Good Practice

Information security 2019/2020

DeNederlandscheBank
EUROSYSTEEM

Good Practice - Information security 2019/2020

Introduction

This Good Practices document provides the institutions under our supervision with practical guidance on the implementation of control measures to ensure the integrity, continuous availability and security of electronic data processing.

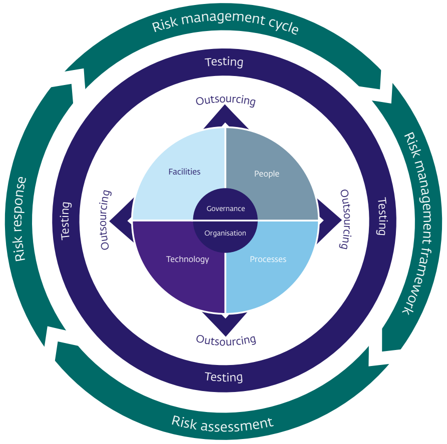
Based on a risk analysis, institutions implement control measures aimed at managing their information security and cybersecurity risks. These control measures should be in line with nature, scale and complexity of the risks associated with the institution's activities and the complexity of its organisational structure. These control measures are not limited to technological solutions (*Technology*), they also address human actions (*People*), *Processes* and *Facilities*.

In addition, institutions assess the design, existence and operating effectiveness of control measures on a regular basis as part of their *Risk management cycle*, in order to deal with constantly changing information security and cyberthreat risks. They improve or replace any control measures that are not effective. Institutions set up their *Governance* and *Organisation* in such a way as to steer this process.

Also, institutions ensure that they are in control of information security and cybersecurity regarding outsourced activities (*Outsourcing*) and that they *Test* their resilience to cyberthreats. This Good Practices document includes the *maturity model* that we use to assess information security and cybersecurity risk management levels at the institutions under our supervision.

Reader's guide

The Good Practices document is based on the following model:



The Good Practices document can be approached from the following two perspectives.

1. As an overview of the relevant control measures for each of the elements in the model, summarised for managers and policymakers.
   The main control measures that are relevant to an institution are explained in brief, with examples.
   The role of management in implementing and monitoring the control measures is also addressed.

2. As a detailed list of control measures, including additional examples.
   There are links to the relevant control measures under each of the elements in the model. For the sake of readability each control measure is listed under one element in the model only, while a control measure may be relevant to multiple elements.

You can access the elements through the links in the Contents tab. There are also separate tabs for the Q&A on Information security and for the maturity model.

Background

DNB has been researching the quality of information security in the financial sector for several years. Since 2010, this research has been based on periodic self-assessments completed by the institutions subject to our supervision. Our Q&A on the "Assessment Framework for DNB Information Security Examination" provides guidance for completing these self-assessments.

In recent years, the number of potentially very serious cyberthreats for the financial sector and beyond has increased significantly. The financial sector increasingly operates in chains as a result of various forms of outsourcing and partnerships. As a consequence the associated opportunities and risks for information security and cybersecurity are also increasing. During our examinations we have observed many good practices to mitigate these risks.

This prompted us to update our Q&As and compile this Good Practices document. Cybersecurity and information security in outsourcing have been given a more prominent position. Together, this Good Practices document and the Q&A on Information security represent the updated version of the "Assessment Framework for DNB Information Security Examination".

What has changed compared with the previous Assessment Framework?

While the Good Practices document follows the structure of the previous assessment framework[1], it no longer directly links to COBIT.[2] The controls and points to consider from the previous assessment framework are now included as part of the control measures in this Good Practices document. We have also incorporated cybersecurity and outsourcing and we have included practical examples that can help institutions when implementing control measures.

Four new control measures have been added:

1. Employee awareness: Actively promoting employee awareness in the area of cyber risks. See the *People* element, no. 9.3
2. Vulnerability management: Actively monitoring and resolving vulnerabilities in the IT structure and in IT applications. See the *Technology* element, no. 19.2
3. Application Life cycle management: Ensuring timely maintenance and phasing out of applications, so as not to compromise the desired information security level. See the *Technology* element, no. 19.3
4. Penetration testing and ethical hacking: Testing the institution's resilience against cyberthreats. See the *Testing* element, no. 22.1.

A new item in this Good Practices document is the explicit description of the role of management. In addition, the Good Practices document will be part of a feedback loop to be set up in consultation with the sector, in which the institutions involved can provide input to keep the examples in this Good Practices document up-to-date.

Information security and cybersecurity

In this Good Practices document, information security is understood to mean the set of preventive, detective, repressive and corrective controls and the procedures and processes ensuring the availability, exclusivity and integrity of all forms of information within an institution. The aim is to safeguard the continuity and reliability of IT, information and information services and to limit the consequences of security incidents to an acceptable, pre-determined level. The information security procedures and technical measures in place must be appropriate to the nature and objectives of the institution. We regard Cybersecurity as an inseparable part of information security.

[1] For easy recognition, the control measures in this document have the same numbering used in the previous document (2010-2018).

[2] Relevant international standards such as COBIT (Control Objectives for Information and related Technology), ISACA (Information Systems Audit and Control Association), ISO27000 and the NIST Cybersecurity Framework have been incorporated in this Good Practices document and the Q&As.

Scope

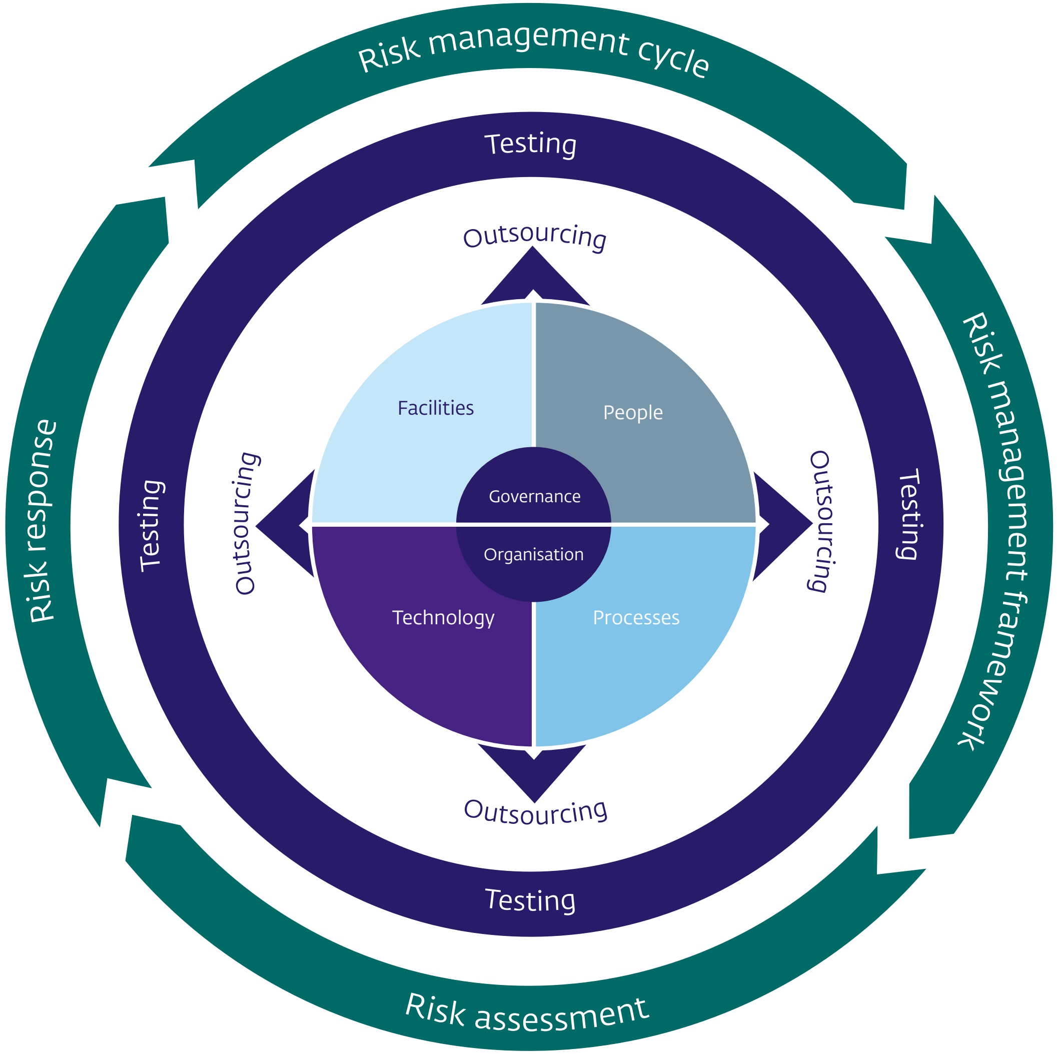
While this Good Practices document is not exhaustive, it explains our views on the correct interpretation of the regulations governing a sound information security and cybersecurity control framework. It is up to the institutions to implement a framework that accurately reflects their nature and size. It cannot be ruled out that some institutions may have to apply the underlying regulations differently or more strictly, or that some parts of this Good Practices document do not apply to them at all.

Disclaimer

This Good Practices document comprises a set of non-binding recommendations. It sets out our expectations regarding observed or envisaged behaviour in policy practice that reflects an appropriate application of the rules regarding information security and cybersecurity.

We encourage institutions under our supervision to take our expectations as well as their own specific circumstances into account in their considerations and decision-making, without them being obliged to do so. Our Good practices documents are indicative in nature and therefore do not alter the fact that some institutions require a non-standard, more strict application of the underlying rules. It is the institution's responsibility to take this into account.

DNB Good Practices - Information security - 2019-2020



Q&A on Information security

Open Book on Supervision, https://www.toezicht.dnb.nl/en/3/51-203304.jsp

Introduction

DNB has been researching the quality of information security in the financial sector for several years. Since 2010, this research has been based on periodic self-assessments completed by the institutions subject to our supervision. Our document "Assessment Framework for DNB Information Security Examination" provided guidance for completing these self-assessments[3]. This Q&A, together with the Good Practices for Information Security document (see under "Related downloads" on this page for a link to this document), serves as an update of the "Assessment Framework for DNB Information Security Examination".

Question:
How can institutions under DNB's supervision comply with the statutory requirements regarding the integrity, continuous availability and security of electronic data processing?

Answer:
In accordance with Section 3:17 of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), in conjunction with Section 20 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*) and the Pensions Act (*Pensioenwet – Pw*, see the relevant links under Law and EU Directives elsewhere on this page), institutions under DNB's supervision must have appropriate procedures and measures in place to control IT risks. These procedures and measures aim to safeguard the integrity, continuous availability and security of electronic data. In this context, "appropriate" means that the procedures and measures are based on the nature, scale and complexity of the risks associated with the institution's activities, and on the complexity of its organisational structure.

In order to comply with these provisions, institutions take measures to control their information security based on a risk analysis. These control measures are not limited to technological solutions (*Technology*), they also address human actions (*People*), *Processes* and *Facilities*.

In addition, institutions assess the design, existence and operating effectiveness of control measures on a regular basis as part of their *Risk management cycle* in order to deal with constantly changing information security and cybersecurity risks. They improve or replace any control measures that are not effective. Institutions set up their *Governance* and *Organisation* in such a way as to steer this process.

Also, institutions ensure that they are in control of information security and cybersecurity regarding outsourced activities (*Outsourcing)* and that they *Test* their resilience to cyberthreats.

The Good Practices for Information Security connected with this Q&A (see the link under "Related downloads") provides institutions with practical guidance in establishing their control measures in the areas of *Governance, Organisation, People, Processes,*

[3] https://www.toezicht.dnb.nl/en/3/51-203304.jsp

Technology, *Facilities*, *Outsourcing*, *Testing* and the *Risk management cycle*. The document contains a selection of recommended control measures to put the requirements of Section 3:17 of the *Wft* in conjunction with Section 20 of the Decree on Prudential Rules for Finacial Undertakings and the Pension Act into practice.

