Samen aanjagen van vernieuwing

BIS

Baseline Informatiebeveiliging SURF

Author(s)	: CISO team
Version	: 1.2
Date	: April 2023
Feature	: Baseline Information Security SURF (BIS)

Table of contents

Translated with Deepl.

1 Information security SURF

1.1 Introduction and scope

Information security is the process of establishing the required security of information systems in terms of confidentiality, availability and integrity and establishing, maintaining and monitoring a coherent set of associated measures.

The Baseline Information Security SURF (hereinafter BIS) is a framework of measures for the security of the information (systems). The purpose of the BIS is to determine a minimum security level that the whole of SURF must meet. Basically, this ensures a reliable and professional provision of services and information.

The BIS applies to the entire SURF organisation. The BIS includes all organisational and technical measures that both the organisation as a whole and all services and systems where information is processed must comply with.

1.2 Information security frameworks and principles

The BIS forms an integral part of SURF's information security policy. In case of contradictions with other documents in the baseline, the BIS prevails.

The following standards, frameworks and documents apply as the basis for the BIS:

- Baseline Information Security Government (BIO)
- SURF information security policy
- ISO 27001 and ISO 27002
- General Data Processing Regulation
- SURF Legal Framework of Standards (Cloud) Services
- Other laws and regulations, such as the AVG

Account has been taken of SURF's privacy policy and associated procedures and measures. The BIS focuses on the security measures needed to adequately secure processing of personal data according to AVG, including the processing of special personal data.

In summary, the following applies to the BIS:

- Line management is responsible for information safety and the security of information (systems).
- Line management sets the classification on information in its systems for the aspects of reliability, integrity and confidentiality (see Chapter 3, Classification).
- The classification determines the security requirements to be met by the system (according to the 'comply or explain' principle).
- Based on the classification, line management implements and propagates the measures
- Information security is a cyclical process according to the PDCA cycle (Plan-Do-Check-Act).

1.3 Evaluation and adjustment

With developments in technology, information security measure sets can quickly become outdated. The BIS is therefore written as much as possible at a level of abstraction so that such developments have as little impact as possible on the content: the BIS describes the what and not the how. Procedures and guidelines for operational implementation are thus not incorporated in the BIS.

Nevertheless, changes may have to be made, e.g. due to changes in underlying laws and regulations, new or renewed policy guidelines, ISO standard or new threats and vulnerabilities, etc. This document is therefore reviewed regularly, at least annually, in its entirety and updated as necessary. To increase its practical applicability, this also includes a check to see whether any changes/additions to the measures and (operational) procedures and guidelines are necessary or desirable.

2 The BIS measures

2.1 ISO 27001 controls as a basis

The ISO 27002 standard can be seen as a specification of the ISO 27001 standard. The ISO 27002 standard (2018) helps as a practical guideline to define information security measures for availability, integrity and confidentiality of the information facility. This ISO standard consists of 114 controls (security objectives).

The list of management measures follows this standard and accompanies this document. An overview of the BIS measures list is attached. From a practical point of view, the list has also been made available via intranet.

2.2 Roles and responsibility

SURF's Executive Board is ultimately responsible for overall security and the set-up and operation of the security organisation. In that capacity, SURF's Executive Board is ultimately responsible for the implementation of all security frameworks in the organisation, including the correct application of the BIS.

The SURF Information Security Policy stipulates that line management is responsible for determining that the measures taken demonstrably comply with the security requirements and that they are complied with.

The service provider or any assigned process owner is responsible for making classification decisions. This determines the required level of information security for services and information processing. This takes into account the classification of the data to be processed by determining what information the service should be suitable for (see Chapter 3).

The BIS categorises services into two roles in terms of responsibility for implementation of security measures. Each control indicates who is responsible for implementing the security measure. In some cases it is the service owner, in other cases SURF takes care of the implementation of the security measure centrally.

