcome of these scans is compared with the contents of the CMDB and if any deviations occur, they are analyzed and action is taken.

14.1 Third party and supplier services management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board approves and periodically reviews the outsourcing policy.
- Before the institution proceeds with outsourcing, it determines an appropriate level of protection for the confidentiality of data, the continuity of the outsourced activities and the integrity and traceability of data and systems, in accordance with policy and applicable regulations.
- The institution processes the requirements arising from these protection levels in agreements with the service providers at all links in the critical or important outsourcing chains.
- The institution has agreed specific quantitative and qualitative performance criteria with its service providers who report on them to the institution in reports or dashboards.
- The reports or dashboards are further analyzed to identify both positive and negative trends and developments for both institution-specific and generic services.
- The responsible line management is informed about the quantitative and qualitative performance as well as about the trend analysis

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution periodically receives reports or has access to dashboards in which the actually measured service levels are clearly included and compared to the service level objectives agreed in the Service Level Agreement (performance and quality standards).
- The institution receives an integrated report from its ICT service providers in which subcontractor performance is integrated into the measured performance criteria.
- Aggregated reports provide the institution's management at various management levels with insight into all outsourcing risks, compared to its risk appetite.
- The institution pays attention to the mechanisms for integrating the cloud services into the institution's systems, for example the application programming interfaces (APIs) and a good user and access management process.
- The institution only enters into arrangements with service providers that meet its standards in the field of information security and continuity. When these contractual agreements concern critical or important functions, the institution must carefully determine, before concluding the arrangements, whether the most current and highest quality standards for information security are applied by these service providers.
- Before concluding an arrangement, the institution assesses:
  - whether the arrangement relates to critical or important functions;
  - whether the supervision conditions have been met;
  - all relevant risks including the possibility of an increase in concentration risk;
  - whether the service provider is suitable based on the results of due diligence investigations;
  - conflicts of interest that may arise from the arrangement.

14.2 Third party and supplier risk management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution maintains a register of all contractual arrangements as part of the control framework for IT and outsourcing risks.
- The institution has made an inventory of the risks it faces from service providers and has included a strategy with regard to these risks in the outsourcing policy. These risks are regularly evaluated, including the concentration risk and the consequences of complex outsourcing chains on the risk profile.
- Through this analysis, the institution has an up-to-date picture of the inherent information security risk of all outsourcing and/or outsourcing chains. The institution itself monitors which control measures have been taken in accordance with the information policy and to what extent they demonstrably work. The board has been and will be informed of this.
- The institution has determined for its service providers and any subcontractors affiliated therewith which control measures from the institution and/or this Good Practice apply and which reports must be obtained.
- The register distinguishes between service providers that support critical or important functions and service providers that do not.
- Contracts are drawn up according to market standards and are in accordance with applicable legal provisions.
- The institution continuously assesses the availability of critical or important outsourced services, fallback options to continue services in an alternative manner and compliance with standards in the field of information security and cybersecurity.
- The institution takes a risk-based approach to information security with respect to the location(s) (i.e. country or region) for data storage and processing.
- The institution has a thorough and well-documented incident management process, including the responsibilities of all parties involved, for example by establishing a cooperation model in the event of actual or suspected incidents.
- The institution has documented a comprehensive exit strategy for the service providers that support critical and important functions and has tested and/or practiced it where possible.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution, together with its service providers, draws up a risk analysis and a strategy with regard to the continuity and reliability of the services and updates them at a fixed frequency. Risks at service providers to which services have been outsourced are included in the risk analyses.
- The outsourcing policy contains a strategy for the use of ICT services to support critical or important functions provided by ICT service providers and their chain partners.
- To assess concentration risk, it is assessed whether the contract with a service provider is easily substitutable and whether there are multiple contractual arrangements with the same service provider or with closely related service providers. The costs and benefits of alternative solutions are weighed against each other with a view to digital resilience.
- Where there is a possibility that a service provider may sub-outsource a critical or important task, the benefits and risks that may arise from this are weighed, especially where the subcontractor is located in a country in which the institution itself is not located.
- The institution has agreed an exit plan with its service providers. This contains agreements about a controlled termination of the services, such as the method of transition / migration, liability and the deletion of the (back-up) data of the

institution after the exit. Sub-outsourcing is in the scope of the exit plans. The institution has taken control measures to ensure the continuity of maintenance of software specifically developed for the institution (self-build and custom). Escrow agreements and/or agreements regarding continuation have been concluded for this purpose. The institution checks for critical or important systems to what extent these agreements in the agreements have been complied with.