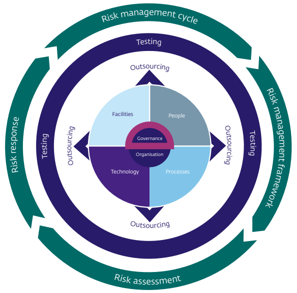
Relevant laws and regulations

- Financial Supervision Act (Wet op het financieel toezicht – Wft)
  - Section 1:1: definitions
  - Section 3:17(1): sound and ethical business operations
  - Section 3:17(2): managing business processes and operational risks
- Decree on Prudential Rules for Financial Undertakings (Besluit prudentiële regels Wft – Bpr)
  - Section 17: a financial institution is defined as a payment institution, clearing institution, special purpose reinsurance vehicle, credit institution, premium pension institution, insurer or branch office
  - Section 20(2): procedures and measures in place to ensure the integrity, continuous availability and security of electronic data processing.
- Pensions Act
  - Section 143(1): safeguarding sound and ethical business operations
- Mandatory Occupational Pension Scheme Act
  - Section 138(1): safeguarding sound and ethical business operations
- Good practice document on outsourcing for insurers, published by De Nederlandsche Bank N.V., August 2018
- Guidance document on outsourcing for pension funds, published by De Nederlandsche Bank N.V, June 2014

* DNB is of the opinion that the corresponding applicability to pension funds and occupational pension funds of the general standard to have an organisational structure in place that ensures sound and ethical business operations entails that where applicable and with due observance of the principle of proportionality these institutions must also have in place procedures and measures to ensure the integrity, continuous availability and security of electronic data processing.

# We will add relevant laws and regulations issued by EIOPA and EBA once these have entered into effect.

Governance



What we mean by this element

Governance is about the strategic, tactical and operational management of information security and cybersecurity in line with the institution's strategy, its risk appetite and the applicable legal and regulatory requirements. The nature, size and complexity of the institution is taken into consideration.

Relevant control measures

For the *Governance* element, we check whether an institution has drafted an information security policy, how it is implemented and kept up to date, and whether it is translated into a comprehensive information security plan with a clear distribution of tasks and responsibilities and formal reporting lines. Resilience to cyberthreats should be specifically addressed in the policy. We check to what extent the policy has been translated into preventive, detective, corrective and repressive measures and whether the institution monitors relevant developments regarding information security and cybersecurity.

We also check whether the set-up of processes and IT systems is in line with the institution's information architecture. The architecture should make clear how the IT systems and data collections support the institution's strategy and processes. The institution could use a classification table[4] listing the relevant security controls regarding data access, encryption, storage and retention, for example. The institution works according to generally accepted technical standards in the area of information security and cybersecurity.

Role of management in implementing these control measures

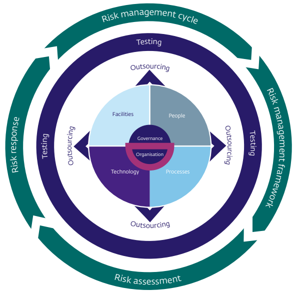
The institution's management board bears ultimate responsibility for governance and ensures the effective management of all aspects of information security and cybersecurity. For example:

- The management periodically establishes an information security policy, along with an information security plan in which the requirements set by the management and the risk and compliance functions have been translated into concrete measures to be taken.
- As part of the Risk management cycle, the management periodically ascertains that the institution's information security and cybersecurity risks are still in line with its risk appetite, for example by considering whether the measures it has in place – *People*, *Processes*, *Technology* and *Facilities* – are effective to mitigate the risks.
- In the event of a major incident, the management is adequately informed about the response, and coordinates the response if necessary. After the incident, the management evaluates it and integrates the outcomes of its evaluation in the risk management cycle.
- Good commissioning: the management ensures that the institution monitors its service providers' compliance with the agreements made in accordance with the information security policy and, if applicable, the implementation of the information security plan.

[4] A table indicating the institution's availability, integrity and confidentiality requirements for IT systems and data.

Control measures:

Organisation



What we mean by this element

Organisation is about the allocation of duties and responsibilities regarding information security and cybersecurity within the institution. This should be clear and unambiguous, and any related activities must be in line with the institution's strategy, its risk appetite and the applicable legal and regulatory requirements.

Relevant control measures

For the *Organisation* element, we check the effective documentation and formalisation of roles and responsibilities for risk management and information security functions. The institution has allocated the duties, responsibilities and competences regarding information security at all levels within the organisation. For example, it has established and communicated rules of conduct, describing how its employees must handle information with due care (e.g. secure passwords, email, a clean desk policy).

We also check the clear allocation of ownership of the data and information systems that the institution uses in its operational management. We check the institution's access rights management regarding data and information systems, according to the principle of segregation of duties in line with the institution's internal control structure.

For example, the institution has a risk-based overview of the segregation of duties for IT applications and, if a process is supported by multiple IT applications, also for each process. This prevents the segregation of duties from being breached at a process level even if the requirements are met at the individual IT application level.
At the same time, institutions should limit the number of high-privileged accounts. This approach will prevent toxic combinations of access rights (undesirable combinations of roles and access rights) and related risks.

Role of management in implementing these control measures

The institution's management board bears ultimate responsibility for an effective organisation of duties, responsibilities and powers and ensures the effective management of all aspects of information security and cybersecurity. For example:

- The management has clearly allocated the duties and responsibilities regarding the organisation, management and control of information security and cybersecurity.
- The management ensures that toxic combinations and the associated risks are avoided in the institution.
- The institution has sufficient capacity, knowledge and expertise available to fulfil these duties and responsibilities, based on the institution's risk profile and the management's risk appetite.
- The management actively propagates the importance of information security and cyber-security within the institution and at its service providers.
- Good commissioning: the management ensures that the institution monitors its service providers' compliance with agreements on the allocation of duties and responsibilities regarding information security and cybersecurity, ownership of data and information systems, and segregation of duties.

Control measures:

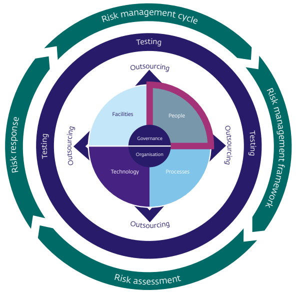
5.1 Responsibility for risk, security and compliance

5.2 Management of information security

6.1 Data and system ownership

7.1 Segregation of duties

People



What we mean by this element

People is about ensuring that all employees, external staff and service providers are aware of the institution's information security policy and of their own responsibilities in this regard, and that they work in line with this policy and the institution's risk tolerance.

Relevant control measures

The human factor is crucial to the management of information security and cybersecurity risks. For the *People* element, we check the institution's ability to recruit and retain personnel with adequate knowledge of information security and cybersecurity that is in line with its ambition and risk profile. We expect the institution to invest in education and training to keep its personnel's knowledge of information security and cybersecurity up-to-date. Basic knowledge of information security and cyberthreats is shared across the institution. In-depth knowledge is shared with IT managers and information security specialists. The institution has set up security awareness programmes to draw explicit attention to cyberthreats. The institution shares its knowledge on cyberthreats with other institutions and authorities, for example through participation in forums such as the sectoral Information Sharing and Analysis Centres (ISACs), in which information about cybersecurity threats and attacks is shared confidentially.

We also check whether institutions, based on their risk tolerance and risk analysis, determine if and to what extent they may be relying too much on the knowledge of information security and cybersecurity resting with individuals. The institution has taken measures to ensure it limits excessive dependence on individuals (key person risk).

In addition, we check whether institutions carry out pre-employment screening of internal and external personnel, depending on the risk profile of their positions. They are rescreened on a regular basis during the period of employment or insourcing. If the employment or insourcing relationship ends or changes, any access rights associated with the old position are revoked as soon as possible.

Role of management in implementing these control measures

The institution's management board bears ultimate responsibility for maintaining an appropriate level of knowledge among its personnel and ensures the effective management of all aspects of information security and cybersecurity. For example:

- The institution's management board has at least basic knowledge of information security and cybersecurity. They have followed training courses or educational programmes in order to be able to understand the most important IT risks and control measures for their institution.
- The management board sets the standard in terms of awareness of information security and cybersecurity risks and compliance with the procedures to ensure information security (tone-at-the-top). Management overrides of existing processes and procedures by the management board and senior management are avoided where possible.
- Good commissioning: the management board must ensure that the institution monitors its service providers' compliance with the personnel aspects of information security and cybersecurity.

Control measures:

8.1 Personnel recruitment and retention

8.2 Personnel competencies

8.3 Dependence upon individuals

8.4 Personnel clearance procedures

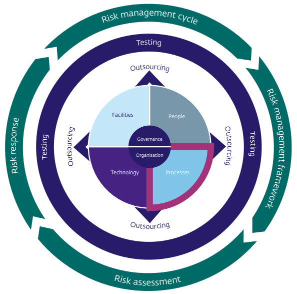
8.5 Job change and termination

9.1 Knowledge transfer to end users

9.2 Knowledge transfer to operations and support staff

9.3 Employee awareness

Processes



What we mean by this element

Processes is about facilitating sound operational management. Processes are essential for controlling the risks related to information security and cybersecurity.

Relevant control measures

For the *Processes* element it is important that the institution has drafted an IT continuity plan and keeps this plan up-to-date. The aim of the plan is to limit the impact of a major disruption on the institution's key operational functions and processes, and to promote the continuity of its information security functions during disruptions or cyberattacks. We check how the institution deals with security and cybersecurity incidents, with to the aim of limiting any resulting damage and preventing the incident from recurring. We check whether the institution has in place a formal policy for incident management, including an escalation procedure and escalation criteria. Cybersecurity incidents must be reported to the relevant authorities in accordance with applicable laws and regulations. How incidents are resolved is regularly analysed to improve processes and IT systems. An example includes setting up a Computer Emergency Response Team (CERT).

We also check that institutions implement changes in a controlled manner, in order to prevent such changes from resulting - either intentionally or unintentionally - in a lower information security level, leading to disruptions in operational processes or having a negative impact on data integrity. The institution ensures that changes in IT applications, IT infrastructure, IT processes and critical system parameters must be implemented using a standardised and controlled path, in which they are registered (audit trail), approved and evaluated.

We also check that criteria for the protection of production and test data are set out and followed, and that test data and production data are segregated. Changes are tested according to a test plan with acceptance criteria, including for security and IT performance.

We also look at the way in which the institution safeguards the quality of its IT processes. The institution implements and maintain procedures amongst other things.

- configuration (maintaining and updating the institution's IT systems including its parameter settings),
- back-up and recovery of systems and data,
- availability of data and back-up data at an external location,
- storage, archiving and destruction of data in accordance with statutory and regulatory requirements,
- removal, transfer, processing and distribution of sensitive data,
- compliance with current legal and regulatory requirements,
- access to the institution's information systems and data.

We check whether the institution receives regular independent assurance on the effective functioning of control measures, for instance in the form of a report from the internal or external auditor, with an opinion on the design, existence and effective operation of control measures during a certain period.

Role of management in implementing these control measures

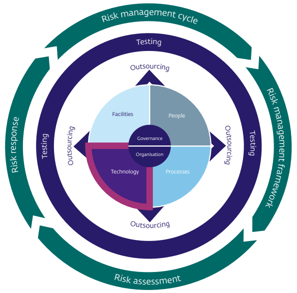
The management board bears ultimate responsibility for ensuring that the institution's strategy and overall IT security plan are in line with the board's guidelines and operational processes. For example:

- The Management Board instructs its staff to check on an annual basis whether the IT continuity plan is still in line with the IT environment, and to report on this.
- The Management Board actively participates in continuity tests and ensures that current cyberthreats are incorporated in the continuity plans (scenarios).