3 Classification

3.1 Information and suitability classification

Classifying data clarifies the security level required for availability and integrity & confidentiality (B and IV). At SURF, classification is divided into two components:

1. Information classification - internal SURF data is given a classification that makes it clear what type of information it is about.
   For example, 'financial information' or 'personnel information'.
2. Suitability classification - SURF services are given a designation showing the type of information for which the service is suitable.
   For example: SURF service NAME is suitable for data with a classification Basic (B)/High (IV).

Institutions themselves are responsible for checking whether their own data classification and associated control measures are comparable to SURF's suitability classification.

For SURF internally, data may only be processed in information systems with the appropriate suitability classification.

3.2 Classification model

The classification determines the management measures to be taken. We choose a simple model whose applicability is high. Security measures for integrity and confidentiality are similar; both aspects are therefore combined. Four risk level designations in combination between Availability and Integrity & Confidentiality are possible:

Basic|basic, basic|high, high|basic, high|high

Availability (B)	Integrity & confidentiality (IV)
BASIC Total loss or unavailability for longer than **1 working day** causes noticeable damage to the interests of user and organisation.	BASIC Business process allows some to **few integrity errors**. Information accessible to limited to large group of users. Information is **public to confidential** and may contain personal data.
HIGH Total loss or unavailability for more than **2 hours** causes significant damage to the interests of user and organisation.	HIGH Business process **does not allow integrity errors**. Information accessible only to specific individuals. Information is **highly confidential or sensitive** and may contain sensitive or special personal data. Inadvertent disclosure outside this group causes great harm to the interests of user and organisation.

3.3 Apply or explain

The controller of a service or processing provides a record of the BIS measures that cannot or cannot yet be fully met, why they cannot (yet) be met, including an inclusive explanation of the resulting risks. This is the justification (also called 'explain') according to the 'comply or explain' principle. Such risks must be formally accepted (unless the estimated impact is low). The risk acceptance matrix in the information security policy defines who - depending on the estimated impact - may formally accept risks if measures are not implemented in line with the BIS ment.

A hardship provision applies: if a control cannot apply to a specific case, the control is not applicable. This applies, for example, to a control that relates to an external link, while the information system in question has no external link. The risk assessment underlying this ('comply or explain') should be recorded.

Details of the measures are included for most controls. These measures do not always cover the entire security objectives of the control. Here, too, there is a hardship provision: if a measure cannot apply to a specific case, the obligation lapses. The risk assessment underlying this ('comply or explain') should be recorded.

With stacked services within SURF, explains can result in a difference in protection. This creates a risk for the processed (and shared) information. For a service that uses other SURF services, the lowest suitability classification of the sub-service in the chain determines the maximum suitability classification (the weakest link determines the maximum strength). Services for which explains are registered should therefore seek coordination among themselves. The purpose of such coordination is to jointly take appropriate measures or temporary measures that mitigate or reduce the risk until the explains are implemented according to the BIS.

4 Definitions

AVGAGeneral
Data Protection Regulation dated 27 April 2016

Comply or explain
the principle of 'comply or explain' as referred to in SURF's information security policy

Control
a management measure as referred to in ISO 27001/ISO 27002

Information system
a coherent set of data collections and their associated persons, procedures, processes and software and the storage, processing and communication facilities provided for the information system

ISO 27002
the ISO 27002 'Code for Information Security' provides guidelines and principles for initiating, implementing, maintaining and improving information security within an organisation

Procedures
concrete step-by-step instructions on how to carry out certain tasks or actions, these have a mandatory character

Guidelines
management recommendations that are not mandatory in nature and are not essential to the operation of a system; a guideline provides an example of how to implement or use certain norms, standards, techniques or measures and may be tailored more specifically to a team or to a particular focus area

Standard
standard measures that are mandatory to implement

5 Baseline Information Security SURF - 2023

BIS - Chapter Overview

Below is the overview of BIS controls and measures (starting with 5 according to ISO numbering). The complete list can be found in SURF's Information Security Management System (ISMS).