- The institution has a standard confidentiality agreement for every organization that enters into a contractual relationship with the institution. The signing of the statement by relevant parties is monitored.
- The institution periodically assesses the solvency and agility of its critical or important service providers and takes action where necessary.
- The institution determines in advance, in a risk-based manner, the frequency and scope of the audits and inspections and whether the executive auditors/external accountants have appropriate skills and knowledge.
- The institution terminates contractual arrangements:
  - in case of violation of laws, regulations or provisions by the service provider;
  - in circumstances that may cause undesirable changes in the performance of the services provided by the service provider;
  - in case of weaknesses of the service provider in the general management of the ICT risk;
  - when the competent authority can no longer carry out effective supervision.

15.1 Security incident policy and definition

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has a formalized incident management process, which is linked to an escalation procedure and escalation criteria.
- The escalation procedure is based on agreed service levels for incidents that cannot be resolved immediately. The institution uses a clear definition for security incidents that is known to all stakeholders in the institution.
- In the incident management process, (cyber) security incidents are classified separately with the aim of responding to such incidents quickly and with the right expertise. When handling (cyber) security incidents, all steps and associated information are recorded in a log.
- The institution has established procedures for reporting cybersecurity incidents, responding to (cyber) security incidents, limiting damage as a result of those incidents and carrying out repair work.
- (Cyber)security incidents are reported to the authorities in accordance with applicable rules.
- After major ICT-related incidents that disrupt the institution's core activities, the causes of the disruption are analyzed and the necessary improvements are identified and implemented in a timely manner.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has set up a process that ensures that all (potential) security incidents are centrally reported and registered.
- The institution classifies ICT-related incidents and determines their impact based on, among others, the following criteria:
  - the number and/or relevance of affected clients or financial counterparties and, if applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational damage;
  - the duration of the ICT-related incident, including the service downtime;
  - the geographical distribution with regard to the areas affected by the ICT-related incident, especially if it concerns more than two regions;
  - the data loss that the ICT-related incident entails, such as continued availability, integrity, confidentiality or loss of authenticity;
  - the criticality of the services involved, including the institution's transactions and operations;
  - the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident, both in absolute and relative terms.
- The evaluation of the incident determines whether the established procedures were followed and the control measures taken were effective, including with regard to:
  - the speed of response, determining the impact of ICT-related incidents and their severity;
  - the quality and speed in carrying out forensic analyses;
  - the effectiveness of incident escalation;
  - the effectiveness of internal and external communication.

15.2 Incident escalation

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Significant incidents are reported to the board and it is at least informed of the impact, response and lessons learned.
- The institution has manpower, expertise and procedures available to act as a Computer Security Security Incident Response Team (CSIRT).
- Categorization and prioritization of incidents is based on impact analysis, defined criteria and service levels.
- The appropriate criteria and thresholds are established to classify an event as a security incident, as well as early warning indicators to enable early detection of these incidents.
- Responding to information security and cybersecurity incidents is trained.
- Incidents are assigned to an owner.
- Escalation procedures and responsibilities regarding decision-making in (cyber) incidents are known within the institution and are complied with. Procedures for incident reporting and activation of crisis management have been drawn up.
- (Cyber)security incidents are reported to the authorities in accordance with applicable rules.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has established a CSIRT, consisting of specialized ICT professionals, that is able to act quickly in the event of an information security or cybersecurity incident. The CSIRT aims to reduce damage and promote rapid restoration of services.
- For example, the CSIRT uses the cybersecurity incident response process as described by the SANS institute, where it looks at the next steps 1. Preparation. 2.Identification. 3. Containment. 4. Eradication. 5. Recovery 6. Post Incident.
- The Security Officer assesses the registered security incidents (at least) daily and determines their impact.
- The institution and the service providers work proactively together to detect and respond to cybersecurity incidents in the chain of outsourced services and ICT infrastructure. The institution has set up a Security Operations Center (SOC) or Cyber Defense Center for this purpose.
- As an alternative to setting up its own SOC or Cyber Defense Center, the institution uses a commercial external SOC or a SOC that it manages together with other institutions.
- The institution uses tools such as a SIEM to collect, combine and analyze ICT-related security information, with the aim of gaining timely insight into and proactively responding to (possible) security incidents.
- The institution's CSIRT also focuses on the prevention of cybersecurity incidents and the preparation of the institution for such incidents.
- If necessary, the board directs this response and evaluates the incident afterwards and includes the results of this evaluation in the risk management cycle.
- Specific external communication plans for critical business functions and processes are developed to:
  i. Collaborate with relevant stakeholders;
  ii. Provide timely information, including incident reporting, to external parties (e.g. customers, other market participants, the relevant (supervisory) authorities, where applicable and in accordance with applicable regulations).