Control measures:

- 10.1 Change standards and procedures
- 10.2 Impact assessment, prioritisation and authorization
- 10.3 Test environment
- 10.4 Testing of changes
- 10.5 Promotion to Production
- 11.1 IT Continuity plans
- 11.2 Testing of the IT Continuity plan
- 11.3 Offsite backup storage
- 11.4 Backup and 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 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 Management
- 17.2 User account management

Technology



What we mean by this element

Technology is about taking technical measures to control information security and cybersecurity.

Relevant control measures

For the *Technology* element, we check that technical control measures are implemented so as to safeguard a high level of availability, exclusivity and integrity and that the institution's risk analysis take current cyberthreats into account. Examples include the SANS[5] Top 20, the NCSC's[6] and ENISA's[7] threat analyses and the outcomes of penetration testing and ethical hacking. We check whether maintenance of the IT infrastructure and IT applications is a structured and planned process, in line with the institution's change management procedures and life cycle management process.

For example, the institution ensures that technological obsolescence of its IT infrastructure and IT applications remain within its risk tolerance limits and that security updates are implemented. We also check that institutions know on which part of the IT infrastructure and on which IT applications their operational processes depend, and that they are aware of the degree to which their IT systems are vulnerable to cyberattacks. For example, an institution can carry out regular vulnerability scans of its IT infrastructure and IT applications based on a risk analysis and threat intelligence.

The institution implements preventive, detective and corrective controls to protect its IT systems against cyberattacks such as viruses, malware, cryptoware, spyware and DDoS attacks. As regards preventive controls we check whether the institution applies up-to-date technical security measures (e.g. firewalls, network segmentation and intrusion detection) and whether it has the associated procedures in place to restrict access to the IT infrastructure to authorised persons. The institution applies modern firewall technologies in line with generally accepted standards such as GovCert, ISO/IEC[8] and ITSEC[9].
The institution has a policy that defines the rules for sharing confidential information. For example, confidential data on laptops should be encrypted and Data Loss Prevention software should be used to check the confidentiality of outgoing messages. The institution must manage its encryption keys in a controlled way.

We monitor that an institution's focus on customer experience and time-to-market does not lead

[5] System Administration, Networking and Security Institute. See https://www.sans.org/

[6] National Cybersecurity Centre. 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

[9] Information Technology Security Evaluation Criteria. See https://www.itsec.org

to postponement of security measures and of investments in the reduction of any technological debt.

Role of management in implementing these control measures

The institution's management board is responsible for establishing and implementing the institution's IT strategy. For example:

- The management board ensures that it is kept informed of the risks in the area of information security and cybersecurity and of new technological developments (which in turn may bring new opportunities as well as risks in the areas of information security and cybersecurity).
- The management board weighs these risks in the Risk Management Cycle, see the relevant element in the model.

Control measures:

18.1 Infrastructure resource protection and availability

18.2 Infrastructure maintenance

18.3 Cryptographic key management

18.4 Network Security

18.5 Exchange of sensitive data

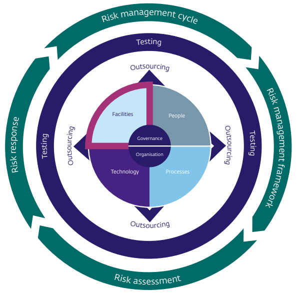
19.1 Malware prevention, detection and correction

19.2 Vulnerability assessment

19.3 Application Life cycle management

20.1 Protection of security technology.

Facilities



What we mean by this element

Facilities is about ensuring the physical security of access to data, e.g. measures to restrict access to office buildings and data centres.

Relevant control measures

For the *Facilities* element, we check whether the institution has established and implemented a policy that is updated on a regular basis and is in line with the institution's risk profile with respect to the following aspects:

- 1. physical security of office buildings, grounds and critical IT infrastructure locations such as data centres and server rooms.
- 2. access to buildings and locations that are critical to the institution's operational processes.

The institution should also take measures to protect its security systems. Examples include additional physical access security measures, strict network segmentation, a stricter patch regime and swift follow-up of alerts and incidents that relate to security sytems.

We also check whether the institution tests the effectiveness of its physical access security measures on a regular basis and reports the outcomes to senior management. For example, the institution could use a "mystery guest" to test the physical access security measures.

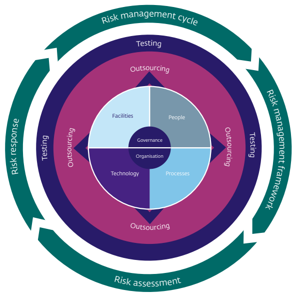
Role of management in implementing these control measures

The management board is responsible for establishing, implementing and checking the institution's policy. For example:

- The management board demonstrates its commitment to adequate physical access security and implements risk profile-based measures at all locations.
- The management board ensures it is kept informed and reminds the organisation of its obligations in case of any breaches (tone at the top).

Control measures:

Outsourcing



What we mean by this element

Outsourcing is about engaging the services of third parties to operate important operational processes such as IT, asset management and customer, pensions, policy and financial administration. Outsourcing processes brings benefits, but also exposes institutions to risks. For example, a service provider may not handle the institution's confidential data in the appropriate way which could lead to reputational damage to the institution. Another risk is that the security of confidential data is not in line with the institution's internal policy due to subcontracting by the service provider.

Relevant control measures

In case of outsourcing of activities, the institution still bears ultimate responsibility for information security and cybersecurity. For the *Outsourcing* element, we check whether the institution has a process in place to ensure at least the following.

- The institution has made agreements with the service provider to ensure compliance with the institution's information security policy and, if applicable, the execution of the information security plan. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

This Good Practices document includes three control measures (14.1, 14.2 and 16.3) with a specific focus on outsourcing.

We check whether the institution and its service providers have made agreements on specific performance criteria, whether these agreements are monitored and whether the outcomes are reported to the relevant stakeholders. The institution analyses the reports submitted by its service providers to identify relevant trends and developments and to steer service provision if necessary.

In the agreement preparation phase, the institution should specify how the service provider will continue to meet its contractual obligations and comply with rules and regulations, and how it is ensured that outsourcing does not obstruct supervision. Together with its service providers, the institution must perform a risk analysis and agree on how to deal with any residual risks. The analysis should address the risks associated with the parties to which activities are subcontracted.

The institution and its service providers must also establish an exit plan with agreements on the orderly termination of services. The exit plan must specify how the institution's data (including back-ups) are to be removed following the termination of services, including in the event of subcontracting.

This Good Practices document also includes examples of measures to control outsourcing.

Role of management in implementing these control measures

The institution's management board bears ultimate responsibility for effective management of outsourced activities by making contractual agreements with service providers, monitoring compliance with these agreements and making the necessary adjustments in the event of deviations from the agreements. For example:

- The management board evaluates the institution's outsourcing policy at least once a year and discusses the outsourcing strategy also from the perspective of information security. Based on the evaluation, the management board adjusts the policy if necessary, or decides to adjust or terminate existing outsourcing agreements.

- When making decisions about the outsourcing strategy, the management board also takes into account the associated information security risks, and how they are to be controlled on an ongoing basis.

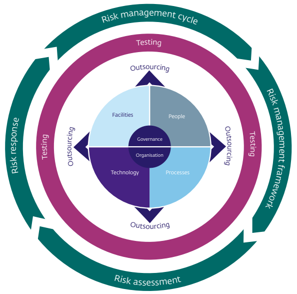
Control measures:

14.1 Monitoring and reporting of Service Level Achievements

14.2 Supplier risk management

16.3 Internal control at third parties

Testing



What we mean by this element

Security testing is about effectively improving the institution's information security and cyber resilience on an ongoing basis. Security tests can be applied to various elements in the model. Tests can be used to detect weaknesses in e.g. the institution's infrastructure (*Technology*), but also in human behaviour and human acts (*People*) or in access to buildings (*Facilities*). The scope of Security testing includes the internal organisation, but may also include major outsourcings.

Relevant control measures

For the *Security testing* element we check that the institution determines the security tests to be performed, as well as their scope and depth, based on a risk analysis and current cyberthreats. The nature and frequency of testing depends on the institution's risk profile. For example, the institution can perform or have a third party perform several types of security tests, such as pen tests targeting infrastructure and application security, red teaming, physical security tests and human behaviour tests in relation to information security and cybersecurity. These tests can be performed by internal or external parties.

We check whether the institution has ascertained that the party performing the tests has adequate knowledge and experience and is certified to do so. For example, the institution makes an annual security testing plan based on a risk analysis.

Role of management in implementing these control measures

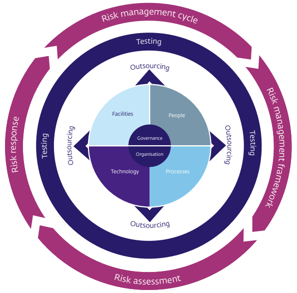
The institution's management board bears ultimate responsibility for initiating, monitoring and performing security testing. For example:

- The management board makes available sufficient resources to perform periodic security tests.
- The management board checks whether the scope of these security tests includes the various elements that are presented in the model in this Good Practices document and takes them into account when tests are performed.
- The management board ensures that the outcomes of security tests are discussed in the Supervisory Board. The management board takes appropriate measures to follow up on any residual risks identified.

Control measures:

22.1 Penetration testing and ethical hacking

Risk management cycle



What we mean by this element

The *Risk management cycle* applies to all elements in the model. The institution must identify and analyse the relevant information security and cybersecurity risks on a regular basis. Based on the risk analysis, the institution determines its response, takes measures to mitigate the risks and (temporarily) accepts the residual risks. Accepted residual risks are evaluated periodically to update the risk response (e.g. mitigate, terminate or accept).

Relevant control measures

For the *Risk management cycle* element, we check whether the institution has implemented an IT Risk Management Framework to safeguard its control of information security and cybersecurity risks. The framework must be based on a Plan-Do-Check-Act cycle, and the outcomes must be reported to the Management Board on a regular basis. We check whether the institution uses uniform definitions of information security and cybersecurity in its IT Risk Management Framework based on market standards such as NIST, ISO and COBIT, and that they are used consistently throughout the institution's documents and reports. For example, the institution's IT Risk Management Framework must address current cyberthreats such as malware, cryptoware, DDoS attacks and phishing.

We also check that the institution carries out periodic Risk assessments based on qualitative and quantitative methods, in which current cyberthreats are analysed and prioritised. For example, the institution has an overview of its "crown jewels", relate them to current cyberthreats and evaluates them on a regular basis. The institution takes additional control measures where needed. The institution also specifies which risks it formally considers to be acceptable. It should adjust, replace or terminate any control measures that are ineffective.

We also check whether the institution has drafted a risk action plan for unacceptable risks, setting out the institution's risk response. The risk action plan should be approved by the Management Board, and it should be appropriate to the nature and scale of any residual risks. For example, for all current cyberthreats, the institution has explicitly specified which risks are formally accepted and for which residual risks additional measures are needed.

We check that the institution's 1st, 2nd and 3rd line are actively involved in the set-up, implementation and support of the Risk Management Cycle.

Role of management in implementing these control measures

The institution's management board bears ultimate responsibility for initiation, implementation and termination of the measures following from the Risk Management Cycle. For example:

- The management board has established a Risk Management Cycle and is kept informed re information security risks and cyberthreats on a regular basis.
- The management board periodically evaluates the Risk Management Framework and the effectiveness of the information security measures included in this framework, taking current trends and risks into account. Insurers do so in the context of the ORSA, pension funds in the context of the ORA and banks in the context of ICAAP.

- The management board makes available sufficient resources for taking effective measures, based on the institution's risk profile and the management board's risk appetite.
- The management board periodically assesses the information security and cybersecurity risks to which the institution is exposed against the risk tolerance limits it has set.
- The management board periodically assesses whether the mix of measures (comprising the people, processes, technology and facilities elements) is effective to comprehensively mitigate the institution's information security and cybersecurity risks.