5. Information security policy
5.1 Management steering of information security

6. Organising information security
6.1 Internal organisation
6.2 Mobile devices and teleworking

7. Safe staffing
7.1 Prior to employment
7.2 During employment
7.3 Termination and change of employment contract

8. Asset management
8.1 Responsibility for assets
8.2 Information classification
8.3 Handling media

9. Access security
9.1 Operating requirements for access security
9.2 Managing user access rights
9.3 Responsibilities of users
9.4 System and application access security

10. Cryptography
10.1 Cryptographic management measures

11. Physical and environmental security
11.1 Secured areas
11.2 Equipment

12. Security Operations
12.1 Operating procedures and responsibilities
12.2 Protection against malware
12.3 Backup and restore
12.4 Reporting and monitoring
12.5 Control of operational software
12.6 Managing technical vulnerabilities
12.7 Information systems audit considerations

13. Communication security
13.1 Network security management
13.2 Information transport

14. Acquisition, development and maintenance of information systems
14.1 Security requirements for information systems
14.2 Security in development and support processes
14.3 Test data

15. Supplier relations
15.1 Information security in supplier relationships
15.2 Management of supplier services

16. Information security incident management
16.1 Management of information security incidents and enhancements

17. Information security aspects of business continuity management
17.1 Information security continuity
17.2 Redundant components

18. Compliance
18.1 Compliance with legal and contractual requirements
18.2 Information security assessments

BIS - List of management measures

Blue are the ISO controls we use at SURF as the main control measure
Green are the elaborations of the measures at 'basic' level
Orange are the elaborations of the measures at 'high' level

V1.2 - 13-04-2023

Chapter 5 - Information security policy

Sub-chapter	ISO	ID	Control/measure	Classification
Information security policies	5.1.1		Information security policies - For information security, a set of policies should be defined, approved by the board, published and communicated to employees and relevant external parties.	BIV-Basic
Information security policies		5.1.1.1	An information security policy has been drawn up by the organisation. This policy has been adopted by the organisation's management and contains at least the following points: a. the strategic principles and preconditions used by the organisation for information security and, in particular, the embedding in, and alignment with, the general security policy and the information provision policy; b. the organisation of the information security function, including responsibilities, tasks and authorities; c. the assignment of responsibilities for chains of Information Systems to line managers; d. the common reliability requirements and standards applicable to the organisation; e. the frequency with which the information security policy is evaluated; f. the promotion of security awareness.	BIV-Basic
Information security policies		5.1.1.2	Per processing, where necessary, additional policies for specific data at level high.	IV-High
Information security policies	5.1.2		Information security policy review - Information security policies should be reviewed at planned intervals or as significant changes occur to ensure that they are appropriate, adequate and effective on an ongoing basis.	BIV-Basic
Information security policies		5.1.2.1	The information security policy is reviewed and updated at least once every three years, or in the event of significant changes due to reorganisation or change in the division of responsibilities.	BIV-Basic
Information security policies		5.1.2.2	Additional policies are reviewed at least once a year, or in case of significant changes due to reorganisation or change in the division of responsibilities, and adjusted if necessary.	IV-High