16.1 Security testing, surveillance and monitoring

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The results of security monitoring are reported to the board. The reporting provides insight into both operational and security incidents and enables the board to make appropriate adjustment decisions about improving measures.
- The institution has taken and recorded security measures. These measures are tested and periodically evaluated to ensure that they continue to meet established security baselines.
- The institution has set up Security Operations Center (SOC) or Cyber Defense Center services.
- Monitoring of unusual activities in ICT systems takes place, exceptions are identified and followed up.
- This monitoring shall include at least the following:
  - users' activities are logged in a risk-proportionate manner;
  - internal and external factors, including business and ICT management functions;
  - transactions by service providers.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has taken security measures that include:
  - Log files. These are protected to prevent unauthorized modification or deletion. Log files are maintained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets. Institutions use this data to facilitate the identification and investigation of irregularities detected in the provision of services.
  - SIEM. The institution has implemented a SIEM (Security Information and Event Management) solution to quickly recognize and respond to abnormal patterns based on logging.
- The institution periodically prepares management reports with an overview of all registered security incidents and the status of follow-up.
- Based on logging from monitored systems, the SIEM identifies events that could pose a security risk ('alerts'). The alerts are assessed and prioritized by SOC analysts. When the potential severity of an alert requires further investigation, a case is created. A case report is drawn up for these cases.
- To optimize its SOC, the institution uses the NOREA *publication Good Practice on assessing the maturity of a Security Operations Center (SOC) using the SOC Maturity Framework (SOC-MF)*[10].
- The institution uses the MAGMA framework (developed by NL FI-ISAC) and/or the Miter ATT&CK framework to develop threat models, evaluate the effectiveness of security tools, develop detection strategies and prioritize security investments.

[10] www.norea.nl

16.2 Monitoring of internal control framework

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution manages its ICT risks and risks in the field of information security and cybersecurity. To this end, the institution has drawn up an ICT control framework (internal control framework), which includes, among other things, an information security policy, standards, procedures, (key) controls and ICT General Controls in line with the objectives of the institution.
- The institution regularly evaluates the design, existence and operation of the internal control framework.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The risk management function, internal auditor and external accountant regularly report their opinions, findings and recommendations on the design, existence and demonstrable operation of the ICT control framework.
- The institution monitors and records the follow-up to recommendations.
- The institution compares Service Level reports and assurance reports from internal and external suppliers with the agreed services and the institution's experiences with the services provided.
- The institution analyzes trends and developments compared to previous reporting periods.

16.3 Internal control at third parties

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution is and remains fully responsible for compliance with all obligations under relevant legislation and regulations.
- During contract preparation, the institution pays attention to the way in which the service provider continues to comply with contractual obligations, legislation and regulations and the reporting and audit arrangements to be made.
- The institution forms an opinion about the internal control measures of its service providers and any subcontractors.
- The service provider complies with legal and contractual provisions.
- The institution has contractually agreed that as a result of the outsourcing, supervision throughout the entire outsourcing chain will not be hindered.
- The institution records the agreements with the service providers centrally and accessible to the parties.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution ensures that its contracts with the service providers include at least the following:
  - a full description of the outsourced functions and services;
  - tasks and responsibilities of parties involved;
  - commitment by the service provider to continue to comply with all applicable laws and regulations;
  - the locations where the functions and services are provided and where data is stored and processed;
  - provisions on accessibility, availability, integrity, security and protection of personal data;
  - descriptions of service levels and precise quantitative and qualitative performance targets;
  - conditions under which the service provider may further outsource, without prejudice to duties and responsibilities;
  - notification periods and reporting obligations of the service provider;
  - obligation of the service provider to provide assistance in the event of an incident at no additional cost or at a predetermined price;
  - obligations for the service provider to implement business contingency plans, test and have security measures in place to ensure safe services;
  - right to permanently monitor the performance of the service provider;
  - obligation of the service provider to cooperate with competent authorities;
  - right of termination and minimum notice period;
  - exit strategies, including the introduction of a mandatory appropriate transition period;
  - participation of employees of service providers in programs and training in digital operational resilience.
- Contracts with service providers that support critical or important services further include:
  - precise quantitative and qualitative performance targets within agreed service levels to enable effective monitoring and appropriate corrective action where necessary;
  - notice periods and reporting requirements, including notification of any development that could have a material impact on the delivery of those critical or important functions;
  - implementing and testing business contingency plans;
  - the service provider’s obligation to participate in and fully cooperate with the financial institution’s Threat-Led Penetration Testing program;

  - the right to continuously monitor the performance of the service provider. Exit strategies and in particular the establishment of a mandatory adequate transition period.
- The institution takes the use of standard contractual clauses into account when drawing up the contract.
- The institution has contractually established its "right to audit" with the service provider and subcontractors and exercises this if necessary.
- The institution obliges the service provider to inform the institution of all intended significant changes to the subcontractors mentioned in the original agreement. The notification period for such changes is determined in such a way that the institution is able to assess the risks resulting from the proposed change and, if necessary, take corrective control measures or trigger the exit clause.
- The institution demonstrably evaluates critical or important outsourcing at least annually, assessing the performance and result agreements and the extent to which the service provider fits the strategy and objectives, as well as the risk appetite of the service provider compared to its own risk appetite.
- During the term of the contract, the institution receives periodic (assurance) reports from the service provider about the performance and demonstrable continued operation of the internal control measures taken at the service provider.
- The service provider provides the institution with an annual assurance statement on IT management, such as a COS/SOC 2 report type II. Control measures in the field of information security and cybersecurity are part of the scope of the assurance statement. The scope covers the entire outsourcing chain including critical or important subcontractors. The institution discusses deviations/exceptions with the service provider. These are addressed in a timely and effective manner by the service provider. The institution monitors the outcome and makes a record of this.
- The institution does not use type 1 assurance reports or ISO certificates to demonstrate the effectiveness of the control measures.