Control measures:

4.1 IT Risk Management framework

4.2 Risk assessment

4.3 Maintenance and monitoring of a risk action plan

Maturity Model

As explained in the introduction to this Good Practices document, we have been examining the quality of information security in the financial sector on a thematic basis for many years now. In the context of this thematic examination we ask the institutions subject to our supervision to complete periodic self-assessments, which measure institutions' operational maturity levels.

The aim of the self-assessments is to establish whether their control of information security and cybersecurity is at the required level. We use a Maturity Model[10] to determine this level. We expect financial institution to be in control, and to be able to demonstrate this. In the model we use, which contains 58 control measures, this corresponds to a maturity level score of at least 3, i.e. verifiable long-term operational effectiveness, for 55 control measures and a maturity level score of at least 4 for the remaining 3 control measures – controls #4.1, #4.2 and #4.3 in the Risk Management Cycle.

The institution takes the definitions from the table below into account when completing the self assessment.

The first column lists the maturity levels, from 0 to 5. The second column contains the maturity level definitions we use in our supervisory examinations. The third column lists explanatory criteria for each maturity level.

The difference between levels 3 and 4 is that at level 3, a control is implemented and effective, while level 4 additionally includes a verifiable evaluation of a control's effectiveness and any follow-up measures resulting from this evaluation.

[10] The maturity level definitions are based on "CobiT 4.1 Research, 2007, Appendix III—Maturity Model for Internal Control, page 175". We have been using these definitions since 2014.

Definitions of maturity levels

Level	Definition Maturity level:	Criteria for clarification:
0	**Non-existent –** No attention has been paid to this control.	
1	**Initial –** The control is (partially) defined but is performed in an inconsistent manner. There is a great dependence on individuals re the implementation/execution of the control.	■ No or limited control implemented. ■ No or ad hoc control execution. ■ Control is not / partially documented. ■ Implementation / execution is dependent on individuals (not standardised)
2	**Repeatable but intuitive –** The control is in place and is executed in a structured and consistent, but informal, manner.	■ The implementation of the control is based on an informal but standardised approach. This approach is not fully documented.
3	**Defined –** The control is documented and executed in a structured and formal manner. The execution of the control can be proved, is tested and effective.	■ The control is defined based on a risk assessment. ■ The cntrol is documented and formalised. ■ Responsibilities and tasks are clearly assigned. ■ Design, existence and effective operation are demonstrable. ■ The operational effectiveness of the control is tested periodically. ■ The assessment of the operational effectiveness of controls is risk-based and demonstrates that the control is effective for a longer period in time (> 6 months). ■ The implementation of the control is reported to management.
4	**Managed and measurable –** The effectiveness of the control is periodically assessed. Where necessary, the control is improved or replaced by other control(s). The assessment is documented.	Criteria for level 3 plus the following distinguishing criteria: ■ Periodic (control) evaluation and follow-up takes place. ■ Evaluations are documented. ■ Tasks and responsibilities re evaluation of controls are formalised. ■ The frequency of evaluation is based on the risk profile of the institution and is at least annually. ■ Operational incidents are taken into account in the evaluation. ■ The results of the evaluation are reported to management.
5	**Continuous improvement –** The control is embedded in the integral risk management framework of the institution that ensures continuous and effective control and risk issues resolution. External data and benchmarking is used to support the continous search for improvement. Employees are proactively involved in improving the effectiveness of controls.	Criteria for level 4 plus the following distinguishing criteria: ■ Continuous evaluation of controls in order to continuously improve the effectiveness of the controls. ■ Making use of the results from self-assessments, gap analyses and root cause analyses. ■ The controls are benchmarked on the basis of external data and are “Best Practice” in comparison with other organisations.

1.1 Information security plan

Good Practices

The institution has a process in place to ensure at least the following:

- Requirements regarding the availability, integrity and confidentiality of information are based on business objectives, operational processes, risk and compliance and are translated into an information security policy and, consequently, an information security plan.
- The information security policy and plan are tied to the institution's operational strategy as well as to its nature and size (proportionality).
- The information security policy addresses the institution's resilience against cyberthreats.
- The information security policy is updated on a regular basis and shared with internal and external stakeholders.
- The institution monitors the execution of the information security plan.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line of defence functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for drafting the information security policy and information security plan, and for monitoring compliance. The institution has set up a process which ensures at least the following (see our Good Practices for outsourcing[11]):

- The institution has made agreements with the service provider to ensure compliance with the institution's information security policy and, if applicable, the execution of the information security plan. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has drafted its information security policy in line with internationally accepted standards such as ISO27001/2 and the NIST cybersecurity framework.
- The information security policy comprises preventive, detective, corrective and repressive measures. In the NIST cybersecurity framework, this is expressed in the *Identify*, *Protect*, *Detect*, *Respond* and *Recover* phases.
- The institution's information security policy describes both IT technical measures and procedural measures in operational processes.
- The institution updates its information security policy with a fixed frequency that is appropriate to the institution's nature and size (e.g. every two years), and increases the frequency when necessary, for example in the event of mergers and takeovers, major outsourcing or new cyberthreats.
- Through awareness programmes, the institution's employees are familiar with the information security policy and know their roles and responsibilities in this respect.

[11] https://www.toezicht.dnb.nl/en/2/51-237170.jsp

1.2 IT Policies Management

Good Practices

The institution has a process in place to ensure at least the following:

- Measures derived from the information security policy and plan are part of standardised, predictable IT working processes (sound business and IT operations).
- IT working processes and procedures ensure controlled IT system development, acquisition of secure hardware and software from reliable sources, data processing and storage, IT system maintenance and IT support.
- Emergency procedures are in place to deal with non-standard situations.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for ensuring sound execution of outsourced IT working processes and procedures. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the sound execution of IT working processes and procedures in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has described and/or set up IT working processes in workflow tooling to ensure the sound execution of these IT working processes and procedures. For example, the workflow tooling enforces the application of the four-eyes principle in the event of adjustments in critical IT systems, system parameters or data and ensures that all activity can be tracked (logging).
- Procedures are based on internationally accepted standards such as ITIL, BISL and PRINCE II.
- The institution updates its IT working processes and procedures with a fixed frequency that is appropriate to the institution's nature and size (e.g. every two years), and increases the frequency when necessary, for example in the event of mergers and takeovers, outsourcing of IT working processes or incidents. If new cyberthreats arise, or if the intensity of cyberthreats increases, the institution assesses whether IT working processes and procedures must be tightened.
- The institution checks to what extent its staff and insourced employees adhere to the IT working processes in place and to what extent they are aware that a proper execution of their activities contributes to information security and resilience against cyberthreats.

2.1 Enterprise Information Architecture Model

Good Practices

The institution has a process in place to ensure at least the following:

- Operational processes and IT systems are set up in line with the institution's information architecture, which in any case addresses the following:
  - Vision on information services;
  - Target architecture of IT systems and processes;
  - Cybersecurity and privacy requirements;
  - System and data classification;
  - Rationalisation of current IT systems; phasing out legacy IT systems and systems that are vulnerable to cyberthreats.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for the set-up and security of its information architecture, also in the event of outsourcing. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider to ensure compliance with its information architecture. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution's information architecture clarifies how the IT systems and data collections support the institution's operational strategy and processes.
- The institution's information architecture is based on internationally accepted standards such as TOGAF and DYA.
- The institution has developed a vision showing how its IT systems and organisational structure will evolve in support of its medium to long-term operational strategy, including an overview of key dependencies on third parties/partners.
- The institution applies architectural principles aimed at enabling easy, flexible, reliable and secure provision of information to authorised staff, customers and third parties.

2.2 Data classification scheme

Good Practices

The institution has a process in place to ensure at least the following:

- The institution's management has established the ownership of systems and data.
- The institution has established a classification policy.
- Based on a risk analysis, the institution has classified its IT systems and data in categories reflecting the degree of availability, integrity and confidentiality of these systems and data.
- The institution uses a classification table listing the relevant security controls for data access, encryption, storage, retention and cleansing, for example.
- The institution regularly checks whether its employees comply with the classification policy.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for drafting the classification policy, and for compliance with the policy.

The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning compliance with the classification policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has set up a risk-based data classification table in which all IT systems and data are classified in categories such as high/medium/low risk and public/confidential/secret.
- The institution takes measures based on this classification, such as encrypted storage of data in the "secret" category.
- The institution monitors the data centre locations in which its business-critical data are stored. The institution periodically establishes that these locations are in compliance with its information security policy.
- The institution uses DLP software to actively monitor outgoing traffic of sensitive data through the institution's network and whether this is in compliance with the data classification.

3.1 Monitor future trends and regulations

Good Practices

The institution has a process in place to ensure at least the following:

- The institution monitors trends in the sector, e.g. in the area of cybersecurity.
- The institution receives timely information about cyberthreats (threat intelligence).
- The potential impact of these trends and threats is assessed and appropriate measures are taken to mitigate any risks ensuing from them.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for monitoring relevant legislation and regulations, trends and developments. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the monitoring of relevant legislation and regulations and trends in the area of cyberthreats and cybersecurity in line with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Employees are active on internet forums and/or subscribed to cybersecurity newsletters.
- The institution engages the services of an external security intelligence service provider.
- The institution is a member of professional or other sectoral associations that share knowledge and expertise in the area of cybersecurity, such as ISACs.
- The institution has made contractual agreements with its key outsourcing partners about cooperation and exchange of information in the area of information security and cybersecurity.

3.2 Technology standards

Good Practices

The institution has a process in place to ensure at least the following:

- The institution works according to generally accepted technical standards in the area of information security and cybersecurity. These are tailored to the nature and the size of the institution.
- Employees are informed of the requirement to work according to set standards and they are aware of the standards that are relevant to their work.
- New IT systems and changes to existing IT systems comply with the established standards.
- The institution monitors whether the established standards are complied with.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for working in accordance with established standards. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service providers about working in accordance with established standards. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution works according to internationally accepted standards for information security and cybersecurity such as ISO27001/2, NIST cybersecurity framework and/or SANS.
- The standards have been communicated to internal and external employees, including IT security officers, IT architects, project managers, software developers, functional and technical administrators, IT risk managers and IT auditors.
- The institution's IT security officer assesses new standards in the area of information security and cybersecurity and provides advice on how these may strengthen the institution's information security and cybersecurity measures.
- The institution's formalised IT architecture and standards also apply to the institution's service providers. The institution periodically assesses whether its service providers have set up their IT environment in accordance with these standards.
- The institution annually assesses its IT infrastructure and IT application landscape against current security baselines and market standards.

4.1 IT Risk Management Framework

Good Practices

The institution has a process in place to ensure at least the following:

- The institution develops and maintains an IT Risk Management Framework.
- The IT Risk Management Framework is in line with the institution's general Risk Management Framework.
- The institution addresses information security and cybersecurity risks in its IT Risk Management Framework.
- The institution has established and laid down its risk tolerances regarding information security and cybersecurity.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for managing the IT risks related to its outsourced activities and systems. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the management of IT risks in accordance with the institution's policy and risk tolerances. These agreements also apply if the activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded.

Examples of this include:

- The institution applies uniform definitions of information security and cybersecurity in its IT Risk Management Framework. These definitions are derived from market standards such as NIST CF, ISO 27000 and CobiT and are consistently applied in all IT Risk Management Framework documents and reports.
- Current cyberthreats such as malware, cryptoware, DDoS attacks and phishing are part of the risk management framework.
- Service providers in the outsourcing chain work in accordance with the institution's IT Risk Management Framework.
- The institution periodically assesses whether the parties to which activities and systems are outsourced are working in accordance with the institution's IT Risk Management Framework.
- The institution has a comprehensive overview of information security and cybersecurity risk management based on internal reports and reports from service providers.