Chapter 6 - Organising information security

Sub-chapter	ISO	ID	Control/measure	Classificatio n
Internal organisation	6.1.1		Roles and responsibilities in information security - All responsibilities in information security should be defined and assigned.	BIV-Basic
Internal organisation		6.1.1.1	The organisation's leadership has defined information security responsibilities and roles.	BIV-Basic
Internal organisation		6.1.1.2	The role and responsibilities of the Corporate Information Security Officer (CISO) are defined in a CISO job profile.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Internal organisation		6.1.1.3	A CISO has been appointed in accordance with an established CISO job profile.	BIV-Basic
Internal organisation	6.1.2		Separation of duties - Conflicting duties and responsibilities should be separated to reduce the risk of unauthorised or unintended modification or misuse of the organisation's assets.	BIV-Basic
Internal organisation		6.1.2.1	In critical processes, strict separation of functions is taken into account when assigning responsibilities with regard to final responsibility, ownership and execution.	BIV-Basic
Internal organisation		6.1.2.2	An authorisation process for granting authorisations has been formulated including registration of granted authorisations, so that there is additional control whether the requested authorisations fit the role the employee fulfils in the organisation.	BIV-Basic
Internal organisation		6.1.2.3	Separation of functions is strictly applied to changes to security devices.	BIV-Basic
Internal organisation		6.1.2.4	For gaining access to systems and granting privileges, close attention is paid to which privileges are involved in which roles, with the four-eye principle applying in critical processes, so that several people are involved in the execution of critical work.	IV-High
Internal organisation		6.1.2.5	Separation of functions also considers involvement in specific processing operations in combination with any conflicting work. These are strictly applied where required, from specific policies.	IV-High
Internal organisation	6.1.3		Contact with government agencies - Appropriate contacts with relevant government agencies should be maintained.	BIV-Basic
Internal organisation		6.1.3.1	The organisation has worked out who has contact with which (government) agencies and regulators for information security matters (permits/incidents/disasters).	BIV-Basic
Internal organisation		6.1.3.2	The contact overview is updated annually.	IV-High
Internal organisation	6.1.4		Contact with special interest groups - Appropriate contacts should be maintained with special interest groups or other specialised security forums and professional organisations.	BIV-Basic
Internal organisation		6.1.4.1	The organisation has worked out who has contact with which interest groups.	BIV-Basic
Internal organisation	6.1.5		Information security in project management - Information security must be addressed in project management, regardless of the type of project.	BIV-Basic
Internal organisation		6.1.5.1	Security must be ensured in projects by the principle of 'Security by Design'.	BIV-Basic
Mobile devices and teleworking	6.2.1		Mobile device policies - To manage the risks posed by the use of mobile devices, policies and supporting security measures need to be established.	BIV-Basic
Mobile devices and teleworking		6.2.1.1	Mobile devices (such as a laptop, tablet and smartphone) are arranged so that: a. access to the device is protected by an access security mechanism, and b. the data on the built-in storage devices is protected by encryption.	BIV-Basic
Mobile devices and teleworking		6.2.1.2	When deploying mobile equipment, at least the following aspects will have been implemented: a. behavioural aspects of safe mobile working will be addressed in awareness programmes; b. the device will be part of patch management and hardening; c. where possible, the device will be managed and secured via an MDM Mobile Device Management (MDM) solution; d. company data on mobile devices must be able to be erased remotely via the MDM solution; e. users will sign a user agreement for mobile working, in which they declare that they are aware of the dangers of	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
			mobile working and declare that they will do so safely. This declaration relates to all mobile devices the employee uses for business purposes; f. compliance with the points in paragraphs b, c and d is checked periodically.	
Mobile devices and teleworking	6.2.2		Working remotely - For the security of information accessed, processed or stored from outside SURF locations, policies and supporting security measures must be implemented	BIV-Basic