16.4 Evaluation of compliance with external requirements

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution periodically assesses the extent to which its ICT policy and procedures are in line with legislation and regulations.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution's compliance officer annually assesses the extent to which the ICT policies are in line with current legislation and regulations. Adjustments are made where necessary.
- When introducing new legislation in the field of information security and cybersecurity, the institution assesses its impact and makes adjustments where necessary.
- The institution is proactively informed about changes in relevant external regulations.

16.5 Independent assurance

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board periodically reviews and approves the IT internal audit plans, IT audits and the material changes thereto.
- The institution's governance, systems and processes for their ICT and security risks are periodically audited in accordance with the institution's audit plan.
- This is done by auditors with sufficient knowledge, skills and expertise in the field of ICT and security risks to provide independent assurance to the board about the effectiveness of the control measures taken.
- The frequency and focus of such audits is proportional to the relevant ICT and security risks.
- The results of the independent assessment are submitted to the institution's management.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has the internal or external auditor periodically assess ICT objects such as information security and cybersecurity of ICT infrastructure on the basis of a risk analysis. This assessment relates to the design, existence and demonstrable effectiveness of control measures.

17.1 Identity & Access Management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Logical access security processes are defined, documented, implemented and include anomaly monitoring and recovery.
- Authentication methods are proportionate to the critical nature of the ICT systems, information or process to which access is gained. This concerns at least strong passwords or stronger authentication methods (such as two-factor or out-of-band authentication), based on relevant risks.
- Access to the institution's information systems and data can be traced back to uniquely identifiable persons (internal, external and hired) or to ICT services (e.g. scripts and batch jobs) with a uniquely identifiable owner.
- Access to ICT systems and data are "function based" and only granted on the basis of least privilege principles. Compliance with these principles is periodically evaluated.
- The institution has determined, approved and recorded access to information systems and data (SOLL authorization matrices) and based on the required segregation of duties and business rules (see control measure 7.1).
- The design of the logical access protection (SOLL authorization matrices) is regularly evaluated.
- Access to the institution's information systems and data is controlled and monitored in the ICT infrastructure and in ICT applications, in accordance with the approved SOLL authorization matrices.
- Access rights in ICT systems (IST) are regularly compared with the SOLL authorization matrices.
- Institutions shall maintain authentication methods that are sufficiently robust to appropriately and effectively ensure compliance with access control policies and procedures.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution assigns unique user IDs to all persons with access to the ICT systems and data. The institution's HR system is leading here.
- User identities and access rights are maintained in a central repository.
- The institution uses strong passwords (complexity rules, numeric, use of symbols, age, history) for different types of accounts: system, normal, superuser.
- The institution uses out-of-band authentication, a form of two-factor authentication (2FA) that requires a secondary authentication method over a separate communication channel. This involves several channels: the customer's Internet connection and the wireless network on which its mobile phone operates.
- The institution applies the principle of 'Role Based Access' whereby it periodically defines which role has which identity. To this end, it maps out: Who gets access, What is provided with access, When, Where, Why and How.
- The institution uses an Identity & Access Management (IAM) tool to support the design of access security and its control by business process owners and IT system administrators.
- Remote access to critical ICT systems is only granted according to information needs and when strong authentication tools are used.

17.2 User account management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Requesting, changing or revoking access rights to information systems and data follows formalized steps in which approval is granted by the owners of the relevant business processes, information systems and data.
- The separation of duties or 4-eye principle prevents the aforementioned steps from being carried out by 1 person.
- All activities related to requesting, changing or revoking access rights are logged and can be traced back to individuals.
- Access rights of persons whose employment/contract is terminated will be removed or blocked as quickly as possible. The granting, adjustment and revocation of access rights are recorded in such a way that insight and analysis are facilitated.
- Controls are implemented for privileged system access by strictly restricting and closely monitoring accounts with high access rights (such as administrator accounts).
- Access of applications to data and ICT systems that cannot be traced back to persons is limited to the minimum necessary to offer the relevant services.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution uses User Provisioning, whereby user accounts in the ICT infrastructure and business ICT applications are created, changed, blocked and deleted automatically as much as possible from the central HR system.
- The setting automatically blocks a user account after it has not been used to log in for a preset period.
- Approval is given by the data or system owner for requesting, changing or revoking access rights to information systems.
- The institution limits the use of generic and shared user IDs, including administrator accounts with high privileges, as much as possible. The use of these user IDs is controlled with both technical and procedural measures, such as: approval for use, powerful authentication solutions (2-factor authentication, biometrics), 4-eye principle on activities, (digital) password vault, logging and monitoring activities and evaluation after using the relevant administrator user ID.