4.2 Risk assessment

Good Practices

The institution has a process in place to ensure at least the following:

- The institution periodically carries out IT risk analyses based on qualitative and quantitative methods.
- creating an overview of the opportunities and impact associated with the inherent risks and residual risks related to information security.
- Current cyberthreats are included in these IT risk analyses.
- Residual risks are reported for (temporary) approval to the management level that is relevant to the nature and scale of these residual risks.
- Accepted residual risks are reassessed for acceptance on a periodical basis if they are outside the institution's risk tolerance limits.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for the analysis of risks in the area of information security and cybersecurity related to the outsourced activities and systems. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for carrying out risk analyses in access rights in accordance with the institution's risk management framework. These agreements also apply if the activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution annually carries out an IT risk analysis among all relevant stakeholders within the institution. Current cybertreats are weighted and prioritised based on this risk analysis.
- The institution creates an overview of its "crown jewels", evaluates them on a regular basis and relate them to current cyberthreats and risk management controls. The institution should take additional control measures where needed. It should adjust, replace or terminate any control measures that are ineffective or no longer adequate.
- The institution periodically assesses the risk analyses of parties in the chain for relevance and establishes to what extent they meet the institution's requirements.
- The institution addresses the weighted and prioritised information security and cybersecurity risks and reduces them to a level that is acceptable with respect to the institution's risk tolerance limits.

4.3 Maintenance and monitoring of a risk action plan

Good Practices

The institution has a process in place to ensure at least the following:

- The institution drafts a risk action plan for unacceptable risks, detailing the institution's risk response.
- The risk action plan describes any residual risks and includes compensatory measures.
- Residual cybersecurity risks are part of the institution's risk action plan.
- The risk action plan is approved at a management level that is appropriate to the nature and scale of the residual risks.
- The risk action plan is up to date and follow-up of actions is monitored.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for mitigation of unacceptable residual risks in the area of information security and cybersecurity related to the outsourced activities and systems. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for carrying out risk analyses in access rights in accordance with the institution's risk management framework. These agreements also apply if the activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- For all current cyberthreats, the institution has explicitly specified which risks are formally accepted and for which residual risks additional measures are needed.
- Proposed measures and their implementation status are described in the risk action plan. Deviations from the original schedule are periodically reported to the institution's senior management. The institution's line management draws up an in control statement (ICS) each year.
- The institution periodically assesses the relevance of the risk action plans of service providers in the chain for compliance with its requirements. If any deviations are found, the institution makes agreements to reduce the risk to an acceptable level within the institution's risk tolerance limits.

5.1 Responsibility for risk, security and compliance

Good Practices

The institution has a process in place to ensure at least the following:

- Ultimate responsibility for managing information security and cybersecurity risks rests with the institution's highest management level.
- The duties and responsibilities of the risk management and information security functions are formalised and documented.
- The institution's employees are aware that they are responsible for maintaining compliance with security processes and procedures.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution monitors that the responsibility for information security and cybersecurity also rests with the service providers in the outsourcing chain. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning change standards and procedures in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution's Management Board visibly and actively endorses the importance of information security and cybersecurity.
- The institution has allocated the duties, responsibilities and powers regarding information security at all levels within the organisation.
- The institution has appointed a Chief Information Security Officer (CISO) who reports directly to the Management Board.
- Specific responsibilities in the area of information security and cybersecurity are allocated to a Computer Emergency Response Team (CERT) or Security Operations Centre (SOC).
- The institution ensures that the topics mentioned above apply to its chain partners, both when entering into a relationship with a partner and when monitoring that relationship.

5.2 Management of information security

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has established a Plan-Do-Check-Act cycle for managing its information security and cybersecurity risks.
- The execution of the cycle is risk-based, aligned to the institution's objectives and in accordance with the institution's risk tolerance limits.
- The 1st, 2nd and 3rd line are actively involved in establishing and executing the Plan-Do-Check-Act cycle for managing information security and cybersecurity risks, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for the execution of the Plan-Do-Check-Act cycle for managing information security and cybersecurity risks. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the service provider's role in the Plan-Do-Check-Act cycle in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution uses internationally accepted standards such as the ISO 27000 series for setting up its information security and cybersecurity structure.
- Information security and cybersecurity are part of the 1st, 2nd and 3d line's duties and responsibilities. This is reflected in organisation charts and job descriptions.
- The institution discusses the management of information security and cybersecurity risks with its service providers on a regular basis to check whether there are points for improvement in the chain (PDCA cycle).
- The 1st, 2nd and 3d line (at the institution and at the service providers) all provide input to these regular discussions.
- The outcomes of the Plan-Do-Check-Act cycle for managing information security and cybersecurity are reported to the Management Board on a regular basis.

6.1 Data and system ownership

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has clearly allocated the ownership of the data and information systems that it uses in its operational management.
- Data and information systems are classified by the relevant system owner. Control measures are established in accordance with this classification. See control measure 2.2.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for ensuring that the ownership of data and information systems is clearly allocated. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the ownership of data and information systems in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has defined rules concerning ownership, storage locations, retention periods and applicable laws and regulations in a policy document.
- The institution keeps an overview of all information systems, data and the respective owners.
- The institution has made agreements with cloud service providers for the outsourcing of IT systems and cloud services. The agreements specify the owner as well as the location of the data and information systems.
- The institution has established rules of conduct, describing how its employees must handle information with due care (e.g. secure email, a clean desk policy). The institution monitors compliance with the rules of conduct.

7.1 Segregation of duties

Good Practices

The institution has a process in place to ensure at least the following:

- The segregation of duties is based on the institution's AO/IC structure.
- The detailed segregation of duties is based on a risk analysis and implemented and approved by the institution's senior management.
- Segregation of duties is defined and implemented based on the principles of need-to-know and least privileged, and critical duties and functions are performed by more than one individual.
- Relevant procedures with respect to segregation of duties are assessed and reviewed on a regular basis.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line of defence functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for the segregation of duties. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the segregation of duties. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has established a formal authorisation matrix for the segregation of duties.
- Based on the authorisation matrix (*soll*), the institution frequently checks whether authorisations are enforced (*ist*) in accordance with the segregation of duties requirements (soll-ist comparison).
- The institution periodically assesses the implementation of segregation of duties in its IT systems. An interim assessment is made following major changes to IT systems.
- The institution has a risk-based overview of the segregation of duties for each application and, if a process is supported by multiple applications also for each process. This prevents the segregation of duties from being breached at the process level even if the requirements are met at the individual application level.
- The institution restricts the number of accounts with high-privileged access rights to a minimum. This approach will prevent toxic combinations (undesirable combinations of roles and access rights) and related risks.
- The institution makes every effort to prevent that the duties of employees in their role as project staff conflict with their regular line duties. Exceptions are detected and put up for (temporary) approval to the management.
- The institution applies two-factor authentication for accounts with high privileged access rights (such as administrator accounts).
- The institution does not permit the use of generic or shared accounts, except with specific approval of senior management.
- The segregation 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

Good Practices

The institution has a process in place to ensure at least the following:

- The institution recruits personnel with knowledge of information security and cybersecurity, which is consistent with its ambition and its risk profile.
- The institution invests in education and training to keep its employees' knowledge of information security and cybersecurity up-to-date.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution is still responsible for ensuring that outsourced activities are carried out by personnel with sufficient expertise. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider to ensure there are sufficient staff available with knowledge of information security and cybersecurity specific to the institution, This is also the case if these activities are subcontracted.
- The institution has determined what in-house knowledge is needed to assess and to manage outsourced activities.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has entered into agreements with specialised parties to keep employees and policymakers' knowledge up-to-date in the area of information security and cybersecurity.
- The institution has prepared a gap analysis detailing how it will in the future keep its employees' and policymakers' knowledge up-to-date in the area of information security and cybersecurity.

8.2 Personnel competencies

Good Practices

The institution has a process in place to ensure at least the following:

- Employees' and policymakers' knowledge and competencies in the area of information security and cybersecurity are consistent with the institutions (digital) ambitions.
- There are regular assessments for establishing the extent to which employees' and policymakers' knowledge and competencies in the area of information security and cybersecurity are (still) consistent with the institution's (digital) ambitions.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring outsourced activities are carried out by personnel with sufficient expertise. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider to ensure the activities are carried out by personnel with the relevant expertise, in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Budgets are allocated and are sufficient for permanent education in the area of information security and cybersecurity.
- Policymakers within the institution have at least basic knowledge of information security and cybersecurity. They have demonstrably followed training courses or educational programmes in order to be able to understand the most important IT risks and control measures for their institution.
- Job descriptions include what knowledge and competencies employees are expected to have in the area of information security and cybersecurity.
- The institution has prepared a training plan to ensure that cybersecurity experts' are kept up-to-date with developments in the area of cyberthreats. The progress of this plan is monitored.

8.3 Dependence upon individuals

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has made an inventory of the processes/activities that are critical for its business operations where it is dependent on a limited number of employees.
- On the basis of a risk analysis, the institution has determined where dependence on individuals exceeds its risk tolerance.
- The institution has taken measures to ensure it limits excessive dependence on individuals to within its risk tolerance threshold.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for continuity of activities. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for identifying and reducing the dependence on a few individuals (key person risk), in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has made an inventory of cases of key person risk.
- The training programmes are structured to include ensuring there is also more widespread knowledge and experience of information security and cybersecurity throughout the organisation.
- Task rotation and succession planning for critical functions within the institution.

8.4 Personnel clearance procedures

Good Practices

The institution has a process in place to ensure at least the following:

- Before their appointment, employees are screened based on the risk profile of their job.
- They are also regularly screened during their employment.
- The above applies to both permanent and temporary employees.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring outsourced activities/systems are carried out by employees that are reliable and have integrity. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for screening employees in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has set out professional profiles that make a distinction between jobs with a high, medium and a low risk profile.
- The pre-employment screening requirements have been set out, endorsed and are applied during the recruitment process.
- The institution requests a certificate of good conduct (*verklaring omtrent het gedrag – VOG*) for jobs with an average or a high risk profile, and checks references.
- Regular and in-employment screening is conducted for employees in medium and high risk positions.

8.5 Job change and termination

Good Practices

The institution has a process in place to ensure at least the following:

- If personnel change position then IT system rights are changed as quickly as possible. If employees are no longer entitled to access rights in a new position, these are revoked immediately.
- On release from employment, rights system and processes rights are revoked immediately. There must also be due attention for access rights to systems / services that are outside the purview of the institution, such as internet portals or cloud applications to which the (former) employee is subscribed through the institution.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

For employees working on outsourced activities/ systems, the institution still bears ultimate responsibility for timely revocation of IT system access on release of employment. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the timely revocation of access rights in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution makes use of User Provisioning, where IT system access rights are automatically generated, changed, blocked and deleted through the HR system.
- For Identity Access Management, there is specific attention for joiners, leavers and movers. See also control measures 17.1. and 17.2.
- The institution keeps a register (manually or automatic) of the tools, portals and/or cloud applications which employees can access based on their positions. On release from employment or changing position, the access rights of the employee concerned are reassigned to another employee.

9.1 Knowledge transfer to end users

Good Practices

The institution has a process in place to ensure at least the following:

- Employees have the knowledge and expertise to correctly use the IT applications and systems, in accordance with the institution's procedures and operating instructions.
- Employees know how information technology supports their critical business processes, and are aware of technology-related risks linked to information security and cybersecurity. Employees apply this knowledge in their day-to-day activities.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for sharing of knowledge throughout the entire outsourcing chain. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning knowledge sharing in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Employees receive regular training about the correct use of IT applications and IT infrastructure, where there is also attention to information security and cybersecurity aspects.
- Working instructions for the correct use of IT applications and IT infrastructure are available in the form of Wikis, intranet and help functions in IT applications and systems.
- Through (SLR) discussions with service providers, the institute is alert to the fact that the service provider also devotes sufficient attention to knowledge development and knowledge sharing.