Chapter 7 - Safe personnel

Sub-chapter	ISO	ID	Control/measure	Classification
Prior to employment	7.1.1		Screening - Background verification of all candidates for employment should be conducted in accordance with relevant laws, regulations and ethical considerations and should be proportionate to the business requirements, the classification of information accessed and the risks identified.	BIV-Basic
Prior to employment		7.1.1.1	When appointing new staff, identity papers, diplomas and certificates are verified.	BIV-Basic
Prior to employment		7.1.1.2	If the position requires a Certificate of Good Behaviour (VOG), the employee must submit it upon employment.	BIV-Basic
Prior to employment		7.1.1.3	For specific projects and sensitive data processing at risk level high, the need for a heavier VOG or other screening measures will be considered. This will be set out in the supplementary policy.	IV-High
Prior to employment	7.1.2		Terms of employment - The contractual agreement with employees and contractors should state their responsibilities for information security and those of the organisation.	BIV-Basic
Prior to employment		7.1.2.1	The employment conditions regulations are provided to each new employee as part of the signed employment contract.	BIV-Basic
Prior to employment		7.1.2.2	All employees (internal and external) have been made aware of their information security responsibilities upon appointment or job change. The regulations and instructions applicable to them regarding information security are easily accessible.	BIV-Basic
During employment	7.2.1		Board responsibilities - The board should require all employees and contractors to apply information security in accordance with the organisation's established policies and procedures.	BIV-Basic
During employment		7.2.1.1	There is affiliation to a whistle-blowing scheme so that everyone is able to report security issues anonymously and safely.	BIV-Basic
During employment	7.2.2		Information security awareness, education and training - All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular refresher training on organisational policies and procedures, as relevant to their functions.	BIV-Basic
During employment		7.2.2.1	All employees have a responsibility to protect company information. Everyone knows the rules and obligations related to information security and, where relevant, the special requirements for classified environments.	BIV-Basic
During employment		7.2.2.2	All employees and contracts are updated through awareness training, presentations and/or campaigns.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
During employment		7.2.2.3	All employees and contractors using the Information Systems and Services have attended an induction 'information security' within two months of commencing employment.	BIV-Basic
During employment		7.2.2.4	Line management stresses the importance of information security education and training to its employees and contractors when appointing and transferring internally and, for example, in work meetings or staff interviews, and actively encourages them to follow it periodically	BIV-Basic
During employment		7.2.2.5	Employees involved in level-high processing operations are explicitly and in detail informed by the supervisor about the higher level of requirements related to risk level-high processing operations and their responsibilities therein.	IV-High
During employment	7.2.3		Disciplinary procedure - There should be a formal and communicated disciplinary procedure to take action against employees who have committed an information security breach.	BIV-Basic
During employment		7.2.3.1	The employment conditions package contains disciplinary measures that are, among other things, related to and can be applied in case of violations of security policy standards and measures.	BIV-Basic
During employment		7.2.3.2	Reference to disciplinary measures is made in relevant documents so that employees are aware of their existence and so that they can be applied in case of violations.	BIV-Basic
During employment		7.2.3.3	For specific projects and sensitive data processing at classification high (for confidentiality and integrity), a more explicit link is made between the employee's role regarding these processing operations and disciplinary measures. It should be communicated that the threshold for proceeding to the application of disciplinary measures is lower due to the nature of the processing operations and the sensitivity of data processed	IV-High
Termination and change of employment	7.3.1		Termination or change of employment responsibilities - Responsibilities and tasks related to information security that remain in effect after termination or change of employment should be defined, communicated to the employee or contractor, and implemented.	BIV-Basic
Termination and change of employment		7.3.1.1	For termination and change of employment, procedures must be in place that describe how responsibilities and rights are transferred. The procedure must include at least the following aspects: a. transfer of keys, passes and the like; b. transfer of roles and rights; c. transfer of data; d. removal of corporate data from ICT resources not managed by SURF; e. transfer of SURF-managed ICT resources. The procedures must be checked at least annually.	BIV-Basic

Chapter 8 - Asset management

Sub-chapter	ISO	ID	Control/measure	Classification
Responsibility for assets	8.1.1		Inventory of assets - Information, other assets associated with information and information processing facilities should be identified and an inventory of these assets should be established and maintained.	BIV-Basic
Responsibility for assets		8.1.1.1	Assets should be tracked through an Asset Management process.	BIV-Basic
Responsibility for assets		8.1.1.2	The Asset Management system clearly notes which systems should be up to classification high (for confidentiality and integrity).	IV-High