18.1 Infrastructure resource protection and availability

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The control measures in the ICT infrastructure components are based on a threat and risk analysis and are designed in such a way that they ensure a high level of continuous availability, integrity, confidentiality and authenticity of information.
- Planning and monitoring processes related to performance and capacity are carried out to prevent, detect and address significant performance problems of ICT systems and ICT capacity shortages in a timely manner.
- The design and implementation of these control measures is monitored and evaluated.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Risk analyses for infrastructure components take into account current cyber threats, as recorded in the ENISA/NCSC threat images or based on the results of recently conducted red teaming exercises and pen tests, etc.
- Security baselines have been determined for technical platforms (for example: Windows, Unix, firewalls, IDS and IPS) and implemented in accordance with those baselines.
- Monitoring takes place to ensure that all platforms comply with the security baselines. Exceptions are followed.
- The institution has taken anti-DDoS measures. A distinction is made between protection against volume-oriented DDoS attacks and application-oriented DDoS attacks.
- The institution has carried out a risk analysis regarding distributed storage and management of private keys and passwords. A well-founded assessment was made at which internal or external location keys and passwords are stored.
- The security and availability of the ICT infrastructure is a permanent agenda item in the relevant bodies in the first, second and third lines of the institution.
- The institution uses automated controls, for example to monitor vulnerabilities in the infrastructure.

18.2 Infrastructure maintenance

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Maintenance of the ICT infrastructure is planned and structured, follows its own baselines and is in line with the institution's change management procedures. When changes are made to the ICT infrastructure, it is checked whether the security of the institution continues to maintain the correct level.
- The institution monitors that the ICT infrastructure it uses is supported by the developer/supplier and that security updates (patches) are made available. Monitoring also takes place on the end-of-support date of the hardware, firmware and middleware used, so that mitigating control measures can be taken in a timely manner.
- The institution has classified the infrastructure components in order to prioritize the implementation of maintenance of the ICT infrastructure.
- Solutions for vulnerabilities in the ICT infrastructure such as patches influence the prioritization of maintenance work on the ICT infrastructure.
- Change management processes are followed that take into account the extent to which the vulnerabilities are critical within the patch management. This is based on change risk assessments (CRAs), risk analyses that are part of the change management process.
- The CRAs pay explicit attention to cyber threats, crown jewels and attack paths. These influence the prioritization of implementation of the changes.
- The risks arising from the use of outdated or unsupported ICT infrastructure are identified, assessed and limited. Decommissioned ICT infrastructure is processed and disposed of safely. To this end, a plan is drawn up that is coordinated with all business units involved. An increased focus at the institution on customer experience and time-to-market does not lead to the implementation of infrastructural (security) measures and investments in technological developments being postponed (too) long.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Implementing critical security patches in the ICT infrastructure is a specific part of the patch management process.
- The status of the ICT infrastructure, including its vulnerability to cyber threats, is periodically inventoried using tools. This is reported and action is taken on overdue maintenance.
- The institution has included the replacement term for ICT infrastructure components in its configuration management database (CMDB) and replacement is planned on this basis.

←
→

18.3 Cryptography and Cryptographic key management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The management of cryptographic keys takes place in a controlled and risk-based manner. The institution has developed policies and procedures regarding the generation, modification, revocation, destruction, distribution, certification, storage, installation, use and archiving of the cryptographic keys.
- Risks of modification and the keys becoming known during these processes have been identified and mitigating control measures have been taken.
- A risk analysis has been made so that the security measures are applied proportionally to the importance of the key in question.
- The institution has recognized the risks of cyber-attacks aimed at modifying and intercepting cryptographic keys and has controlled them with appropriate control measures.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution uses Hardware Security Modules (HSMs) to generate, change, revoke, destroy, distribute, certify, store, insert, use and archive the cryptographic keys.
- Processes, procedures and parameterization are designed in such a way that they protect the cryptographic keys optimally and proportionately.
- The availability of cryptographic keys (across the entire outsourcing chain) is included in the institution's continuity plans.
- The institution has an inventory of the cryptographic landscape (encryption protocols and certificates for network connections, key management and data storage). It is recorded how long (e.g. short, medium, long) the applied protocols are no longer safe and how long replacement or mitigation of a protocol is expected to take.
- The institution monitors the use of unsafe encryption protocols and sends notifications to administrators if unsafe protocols are used.
- The institution is creating a roadmap for its cryptographic landscape that is in line with upcoming threats in the short, medium and long term.
- The institution carries out an annual Cryptography Risk Assessment.
- The institution explores the risks and possibilities of Quantum technology, such as Quantum key distribution or Quantum random number generators.