9.2 Knowledge transfer to operations and support staff

Good Practices

The institution has a process in place to ensure at least the following:

- IT employees have knowledge and expertise to develop, acquire implement and administer applications and systems in accordance with the institution's procedures and operating instructions.
- IT employees know how information technology supports their critical business processes, and are aware of technology-related risks linked to information security and cybersecurity. IT employees apply this knowledge in their day-to-day activities.
- IT employees actively use their specialised knowledge to identify information security risks and cyberthreats and to take appropriate measures to manage them.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring that IT specialists throughout the entire outsourcing chain have sufficient knowledge of information security and cybersecurity. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider to guarantee it has specialist knowledge of information security and cybersecurity in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Targeted security training sessions for specific target groups, such as IT system developers, help desk employees, IT administrators and employees with a role in information security and cybersecurity.
- Through (SLR) discussions with service providers, the institute is alert to the fact that the service provider also devotes sufficient attention to knowledge development and permanent education of specialists.

9.3 Employee awareness

Good Practices

The institution has a process in place to ensure at least the following:

- Guidelines and codes of conduct relating to information security and cybersecurity are in place. Employees at all levels of the institution are familiar with these.
- Raising security awareness is part of the information security policy, which also sets out a security awareness programme with explicit attention to cybersecurity risks
- Basic knowledge of information security and cyberthreats is widespread among the institution and executive management.
- Management and employees know how to act when they suspect there are risks in the area of information security and cybersecurity.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the sharing of knowledge throughout the entire outsourcing chain. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider regarding security awareness of management and employees in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- In the context of security awareness a training programme has been prepared for all employees to ensure they have sufficient training to carry out their duties and responsibilities in accordance with the relevant information security policy and procedures to reduce human error, theft, fraud, misuse or loss.
- The institution introduces a mix of measures to maintain and improve security awareness for its own and external employees. Security coordinators are appointed within the institution.
- Appropriate measures to further improve security awareness include presentations, phishing campaigns mystery guests and e-learnings. Participation in e-learning training sessions is compulsory; results are quantified and followed-up.
- The institution uses interesting examples from its own practice in the security awareness programme, such as security incidents that have occurred. In this respect, there is attention to areas including CEO fraud, ransomware and spear phishing in periods in which the institution is possibly more vulnerable due to (end of year) pressure, vacations or understaffing.
- The institution takes initiatives, together with outsourcing partners to raise awareness of cybersecurity.
- The institution participates in forums in which information about cybersecurity threats and attacks is shared confidentially (such as the sectoral ISACs).
- The institution maintains close contacts with government agencies engaged in cybersecurity such as National Cyber Security Centre (NCSC) or the Digital Trust Center.

10.1 Change standards and procedures

Good Practices

The institution has a process in place to ensure at least the following:

- Changes in IT applications, IT infrastructure, IT processes and critical system institutions follow a standardised and controlled path.
- Duties and responsibilities are set out relating to the review and approval of change requests.
- Changes (including security patches) are prioritised.
- The impact and risks from changes to information security and cybersecurity are estimated before the change is implemented.
- Security experts are involved in the review of changes that affect information security measures.
- Changes in critical systems and infrastructure are not requested, approved and implemented by one and the same person (segregation of duties).
- Changes are registered (audit trail) and evaluated.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the change management process. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning change standards and procedures in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The change management process is based on international standards and methods such as ITIL, Agile, Scrum.
- The institution uses a workflow system that supports the entire process from the change request to the implementation, including logging and documentation.
- The impact analysis of a change takes into consideration a fall-back scenario if the change is unsuccessful.
- The institution has set up a Change Advisory Board (CAB) which makes decisions about changes in various disciplines such as business, IT and IT risk/ IT security.

10.2 Impact assessment, prioritisation and authorisation

Good Practices

The institution has a process in place to ensure at least the following:

- The impact of change requests on operational IT systems is assessed.
- Consequences for information security and for cybersecurity are taken into consideration during the decision-making process for change requests.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the change management process. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the impact assessment, prioritisation and change authorisation, in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The information security role within the institution is involved in the assessment of the impact of measures taken in the context of information security and cybersecurity.
- In determining the impact and priority of the change requests, information security aspects of the changes will be explicitly considered.

10.3 Test environment

Good Practices

The institution has a process in place to ensure at least the following:

- Criteria for the protection of test data are set out and followed.
- Access to test and production IT systems is strictly separated; test and production data are not mixed.
- The institution has an environment available where it can test the effectiveness of the security measures.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the change management process. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning knowledge sharing in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution exclusively uses anonymised representative test data for testing, and a test environment that is separated from production environment.
- The institution uses specific software for the cleansing and anonymisation of data.
- Test and production systems are logically or physically separated (the DTAP concept is followed).
- The institution has a representative environment for testing the effectiveness of new and changed (security) infrastructure such as IDS, SIEM, Web Application Firewall (WAF), routers etc.

10.4 Testing of changes

Good Practices

The institution has a process in place to ensure at least the following:

- Changes to IT infrastructure and IT applications are tested before use (production).
- The tests are carried out according to a test plan, which sets out the acceptance criteria for information security and IT performance.
- Based on the risk assessment, changed IT systems are scanned for their vulnerabilities to cyberthreats.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the change management process. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for change testing in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution carries out various tests (such as a system test, user acceptance test, regression test and integrity test). Determining the effectiveness of the security measures in changed applications and infrastructure. In the case of an agile method, software is tested based on acceptance criteria (Definition of done).
- The acceptance criteria establish that the following requirements are met: Access security works correctly, authorisations function according to the specifications, confidential data are encrypted, critical actions are logged and the system performance meets the set requirements.
- Information security and cybersecurity measures are explicitly incorporated in change testing, such as for example through security and vulnerability scanning and source code reviews.
- If IT applications are outsourced, the institution makes a risk-based determination that the key functionality and security measures work in accordance with specifications.

10.5 Promotion to production

Good Practices

The institution has a process in place to ensure at least the following:

- There is controlled transfer of changes in production systems.
- The most important parties involved in system changes, such as users, system owner, functional and technical administrators are involved in the approval process.
- Based on a risk analysis, the institution determines whether a new system is required, or a modified system operating in parallel to the legacy system. If risky adjustments are required, the institution has a fall-back plan.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the change management process. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the controlled transfer to the production environment, in accordance with the institution's policy. These agreements also apply if the activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Transfer procedures are established for the use of changes in the IT infrastructure and IT applications.
- The institution uses a workflow system for the purposes of a controlled transfer and registration changes in the production environment.
- Changes in critical systems and changes in security parameters are conducted under the four-eyes principle.
- All changes in the production environment are logged. On this basis there are regular checks to determine that no unauthorised changes have been made.

11.1 IT Continuity plans

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has prepared a continuity plan to limit the impact of a major disruption on the key operational functions and processes.
- Alternative processing and recovery options for all critical IT services are available.
- The IT continuity plan takes into account the continuity of cybersecurity measures and the uninterrupted continuation of the information security functions during disruptions and cyberattacks.
- The IT continuity plan addresses resilience against DDoS attacks.
- Crisis management is set up, including the related communication protocols.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for continuity of business. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with service providers to guarantee continuity of IT systems and the related provision of services in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Important changes in IT systems or services are immediately included in the continuity plan.
- The institution also annually checks whether the continuity plan is adequate.
- The institution regularly checks that the IT continuity plan is operationally effective. The results of the tests are processed and follow-up actions taken.
- In case of the implementation of a new system or application, the institution includes this in an updated version of the IT continuity plan and related test cycle.

11.2 Testing of the IT Continuity plan

Good Practices

The institution has a process in place to ensure at least the following:

- Regular testing of the IT continuity plan to ensure effective recovery of IT systems, resolution of shortcomings and continued relevance of the plan.
- Testing of resilience against DDoS attacks and other cyberattacks with an impact on availability.
- Testing of continuity measures covers the entire chain of systems and applications that support critical business processes.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for testing of continuity measures. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with service providers regarding the testing of continuity measures of IT systems and the related provision of services in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution carefully prepares the testing of the IT continuity plan and reports the test results, ensures follow-up of action points and shortly after the first test conducts a retest to establish that the action points have produced the desired results.
- The institution includes chain partners in the testing of continuity measures. The results of the tests are discussed with chain partners and improvement measures are taken if necessary.
- In case of the implementation of a new system or application, the institution includes this in an updated version of the IT continuity plan and related test cycle.
- The institution includes explicit cybersecurity threats in its test scenarios such as DDoS and Advanced Persistent Threats (APTs).

11.3 Offsite backup storage

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has more than one location for storage of the data that is required for sound operational management.
- The risk profile of the locations must be such that any calamity must not be able to affect both locations at the same time.
- The content of the back-up is determined by the owners of the business processes and IT personnel.
- The institution regularly assesses the extent to which the data is complete and correct.
- The data management at the various locations (back-up, data mirroring) is in accordance with the institution's data classification policy.
- Testing and updating of compatibility of hardware and software for the recovery of archived data and periodically archived data.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring back-ups are stored at an external location. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for backup storage at an external storage facility in accordance with the institution's policy. These agreements also apply if the activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Based on a risk analysis, the institution has established the external location for backup storage.
- The institution regularly checks the availability of the off-site backup by moving data back to the test environment. End users are closely involved in this.
- The institution has made agreements with its service providers concerning Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs), and their testing.

11.4 Backup and restoration

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has established and implemented procedures for back-up and recovery of IT systems, IT applications, data and documentation.
- The institution has taken measures to detect and mitigate cyberthreats that target backups.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring that backups are made and can be restored. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service providers about making and restoring backups in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Following a disruption or major system failure, and institution can, with the help of backups or snapshots, restore its data and IT systems within the set time limit, to ensure the continuity of critical business operations with integral data and correctly functioning systems.
- The institution regularly checks whether the back-up and restore function/system works correctly.
- The institution has determined a maximum downtime period for its critical processes, and has established this on the basis of realistic tests (for example, restoring back-ups) that can be feasibly completed within this maximum downtime period.
- The institution has prepared a recovery scenario for cybersecurity incidents.
- The institution has taken various measures to safeguard and monitor access to backups: offline backup, network zoning, detection of failed backups/restore operations.

12.1 Storage and retention arrangements

Good Practices

The institution has a process in place to ensure at least 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 in line with business objectives.
- Storage of data takes into account the statutory requirements for data retention periods.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring that data storage meets the statutory requirements and is in line with business objectives. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider regarding the data retention period in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has a disposal schedule for stored data (and deletes data according to this schedule).
- The institution regularly checks service providers' compliance with the agreed data retention period.
- The institution regularly checks whether the service providers and subcontractors meet the institution's requirements in the area of data storage, archiving and retention.

12.2 Disposal

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has defined and implemented procedures to ensure business requirements are met for the protection of sensitive data and software when data and hardware are removed or transferred.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for destruction of sensitive data. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for the destruction of sensitive data in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has protocols for the destruction of documents and data carriers such as disk drives, SSD storage media and USB sticks.
- The institution has made agreements with the service providers to safely erase and destroy data. The institution regularly checks whether service providers still comply with these agreements.

12.3 Security requirements for data management

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has defined and implemented policy and procedures to safely receive, process, store and provide data in accordance with the institution's policy.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the safe receipt, processing, storage and provision of data. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service providers regarding the for the safe receipt, processing, storage and provision of data. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution's information security policy includes instructions for employees on how to handle confidential information based on the data classification (see control measure 2.2).
- The institution provides its staff with the appropriate means to be able to securely send and receive data, such as encrypted USB sticks, encrypted internet connections, secure e-mail, document vaults, etc.
- The institution regularly checks whether the institution still comply with all applicable regulatory and legislative requirements concerning data storage. The institution adjusts its policy and procedures where necessary.
- The institution regularly assesses whether service providers in the chain fulfil data management requirements.