Sub-chapter	ISO	ID	Control/measure	Classification
Responsibility for assets	8.1.2		Ownership of assets - Assets maintained in the inventory record must have an owner.	BIV-Basic
Responsibility for assets		8.1.2.1	The owner is responsible for the lifecycle of the asset, regardless of where it is physically run (including cloud). At least the following aspects are part of this: installing, managing, keeping the asset up-to-date and secure, phasing out the asset.	BIV-Basic
Responsibility for assets	8.1.3		Acceptable use of assets - For the acceptable use of information and of assets associated with information and information processing facilities, rules should be identified, documented and implemented.	BIV-Basic
Responsibility for assets		8.1.3.1	Acceptable use of the assets should be established and easily accessible.	BIV-Basic
Responsibility for assets		8.1.3.2	All employees are demonstrably made aware of the rules of conduct for the use of company assets.	BIV-Basic
Responsibility for assets		8.1.3.3	For external staff, the rules of conduct for the use of company assets are laid down in the contract in accordance with the house rules or rules of conduct.	BIV-Basic
Responsibility for assets	8.1.4		Return of company assets - All employees and external users must return all company assets held by the organisation upon termination of their employment, contract or agreement.	BIV-Basic
Information classification	8.2.1		Classification of information - Information should orden classified with respect to legal requirements, value, importance and susceptibility to unauthorised disclosure or modification.	BIV-Basic
Information classification		8.2.1.1	The information in all Information Systems is classified through an explicit risk assessment, so that it is clear which protection is needed.	BIV-Basic
Information classification	8.2.2		Information labelling - To label information, an appropriate set of procedures should be developed and implemented in accordance with the information classification scheme established by the organisation.	BIV-Basic
Information classification	8.2.3		Handling assets - Procedures for handling assets should be developed and implemented in accordance with the information classification scheme established by the organisation.	BIV-Basic
Handling media	8.3.1		Management of removable media - Procedures for managing removable media should be implemented in accordance with the classification scheme established by the organisation.	BIV-Basic
Handling media		8.3.1.1	All removable media in stock must be kept in a location accessible only to authorised persons.	BIV-Basic
Handling media		8.3.1.2	Removable media are not used for external transport of information.	BIV-Basic
Handling media		8.3.1.3	For printing, printers with authentication are used.	BIV-Basic
Handling media		8.3.1.4	For destroying prints, there are paper shredders or secure paper containers.	BIV-Basic
Handling media	8.3.2		Disposal of media - Media should be disposed of in a safe and secure manner when no longer needed, according to formal procedures.	BIV-Basic
Handling media		8.3.2.1	To erase all data on the medium, the data is irretrievably deleted. This is done, for example, by overwriting at least twice with fixed data and once with random data. It is checked whether all data has been irretrievably deleted.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Handling media		8.3.2.2	A certificate of destruction is required if an external party provides erasure of data carriers and/or data.	BIV-Basic
Handling media		8.3.2.3	Media containing confidential information are stored in a place not accessible to unauthorised persons. Disposal takes place in a secure manner, e.g. by burning or shredding. Removal of data only is also possible by erasing the data before the media is used for another application in the organisation (reference ISO 27002, implementation guideline 8.3.2.a).	IV-High
Handling media	8.3.3		The use of couriers or carriers for confidential or higher-classified information meets pre-established reliability requirements.	BIV-Basic
Handling media		8.3.3.1	Policies on physical transport of media have been adopted.	IV-High
Handling media		8.3.3.2	The use of couriers or carriers for confidential or higher-classified information meets pre-established reliability requirements.	IV-High