18.4 Network Security

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution applies up-to-date technical security measures, such as firewalls, SIEM, (micro) network segmentation, intrusion detection, data leak prevention systems (DLP) and network traffic encryption.
- The institution conducts an analysis of the network to determine where restrictive network (micro) segmentation as well as the "never trust always verify" (also internal) principle is necessary to protect the crown jewels of the institution.
- The institution applies endpoint security to laptops, tablets and workstations. Endpoints that do not meet the security baselines are banned from the network and/or have limited access to data or ICT systems.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has taken note of, among others, NIST publications on a zero trust architecture such as the *NIST Special Publication (SP) 800-207, Zero Trust Architecture* and the *NIST SP 1800-35A Implementing a Zero Trust Architecture (draft)* in which 'inherent trust' is no longer part of network security.
- Management interfaces of network and security facilities are not directly accessible from (semi) public zones.
- The institution:
  1. Defines the parts of the ICT network that contain the crown jewels, such as specific Data, Applications, Assets and Services (DAAS).
  2. Maps the transaction flows between these parts.
  3. Defines and builds a "Zero Trust Architecture" for those parts by implementing a specific set of control measures.
  4. Establishes Zero Trust policies based on *Who* gets access, *What* is provided with access, *When*, *Where*, *Why*, and *How*.
  5. Monitors and maintains log events of network activities.
- The institution applies the "*never trust always verify*" principle for the previously defined parts of the network, which means that inherent trust is removed from these parts of the network and all actions require explicit verification, including internally.
- The institution uses tooling that actively searches the network infrastructure for unauthorized equipment such as laptops, routers and Wi-Fi access points, with the associated management procedures to limit access to the ICT infrastructure to authorized persons, ICT services and networks. The institution uses modern and secure standards/protocols such as IEEE[11] 802.1X for Port-based Network Access Control (PNAC), Wi-Fi Protected Access (WPA3) and carries out periodic checks on the control measures that focus on network segmentation, such as Access control lists (ACL), VLANs and firewalls between the different network segments.

[11] IEEE stands for the Institute of Electrical and Electronics Engineers

18.5 Protection of sensitive data

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has formulated a policy regarding the secure storage and sharing of confidential data and the integrity of information and monitors whether this policy is complied with.
- The institution has identified which information is confidential and when and where additional control measures are necessary to secure confidential data exchange.
- The institution uses up-to-date secure channels and integrity checks when exchanging confidential data.
- The institution encrypts data at rest, data in use and data in transit in accordance with the data classification policy.
- With regard to outsourced activities, it is examined whether additional specific control measures are required for data in transit, data stored in memory and data at rest, for example the application of encryption techniques (encryption) in combination with appropriate key management.
- The institution provides the right resources that enable its employees to send and receive data securely.

Pay attention to
risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution applies current authentication and encryption techniques to network connections with parties it trusts.
- Controls have been built into the institutions' network infrastructure to ensure the authenticity and integrity of messages, as well as the confirmation of transmission, receipt and the identity of the sender and recipient of confidential data.
- Confidential data is encrypted and stored on laptops, hard drives, USB sticks and other information carriers. The institution uses techniques to increase the security of e-mail, for example through anti-spam, DMARC, SPF, DKIM and e-mail encryption.
- The institution applies Data Loss Prevention software to control outgoing messages and data flows.

←
→

19.1 Malicious software prevention, detection and correction

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has implemented preventive, detective and corrective control measures to protect ICT systems and applications against cyber threats, such as viruses, worms, malware, ransomware and spyware[12].
- The institution has demonstrably made a trade-off between the composition of the different sets of tools, with quality and completeness of coverage prevailing over quantity.
- When applying these control measures, the institution looks at the risks and opportunities of technological developments and takes into account current information about (cyber) threats (Threat Intelligence).

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution uses various sources to map attack techniques and (technical) control measures, including, for example, the MITRE ATT&CK framework.
- The institution has implemented tools for the automatic detection and blocking of viruses, worms, malware and spyware such as modern firewall technology, virus scanners, email security tools (such as antiphishing, domain spoofing, spam), Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), Extended Detection and Response (XDR), Endpoint Detection and Response (EDR) and 'defender tools' with technology that addresses Attack Surface Reduction rules.
- The institution analyzes and learns from incidents that have occurred at peers or other comparable companies.
- Log files from the aforementioned systems are sent to a Security Incident and Event Monitoring (SIEM) system for analysis and (re)action; the institution prioritizes the (re) actions based on a risk assessment.
- The institution continuously monitors the extent to which firewalls, virus scanners, IDSs and IPSs are up to date and reports on this monthly.
- The institution checks to what extent service providers ensure that firewalls, virus scanners, IDSs, IPSs and their infrastructure are up to date. The service provider reports on this to the institution that manages security applications for the institution.