13.1 Configuration repository and baseline

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has comprehensive oversight of the IT assets on which its business processes are dependent.
- The institution has insight into the configuration (parameters) of the IT assets.
- The institution evaluates the suppliers' recommendations for the secure design of the IT infrastructure and the IT applications, and sets out how documents how sets out how it securely configures its IT assets (baselines).
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring the service provider has insight into the IT assets. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the registration of IT assets to be able to immediately ascertain the impact of vulnerabilities in the IT assets. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has made an inventory of its IT assets in a central repository such as a Configuration Management Database (CMDB).
- The institution uses the CMDB to determine the extent to which the IT assets are installed according to a secure baseline situation (baseline).
- The institution uses the CMDB to verify actual IT assets that are present. Differences are analysed.
- The institution uses the CMDB to determine how up-to-date IT assets are and the extent to which they are supported with security updates.

13.2 Identification and Maintenance of Configuration Items

Good Practices

The institution has a process in place to ensure at least the following:

- Changes to the configuration management database (see control measure 13.1) are made in a controlled manner. That means that any changes are agreed and logged. The institution has described the configuration management procedure
- The CMDB is integrated with procedures for change management, incident management and problem management.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the configuration management process. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the identification and maintenance of configuration items in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The configuration management procedures are based in international standards such as ITIL.
- The institution regularly carries out automated inventory scans of the IT infrastructure. The outcome of these scans is compared with the content of the CMDB and if there are any deviations, these are analysed and action taken.
- Based on the assurance reports, the institution establishes that its service providers have sound configuration management.

14.1 Monitoring and reporting of Service Level Achievements

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has agreed specific quantitative and qualitative performance criteria with its service providers that report on this to the institution.
- Reports from service providers are analysed to identify both positive and negative trends and developments for both institution specific and generic services. The responsible line management is kept informed.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of subcontracted activities or systems, the institution takes the following into account:

For both outsourcing and subcontracting, the institution is responsible for monitoring the performances of the service provider in accordance with the service level agreement. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning reporting on the agreements made. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution receives a regular report clearly detailing the actual levels of service measured against the agreed targets set out in the Service Level Agreement (performance and quality standards).
- The institution receives an integrated report from its IT services provider detailing the integrated performance of subcontractors in the measured performance criteria.
- Aggregated reports provide the management of the institution with insight at different management levels into all outsourcing risks compared with its risk appetite.

14.2 Supplier risk management

Good Practices

The institution has a process in place to ensure at least the following:

- Risks regarding the continuous and reliable provision of service by services providers are identified and mitigated.
- Contracts are drawn up according to industry standards and meet all statutory provisions.
- The institution's risk management assesses the continues availability of critical or important services provided by the service providers, fall-back options for alternative ways of continuing the services provided by service providers and conformity with standards in the area of information security and cybersecurity.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the risk management of service providers. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning risk management in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has together with its service providers prepared a risk analysis with respect to the continuity and reliability of the provision of service. Risks for parties where the services are subcontracted are included in the risk analysis.
- The institution has agreed an exit plan with its service providers. The plan contains agreements on the orderly termination of services, manner of transition/migration and the liability and the destruction of back-up data after the exit. Subcontracting is in the scope of the exit plans.
- The institution has taken measures to safeguard continued maintenance of the software that was specifically developed for the institution (own build and tailor made). Escrow agreements have been entered into for this purpose. For critical or key systems the institution determines the extent of compliance with these agreements.
- The institution has a standard non-disclosure agreement for every organisation that enters into a contractual relationship with an institution, and there is monitoring to ensure that all relevant parties sign this statement.
- The institution regularly assesses the solvency of its critical service providers, and takes action where necessary.

15.1 Security incident definition

Good Practices

The institution has a process in place to ensure at least the following:

- The institution applies a clear definition for security incidents that is known to all interested parties in the institution.
- In the incident management process, cybersecurity incidents are individually classified and determined to ensure that there is a rapid response to such incidents, and with the right expertise.
- The institution has established procedures relating to the reporting of cybersecurity incidents, responding to cybersecurity and limiting any damage caused as a result of the incidents and carrying out by repair activities.
- Security and cybersecurity incidents are reported to the authorities in accordance with the applicable regulations.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for rapidly identifying, mitigating and reporting cybersecurity incidents. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for identifying, mitigating and reporting cybersecurity incidents in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has set up a process that ensures that all (potential) security incidents are centrally reported and registered.
- The Security Officer assesses, at least on a daily basis, the security incidents that have been reported and determines the impact and the follow-up.
- The institution and the service providers proactively cooperate to detect and to respond to any cybersecurity incidents in the chain of the outsourced services and IT infrastructure. The institution has set up a Security Operations Center (SOC) for this purpose.
- The institution makes use of tooling such as Security Information and Event Management (SIEM) in order to gather, combine and analyse IT-related security information, in order to gain timely insights and to proactively respond to (potential) security incidents.
- If a significant incident occurs then management is informed about the response. If necessary, management coordinates the response, makes a post-evaluation of the incident, and includes the result of this evaluation in the risk management cycle.

15.2 Incident escalation

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has in place a formal policy for incident management, including an escalation procedure and escalation criteria.
- The escalation procedure is based on the agreed service levels for incidents which cannot be immediately resolved.
- Categorising and prioritising occurs on the basis of impact analysis, defined criteria and service levels.
- There is response training for information security and cybersecurity incidents.
- Incidents are assigned owners.
- Significant incidents are reported to management.
- In the institution there is awareness of escalation procedures, and these are followed.
- How incidents are resolved is regularly analysed to improve processes and IT systems.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for providing insight into incidents at the right management level. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for incident escalation in accordance with the institution’s policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- In addition to the policy and escalation procedures mentioned, the institution has set up a Computer Emergency Response Team (CERT), comprising specialised ICT professionals that are in a position to act in the event of an information security or cybersecurity incident. It is the aim of the CERT to reduce damage and to rapidly restore the provision of service.
- The institution’s CERT is also focussed on preventing cybersecurity incidents and preparing the institution for such incidents.

16.1 Security testing, surveillance and monitoring

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has taken and documented security measures. These measures are tested and periodically evaluated so they continue to meet the established security baselines.
- There is monitoring of unusual activities in IT systems, and exceptions are flagged and followed up.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution at all times bears ultimate responsibility for testing, monitoring and safeguarding the quality of the information security. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for testing, monitoring and safeguarding IT security in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has implemented a SIEM (Security Information and Event Management) solution in order to be able to rapidly identify deviations in patterns and to act on this.
- The institution regularly prepares management reports with an overview of all registered security incidents and the follow up status.

16.2 Monitoring of internal control framework

Good Practices

The institution has a process in place to ensure at least the following:

- The institution manages IT risks and risks in the area of information security and cybersecurity. For this purpose, the institution has set up an IT internal control framework which includes information security policy, standards, procedures (key) controls and IT general controls, in line with the institution's objectives.
- The institution regularly evaluates the design, existence and effective operation of the internal control framework.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for monitoring the provision of services. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for monitoring the provision of service in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The risk management function, internal auditor and external accountant regularly report their assessments, findings and recommendations about the set-up, implementation and effectiveness of the control framework.
- Follow up of recommendations is monitored.
- The institution compares the Service Level reports of suppliers with the agreed provision of service and the experiences of the institution with the services provided.
- The institution analyses trends and developments as compared to prior reporting periods.

16.3 Internal control at third parties

Good Practices

The institution has a process in place to ensure at least the following:

- When preparing contracts the institution focuses on how the service provider continues to comply with contractual obligations, laws and regulations and reporting and monitoring arrangements.
- The institution forms an opinion of the internal control measures at its service providers and any subcontractors.
- The service provider meets statutory or contractual provisions.
- The institution has contractually agreed that outsourcing will not obstruct oversight throughout the entire chain.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for internal control at the service provider. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the internal management of the service provider in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has contractually agreed that it has its "right-to-audit" at the service provider and any subcontractors.
- The institution stipulates in the agreement that the service provider must notify the institution of any intended major changes with respect to the subcontractors listed in the original agreement, or the services that are subcontracted out. The notification period for such changes is determined in such a way that the institution has sufficient time to assess the risk ensuing from the proposed changes and if necessary take appropriate measures or terminate the agreement with the service provider.
- The institution demonstrably evaluates critical or important outsourcing activities at least annually, which also includes assessing the performance and the results agreements, and how far the service provider fits in with the institution's strategy and objectives, as well as the service provider's risk appetite compared to the institution's own risk appetite.
- During the term of the contract the institution receives regular reports from the service provider about the effectiveness of the internal control measures in place at the service provider.
- The institution receives and assesses an independent assurance report about management of risks in the area of information security and cybersecurity at the service provider, in accordance with the agreed provision of services.
- The institution discusses deviations/exceptions with the service provider, which the service provider addresses effectively and on a timely basis. The institution monitors this.
- The service provider issues an assurance statement to the institution each year on IT control, such as type 2 SOC report. Measures in the area of information security and cybersecurity come under the scope of the assurance statement.

16.4 Evaluation of compliance with external requirements

Good Practices

The institution has a process in place to ensure at least the following:

- The institution regularly assesses whether its IT policy and procedures are in line with laws and regulations.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for evaluation of compliance with statutory and regulatory requirements. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning compliance with laws and regulations, in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution's compliance officer assesses on an annual basis whether IT policies are in line with current laws and regulations. Where necessary, adjustments are made.
- In the event of the introduction of new legislation on information security and cybersecurity, the institution assesses its impact and where necessary make adjustments.
- The institution is proactively informed about any changes in the area of relevant external regulations.

16.5 Independent assurance

Good Practices

The institution has a process in place to ensure at least the following:

- The institution obtains regular periodic assurance about how the institution's IT controls function. This includes assurance about the effectiveness of the internal control measures in the area of information security and cybersecurity.
- The results of this independent assessment are presented to the institution's management.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for obtaining assurance about the continuity of activities. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider about obtaining independent assurance about IT control. This includes assurance about the effectiveness of the internal control measures in the area of information security and cybersecurity. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- On the basis of a risk analysis, the institution has the internal or external auditor regularly assess the IT objects, such as information security and cybersecurity. This assessment relates to the design, existence and effective operation of control measures.

17.1 Identity & Access Management

Good Practices

The institution has a process in place to ensure at least the following:

- Access to the institution's information systems and data can be traced to uniquely identifiable people (internal, external and insourced) or to IT services (such as scripts and batch jobs) with a uniquely identifiable owner.
- The institution has established, approved and set out access to information systems (SOLL authorisation matrices) and based on the required segregation of functions and business rules (see control measure 7.1).
- The set-up of the logical access security (SOLL authorisation matrices) is regularly evaluated.
- Access to the institution's information systems and data is controlled and monitored in the IT infrastructure and the IT applications, in accordance with agreed SOLL authorisation matrices.
- Access rights in IT systems (IST) are regularly compared with the SOLL authorisation matrices.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for controlling access to the institution's information systems and data. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the control of access to information systems and data in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution assigns unique user IDs to all persons with access to IT systems and data. User identities and access rights are stored in a central repository.
- The institution applies the principle of 'Role based access'.
- Access to IT systems and data is granted on the basis of the 'need-to-know' and 'least privilege' principles. There is periodic evaluation of compliance with these principles.
- The institution makes use of an Identity & Access Management (IAM) tool to support the set-up of access security and its control through business process owners and It system administrators.
- As far as possible, the institution limits the use of generic and shared user IDs, including administrator accounts with high levels of rights. The use of these user IDs is controlled with both technical as well as procedural measures, such as approval for use, strong authentication solutions (2 factor authentication, biometrics), 4-eye principle for activities, (digital) password vault, logging and monitoring of activities and post-use evaluation of the relevant administrator user ID.