Chapter 9 - Access security

Sub-chapter	ISO	ID	Control/measure	Classification
Business requirements for access security	9.1.1		Access security policy - An access security policy should be established, documented and reviewed based on business and information security requirements.	BIV-Basic
Business requirements for access security	9.1.2		Access to networks and network services - Users should only access the network and network services for which they are specifically authorised.	BIV-Basic
Business requirements for access security		9.1.2.1	Access to network and network services is based on defined security categories.	BIV-Basic
Business requirements for access security		9.1.2.2	Only authenticated devices can access a trusted area.	BIV-Basic
Business requirements for access security		9.1.2.3	Users with their own or unauthenticated devices (Bring Your Own Device, BYOD) will only access an untrusted area.	BIV-Basic
Business requirements for access security	9.2.1		User registration and logout - A formal registration and logout procedure must be implemented to enable allocation of access rights.	BIV-Basic
Business requirements for access security		9.2.1.1	There is a conclusive formal registration and log-out procedure for managing user identifications.	BIV-Basic
Business requirements for access security		9.2.1.2	The use of group accounts is not allowed unless justified and recorded by the process owner.	BIV-Basic
Business requirements for access security	9.2.2		Granting users access - A formal user access granting procedure should be implemented to assign or revoke access rights for all types of users and for all systems and services.	BIV-Basic
Business requirements for access security		9.2.2.1	Access was granted to Information Systems only after authorisation by an authorised officer.	BIV-Basic
Business requirements for access security		9.2.2.2	Based on a risk assessment, it has been determined where and how segregation of duties is applied and what access rights are given.	BIV-Basic
Business requirements for access security		9.2.2.3	There is an up-to-date mandate register showing which persons have powers to grant access rights or job profiles.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Business requirements for access security		9.2.2.4	Previously issued accounts and associated unique identifiers will not be reused....	BIV-Basic
Business requirements for access security	9.2.3		Managing special access rights - The assignment and use of special access rights should be limited and controlled.	BIV-Basic
Business requirements for access security		9.2.3.1	The allocation and use of special powers are minimised.	BIV-Basic
Business requirements for access security		9.2.3.2	Special powers issued are reviewed at least quarterly.	IV-High
Business requirements for access security	9.2.4		Management of users' secret authentication information - The assignment of secret authentication information should be managed through a formal management process.	BIV-Basic
Business requirements for access security	9.2.5		Assessment of user access rights - Asset owners should regularly assess user access rights.	BIV-Basic
Business requirements for access security		9.2.5.1	All access rights issued are reviewed at least once a year.	BIV-Basic
Business requirements for access security		9.2.5.2	Follow-up of findings is documented and treated as a security incident.	BIV-Basic
Business requirements for access security		9.2.5.3	All access rights issued are reviewed at least once every six months.	IV-High
Business requirements for access security	9.2.6		Revoke or modify access rights - The access rights of all employees and external users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, and they must be modified upon changes.	BIV-Basic
Responsibilities of users	9.3.1		Using secret authentication information - Users should be required to adhere to organisational practices when using secret authentication information.	BIV-Basic
Responsibilities of users		9.3.1.1	Employees are supported in managing their passwords by providing a password safe.	BIV-Basic
System and application access security	9.4.1		Limiting access to information - Access to information and system functions of applications should be restricted in accordance with the access security policy.	BIV-Basic
System and application access security		9.4.1.1	Measures are in place to ensure physical and/or logical isolation of information.	BIV-Basic
System and application access security		9.4.1.2	Users can only access and process the information they need to perform their tasks. This is based on the principles of 'Least Privilege' and 'Need-to-Know'.	BIV-Basic
System and application access security	9.4.2		Secure login procedures - If required by access security policy, access to systems and applications should be governed by a secure login procedure.	BIV-Basic
System and application access security		9.4.2.1	Access to all systems and applications (regardless of where they are located) requires multifactor authentication as a minimum.	BIV-Basic
System and application access security		9.4.2.2	Access for management of systems and applications is only allowed from an internal trusted area.	BIV-Basic
System and application access security		9.4.2.3	A risk assessment is carried out in advance before external suppliers are granted access to the network. The risk assessment determines the conditions under which suppliers are granted access. A record shows how rights are granted.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
System and application access security	9.4.3		Password management system - Password management systems should be interactive and ensure strong passwords.	BIV-Basic
System and application access security		9.4.3.1	Passwords must comply with SURF's password policy. The number of login attempts is a maximum of 10. The length of time an account is blocked after exceeding the number of incorrect login attempts is fixed.	BIV-Basic
System and application access security		9.4.3.2	Passwords are renewed according to established guidelines.	BIV-Basic
System and application access security		9.4.3.3	The password policy is enforced automatically.	BIV-Basic
System and application access security		9.4.3.4	Initial passwords and passwords that have been reset have a maximum validity of 24 hours and must be changed on first use.	BIV-Basic
System and application access security		9.4.3.5	Passwords that comply with the password policy have a maximum validity period of one year. Where the policy is not applicable, a maximum validity period of six months applies.	BIV-Basic
System and application access security	9.4.4		Use special system tools - The use of system tools capable of circumventing management measures for systems and applications should be limited and closely monitored.	BIV-Basic
System and application access security		9.4.4.1	Only authorised personnel have access to system resources.	BIV-Basic
System and application access security		9.4.4.2	The use of system tools is logged. The logging is available for research for six months	BIV-Basic
System and application access security	9.4.5		Access protection on programme source code - Access to the programme source code should be restricted.	BIV-Basic
System and application access security		9.4.5.1	If open source is used, (part of) the programme source code can be shared if necessary to improve or maintain the programme.	BIV-Basic