[12] See MITRE ATT&CK®

19.2 Vulnerability management

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The most important ICT assets have been identified and classified based on a risk analysis.
- Periodically, (cyber) vulnerabilities related to ICT assets are identified on the basis of Threat Intelligence and vulnerability scans and the severity of the security problem and possible impact are determined.
- The scope and appropriate frequency of the vulnerability scans are determined.
- The (cyber) vulnerabilities are addressed on a risk-based basis.
- The institution determines a risk response based on its risk tolerances and monitors the follow-up of the risk response based on defined KCIs (metrics).
- An impact analysis of the (cyber) vulnerabilities is made periodically.
- Based on this impact analysis, risk-mitigating actions are determined for threats that fall outside the institution's risk tolerance. If necessary, mitigating control measures are taken (timely) and additional (network) monitoring takes place to detect abuse.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution regularly inventories which ICT assets the business processes use.
- Potential vulnerabilities are prevented by ensuring that ICT systems are up to date, including the software provided by the institution to its internal and external users. It does this by implementing critical security updates in a controlled manner, including updates to antivirus definitions, or by taking compensatory control measures, for example (temporary) isolation of vulnerable systems.
- The institution frequently (daily) inventories vulnerabilities based on Threat Intelligence.
- The institution tailors the frequency and type of scan (such as authenticated or non-authenticated) to the segment and the risk analysis of its own organization. To this end, an analysis has been made that is periodically evaluated.
- The institution determines on a structural and risk-based basis what the impact of these vulnerabilities is on its own ICT assets.
- The institution periodically inventories for which software security updates are not made available or are not made available on time. Clear KPIs are agreed with suppliers for resolution times. It is also monitored that software (in accordance with the user period) is provided with security updates. Mitigating control measures are taken for software that is (soon) end-of-life.
- Where possible, checks on (parts of) security baselines are included in vulnerability scans.
- The institution regularly discusses reports/dashboards with its service providers regarding the results of vulnerability scans carried out.

19.3 Application Maintenance

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- Maintenance of ICT applications is planned, structured and in line with the institution's change management procedures.
- The institution monitors that the ICT applications it uses are supported by the developer/supplier and that security updates (patches) are made available. Monitoring also takes place at the end-of-life date of the application software used, so that mitigating control measures can be taken in a timely manner. The institution prioritizes the implementation of maintenance of the ICT applications.
- Solutions for vulnerabilities in applications such as patches influence the prioritization of regular maintenance work on ICT applications.
- Change management processes are followed that take into account the extent to which the vulnerabilities are critical within patch management. This is based on risk analyses that are part of the change management process (change risk assessments (CRAs)).
- The CRAs pay explicit attention to cyber threats, crown jewels and attack paths. These influence the prioritization of implementation of the changes.
- The risks arising from the use of outdated or unsupported ICT applications are identified, assessed and limited. ICT applications that have been taken out of service are processed and disposed of safely. To this end, a plan is drawn up that is coordinated with all business units involved.
- An increased focus at the institution on customer experience and time-to-market does not lead to the implementation of application (security) measures and investments in technological developments being postponed (too) long.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution applies acceptance criteria in the field of information security and cybersecurity when developing and purchasing ICT applications.
- The institution has included the replacement period for applications in its configuration management database (CMDB) and replacement is planned on this basis.
- Deploying critical security patches from application vendors is a specific part of the patch management process.

←

→

20.1 Protection of security technology

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The institution has insight into the security technology relevant to it.[13]
- Given their inherently high risk profile, specific security measures apply to the security technology and the employees responsible for the operation of the technology.
- Documentation about the security technology and security measures as well as authorizations for administrators of the ICT infrastructure, including network administrators, is based on the principle of least privilege, which means that access is only granted to security technology on a 'need-to-know/ need-to have' basis.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution has taken additional control measures for security technology, such as tightened physical and logical access security, 4-eye principle on management and maintenance, a stricter patch regime and/or accelerated follow-up based on alerts from the monitoring system, 'tamper resistant' measures, etc.
- Administrative actions on security systems are logged and monitored. This applies to all access methods (e.g., lights-out/ out-of-band management, remote). Session recording takes place on the basis of a risk analysis.
- (Remote) access to systems takes place over an encrypted channel.
- Administrative access to systems preferably takes place via bastion hosts.
- ICT systems that play a role in the security of the institution are connected to a SIEM.
- Specific security research is carried out on the institution's security technology by specialized parties.

[13] Security technology includes: firewall equipment and software, encryption software and equipment, hardware security modules (HSM) for the storage of certificates and private keys, etc.