17.2 User account management

Good Practices

The institution has a process in place to ensure at least the following:

- The granting, changing or revocation of access rights to information systems and data is based on formalised steps in which approval is granted by the owners of appropriate the business processes, information systems and data.
- Segregation of duties or the 4-eye principle prevents one person from being able to carry out the above-mentioned steps.
- All activities relating to granting, changing or revoking access rights and can be traced to people.
- The access rights of people leaving the employment of the institution/ who have their contracts terminated are removed or blocked as quickly as possible.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for granting, changing and deleting access rights to information systems and data in a controlled manner. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for granting, changing and deleting access rights to information systems and data in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution makes use of User Provisioning, where user accounts in the IT infrastructure and business IT applications are as far as possible automatically generated, changed, blocked and deleted through the central HR system.
- The institution automatically blocks a user account after it has not been used to log in with for a pre-determined period.

18.1 Infrastructure resource protection and availability

Good Practices

The institution has a process in place to ensure at least the following:

- The control measures in the IT-infrastructure components are set-up so as to safeguard a high level of availability, exclusivity and integrity.
- Responsibility for designing and implementing these control measures is clearly assigned.
- The design and implementation of these control measures is monitored and evaluated.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the availability and integrity of the IT infrastructure. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the availability and integrity of the IT infrastructure in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Risk analyses for infrastructure components take account of actual cyberthreats as is for example set out in the SANS Top 20, ENISA/NCSC threat assessments or based on the outcomes of the recent red teaming exercises and pen testing, etc.
- Security baselines are set out for technical platforms (for example: Windows, Unix, firewalls, IDS and IPS) and in accordance with the implemented baselines.
- The use of 'scrubbing services' (re-routing traffic to an anti-DDoS environment) to mitigate DDoS attacks. In this respect there is a distinction made between the DDoS volumetric attacks and application attacks.
- The institution has carried out a risk analysis of the distributed storage and control of 'private keys' and passwords, and substantiated consideration of the internal or external location in which keys or passwords or stored.
- The protection and the availability of the It infrastructure is a permanent item on the agenda in the agenda at meetings of the institution first, second and third line of defence.

18.2 Infrastructure maintenance

Good Practices

The institution has a process in place to ensure at least the following:

- IT infrastructure maintenance is structural and scheduled, in line with the institution's change management procedures.
- The institution has classified the infrastructure components, making a distinction between the critical and less critical components.
- In prioritising and carrying out maintenance to the IT infrastructure takes the classification of infrastructure components into consideration.
- Solutions for vulnerabilities in the IT infrastructure, such as patches, influence the prioritisation of IT infrastructure maintenance activities.
- Here, change management processes are followed, and there is consideration of patch management for critical and less critical vulnerabilities. This is based on risk analyses that form part of the change management process (change risk assessments - CRAs).
- In the CRAs there is explicit attention to cyberthreats. These have an influence on the prioritisation and the implementation of the changes.
- The institution's heightened focus on customer experience and time-to-market does not lead to postponement of infrastructural security measures and technological investments.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring maintenance of the IT infrastructure. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for IT infrastructure maintenance in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Implementation of critical security patches is a specific element of the patch management process.
- With the help of tools, a regular inventory is taken of the status of IT infrastructure, including vulnerability to cyberthreats. This is reported on and deferred maintenance is carried out.

18.3 Cryptographic key management

Good Practices

The institution has a process in place to ensure at least the following:

- Encryption keys are managed is a controlled way. The institution has set out policy and procedures regarding generating, changing, revoking, destroying, distributing, certifying, storing, installing, using and archiving encryption keys.
- The risks of modification and disclosure of the keys during these processes are identified and mitigating measures are taken.
- The institution is aware of the risks of cyberattacks intended to modify and intercept encryption keys and has taken appropriate measures to manage this.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for managing encryption keys. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for managing encryption keys in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution uses Hardware Security Modules (HSMs) for generating, changing, revoking, destroying, distributing, certifying, storing, installing, using and archiving encryption keys.
- Processes, procedures and parameterisation are set up in such a way that they provide optimal protection for the encryption keys.
- The availability of encryption keys is included in the institution's continuity plans.

18.4 Network Security

Good Practices

The institution has a process in place to ensure at least the following:

- The institution applies up-to-date technical security measures to (such as firewalls, network segmentation and intrusion detection) and the associated management processes to limit the access to IT infrastructure to the authorised personnel, IT services and the exchange of information between networks.
- Authorisation for IT infrastructure administrators, including network administrators is soundly set up (see control measure 17.1 and 17.2)
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for network security. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning network security in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution applies modern firewall technologies in its network infrastructure which are in line with best practices such as GovCert, ISO/IEC and ITSEC.
- Reports of cyberattacks on the IT infrastructure are logged and these logs are automatically analysed on which basis the institution takes the appropriate action.
- The availability of network infrastructure (uptime and downtime percentages) are registered and monitored. During downtime the institution carries out targeted research on the basis of security incidents.
- The institution makes use of tooling which in the network infrastructure actively seeks unauthorised devices such as laptops, routers and Wi-Fi access points.
- The institution applies endpoint security to laptops, tablets and workstations.

18.5 Exchange of sensitive data

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has in place a policy laying down the rules for sharing confidential information.
- The institution has facilities that enable the exchange of confidential information through secure channels.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for ensuring that sensitive data can only be transferred through secure channels. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for exchanging sensitive data in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution applies up-to-date authentication and encryption techniques to network connections with parties it trusts.
- Embedded in the institution's network infrastructure are controls that safeguard the authenticity of the integrity of messages, as well as confirmation of sending of receipt and the identity of the sender and receiver of confidential data.
- Confidential data stored on laptops, hard drives, USB sticks and other information carriers is encrypted.
- The institution applies Data Loss Prevention software for checking outgoing messages.
- The institution follows protocols for wiping and destroying media that may contain confidential data such as hard drives USB sticks and SSDs.

19.1 Malware prevention, detection and correction

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has implemented preventive, detective and corrective controls to protect its IT systems against cyberthreats such as viruses, malware, worms, malware, cryptoware, spyware cryptojacking and spyware.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for prevention, detection and correction of malicious software. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning the prevention, detection and correction of malicious software in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution has implemented tools for the automatic detection and blocking of viruses, worms, malware and spyware, such as modern firewall technology, virus scanners, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
- Log files from the systems are sent to a Security Incident and Event Monitoring (SIEM) system for the purposes of analysis and response/action.
- The institution applies network segmentation to limit as far as possible the impact of any successful malware attacks.
- The institution constantly monitors whether firewalls, virus scanners, IDS and IPS are up-to-date and reports this on a monthly basis.
- The institution monitors whether service providers ensure that firewalls, virus scanners, IDSs and IPSs and their infrastructure are up-to-date. The service provider reports this to the institution.

19.2 Vulnerability management

Good Practices

The institution has a process in place to ensure at least the following:

- The most important IT assets are identified on the basis of a risk analysis.
- Partly on the basis of threat intelligence and vulnerability scans, the institution regularly performs checks of IT assets to establish whether there are cyber vulnerabilities, and determines the impact of these on its processes.
- Risk mitigating actions are determined for those threats falling outside the institution's risk tolerance.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for vulnerability management. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning vulnerability assessments in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution regularly makes an inventory of which IT assets are used in business processes.
- The institution frequently (daily) makes an inventory of vulnerabilities based on Threat Intelligence.
- The institution uses tools to make an automated inventory of vulnerabilities (vulnerability scanning).
- The institution structurally determines the impact of these vulnerabilities are on its IT assets, using a risk-based approach.
- The institution determines a risk response based on its risk appetite and monitors follow up of risk response based on defined KPIs.
- The institution regularly discuses with its services providers reports/dashboards concerning the results of the vulnerability scans carried out.

19.3 Application life-cycle management

Good Practices

The institution has a process in place to ensure at least the following:

- Application maintenance is structured and planned process, in line with the institution's change management procedures.
- The institution checks that the IT infrastructure and IT applications that it uses are supported by the developer/supplier and that the security updates (patches) are made available.
- Solutions for vulnerabilities in the applications, such as patches, influence the prioritisation of regular maintenance activities for IT applications.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for application life-cycle management. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for application life-cycle management in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The institution applies acceptance criteria in the area of information security and cybersecurity for the development and acquisition of IT applications.
- In its configuration management database (CMDB), the institution has included the replacement schedule for applications and replaces them on this basis.

20.1 Protection of security technology

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has insight into the security technology that is relevant to it[12]
- In view of the inherently high risk profile, specific security measures apply to the security technology.
- Documentation about the security technology and the security measures is only available on a 'need-to-know' basis.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for security-related technology. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for screening personnel in accordance with the institution's policy (which also apply to any subcontractors).
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Additional measures apply to these elements such as enhanced physical and logistical access security, four-eye principle for management and maintenance, stricter patch regime and more rapid follow-up for alerts from the monitoring system, 'tamper resistant' measures, etc.
- IT systems that play a role in the security of the institution are linked to a SIEM system.
- IT security elements are tested (hack tests) by a party that is specialised in conducting these tests.

[12] - Security-related technology is understood to mean: 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

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has defined and implemented a policy for the physical security of office buildings, grounds and IT infrastructure locations such as data centres and server rooms.
- Physical access security measures are in line with the institution's risk profile.
- Physical access security measures are regularly maintained and tested.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for physical security of IT assets. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for physical security of IT assets in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- On the basis of a risk analysis, the institution has determined zoning with different clearance levels (such as: public, staff and restricted).
- The four-eye principle applies when carrying out physical maintenance of security equipment.
- The institution has a "Mystery Guest" check the security measures once a year.

21.2 Physical access

Good Practices

The institution has a process in place to ensure at least the following:

- The institution has defined and implemented a policy for the security of buildings, grounds, zones, data centres and server rooms which are critical to the institution's operational processes.
- Access profiles are authorised by management. Access to buildings, areas, zones and server rooms is based on the position and the responsibilities of the employee/visitor.
- The institution regularly checks the effectiveness of the physical access measures and reports the outcomes to management. Assessment of the access rights granted (SOLL-IST) and the assessment of the logging of the security access system is also included.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for physical access. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider concerning physical access in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- Physical access to buildings and zones is managed with the help of key cards and access gates.
- The institution has a "Mystery Guest" check the physical access measures once a year.
- IT components that play a role in the physical access security of the institution are linked to a Security Information and Event Management (SIEM) system.

22.1 Penetration testing and ethical hacking

Good Practices

The institution has a process in place to ensure at least the following:

- On the basis of a risk analysis and current cyberthreats, the institution determines the security tests to be performed, as well as their scope and depth.
- The nature and frequency of these tests depends on the institution's risk profile. These can include the following types of security tests: pen testing, ethical hacking and/or red teaming.
- The institution ensures that the party that carries out the security tests has adequate knowledge, experience, certification and references.
- Duties and responsibilities concerning the above areas are assigned to first-line, second-line and third-line functions, and formal reporting lines are set up.

In the event of outsourcing, activities or systems, the institution takes the following into account:

The institution still bears ultimate responsibility for the testing of information security and cybersecurity. The institution has set up a process which ensures at least the following (see Good Practices for outsourcing):

- The institution has made agreements with the service provider for testing information security and cybersecurity in accordance with the institution's policy. This is also the case if these activities are subcontracted.
- The institution receives service level reports (SLRs) and/or assurance reports with the correct scope and detail, on which basis the agreements can be monitored.
- The institution intervenes when its risk tolerances are exceeded (see Risk Management cycle).

Examples of this include:

- The determine the types of security tests in its risk analysis, the institution has included current cyberthreats such as phishing, DDoS, cryptoware and CEO fraud.
- Based on a risk analysis, the institution makes an annual plan with the tests to be conducted. Part of this plan involves conducting pen tests for all (new and changed) critical IT applications and for performing red teaming activities.
- For example, the institution can perform or have a third party perform several types of security tests, such as pen tests targeting infrastructure and application security, red teaming, physical security tests and human behaviour tests in relation to information security and cybersecurity.
- The institution has a specialised party carry out the pen tests.
- The institution regularly changes the party that conducts these pen tests.
- The institution involves its critical security providers in its security tests.