21.1 Physical security measures

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- In line with the institution's risk profile, physical security measures have been established, documented and implemented to protect sensitive locations such as the grounds, data centers, cabling and (remote) work locations against unauthorized physical access and (environmental) threats such as power outages, fire and water damage.
- Appropriate control measures to protect against threats are proportionate to the importance of the buildings and the critical nature of the activities or ICT systems located in these buildings.
- Physical access security measures are regularly maintained and tested.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- Based on a risk analysis, the institution has classified its data centers into classes (tiers) such as Tier I - The basics, Tier II - Redundancy of electricity production and cooling, Tier III - Maintainability or Tier IV fault tolerance and has implemented control measures in accordance with these classes.
- The institution applies physical zoning with different levels of access (for example: public, staff and restricted) based on a risk analysis.
- The institution's ICT-critical buildings are equipped with intrusion detection, the operation of which and any notifications are continuously monitored (24/7).
- The buildings of the institution that are critical to its business operations are equipped with technical management measures to ensure continuity and limit damage caused by, for example, fire, lightning, humidity and temperature increases, such as smoke detectors, fire detectors, extinguishing systems, lightning rods, air conditioning and electricity (emergency power) facilities.

21.2 Physical access

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- A policy has been defined and implemented for the access security of buildings, sites, zones, data centers, server rooms and remote work locations that are important for carrying out business processes.
- Physical access security measures are in line with the risk profile of the institution.
- Access profiles are authorized by the management of the institution. Access to buildings, areas, zones and server rooms is based on the position and responsibilities of the employee/ visitor in question.
- The effectiveness of physical access security measures is regularly checked and the results are reported to management.
- Assessment of the granted access rights (SOLL-IST) and assessment of logging of the access security system are included.
- Unnecessary access rights are immediately revoked/removed and physical access security measures are maintained and tested.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- The institution checks that any access to a data center has been requested 24 hours in advance with a change request and in case of emergency only under strict conditions.
- Physical access to buildings and zones is controlled using access cards and gates.
- The 4-eye principle applies to physical maintenance of security equipment.
- The institution has the physical access security measures checked by a “Mystery Guest”.
- ICT components that play a role in the institution’s physical access security are connected to a SIEM (Security Information and Event Management).

←

→

22.1 Penetration testing and ethical hacking

Market standards* indicate that the institution sets up a process that ensures, among others, the following:

- The board makes sufficient resources available to implement a test program, discusses the most important outcomes of the test program and ensures that procedures are in place to ensure that security test results are monitored, evaluated and prioritized.
- The board ensures that any identified vulnerabilities are mitigated without delay with clear deadlines, taking into account how critical the vulnerabilities and/or the affected ICT system are.
- In the testing program linked to the (ICT) risk management framework, a variety of different information security evaluations, assessments and tests are carried out to ensure effective identification of vulnerabilities in the ICT systems and services.
- The institution determines on the basis of a risk analysis which types and with what frequency, scope and depth security tests are carried out to validate the robustness and effectiveness of the information security measures.
- The risk analysis takes into account current cyber threats, the changing landscape of ICT risks, and any specific risks to which the institution is or could be exposed.
- The institution verifies that the internal or external party that carries out the security tests is sufficiently independent and equipped to carry out such tests (correct knowledge, experience and references) and that the tests are carried out in a secure manner.
- Testing of security controls is performed in the event of changes to infrastructure, processes or procedures, and if changes are implemented due to major operational or security incidents, or due to the release of new or significantly modified critical applications.

Pay attention to

risk-based, outsourcing and the three lines model

Good Practices here are:

- To determine types of security tests, the institution includes current cyber threats in its risk analysis, such as phishing, DDoS, ransomware and C-level fraud. Based on a risk analysis, the institution draws up an annual plan for the tests to be carried out. Part of this plan is to carry out pen tests, ethical hacking for all (new and changed) critical ICT applications and to carry out a red teaming activity.
- The institution carries out various types of security tests, including pen tests aimed at the security of infrastructure and applications, red teaming, testing physical security, testing human actions in relation to information security and cybersecurity[14].
- The institution uses a bug bounty/responsible disclosure program.
- The institution has pen tests carried out by specialized parties with the correct knowledge, experience, certifications and references.
- The institution regularly changes the party that carries out the pen tests.
- The board participates in biennial tabletop exercises.

[14] This also includes vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, questionnaires and scanning software solutions, source code reviews, scenario-based testing, compatibility testing, performance testing and end-to-end testing.

- The institution involves its critical or important service providers in its security tests.
- The institution joins TIBER for triennial Threat Led Penetration Testing (TLPT). These tests address an institution's critical functions and services and are performed on live production systems that support the critical functions and services. When outsourced activities fall within the scope, the financial institution guarantees the participation of the service provider involved.

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:

DeNederlandscheBank
EUROSYSTEEM