Chapter 10 - Cryptography

Sub-chapter	ISO	ID	Control/measure	Classification
Cryptographic management measures	10.1.1		Policy on the use of cryptographic management measures - To protect information, a policy on the use of cryptographic management measures should be developed and implemented.	BIV-Basic
Cryptographic management measures		10.1.1.1	The cryptography policy elaborates at least the following topics: a. when cryptography is deployed; b. who is responsible for implementation; c. who is responsible for key management; d. which standards serve as the basis for cryptography and how the standards of the standardisation forum are applied; e. how the level of protection is determined;	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
			f. for communications between organisations, the policy is mutually established.	
Cryptographic management measures		10.1.1.2	Cryptographic applications comply with appropriate standards.	BIV-Basic
Cryptographic management measures	10.1.2		Key management - The use, protection and lifetime of cryptographic keys require the development and implementation of lifecycle policies.	BIV-Basic
Cryptographic management measures		10.1.2.1	The standard ISO 11770 is used for cryptographic key management.	BIV-Basic

Chapter 11 - Physical and environmental security

Sub-chapter	ISO	ID	Control/measure	Classification
Physical and environmental security	11.1.1		Physical security zone - Security zones should be defined and used to protect areas containing sensitive or critical information and information processing facilities.	BIV-Basic
Physical and environmental security		11.1.1.1	Standards for setting up secure areas are used.	BIV-Basic
Physical and environmental security	11.1.2		Physical access security - Secure areas should be protected by appropriate access security to ensure that only authorised personnel have access.	BIV-Basic
Physical and environmental security		11.1.2.1	Access rules are established. Access to rooms in which systems and/or information are stored are secured with an identification, authentication, and authorisation system, and logging of access takes place. Identity must be established in advance	BIV-Basic
Physical and environmental security	11.1.3		Securing offices, spaces and facilities - Physical security should be designed and implemented for offices, spaces and facilities.	BIV-Basic
Physical and environmental security		11.1.3.1	Key management is set up on the basis of a key plan.	BIV-Basic
Physical and environmental security	11.1.4		Protect against external threats - Against natural disasters, malicious attacks or accidents, physical protection must be designed and implemented.	BIV-Basic
Physical and environmental security		11.1.4.1	Security measures have been taken against external threats based on explicit risk assessment.	BIV-Basic
Physical and environmental security		11.1.4.2	Housing IT equipment takes into account the likelihood of consequences of disasters caused by nature and human activity.	BIV-Basic
Physical and environmental security	11.1.5		Working in secure areas - Procedures should be developed and implemented for working in secure areas.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Physical and environmental security		11.1.5.1	In secure areas, everyone must wear visible identification (including guests).	BIV-Basic
Physical and environmental security	11.1.6		Loading and unloading site - Access points such as loading and unloading sites and other points where unauthorised persons may enter the site should be controlled and, if possible, shielded from information processing facilities to avoid unauthorised access.	BIV-Basic
Equipment	11.2.1		Placement and protection of equipment - Equipment should be placed and protected so as to reduce risks from external threats and hazards and the likelihood of unauthorised access.	BIV-Basic
Equipment	11.2.2		Utilities - Equipment should be protected from power outages and other disruptions caused by utility disruptions.	BIV-Basic
Equipment	11.2.3		Protection of cabling - Power and telecommunication cables used to transmit data or that support information services should be protected from interception, disruption or damage.	BIV-Basic
Equipment	11.2.4		Equipment maintenance - Equipment must be properly maintained to ensure its continuous availability and integrity.	BIV-Basic
Equipment		11.2.4.1	Maintenance contract with supplier for support during office hours and response within 4 hours office hours.	BIV-Basic
Equipment		11.2.4.2	Maintenance contract with supplier for support 24 hours x 7 days and response within 2 hours. Agreements for on-site presence of replacement components should be considered.	B-High
Equipment	11.2.5		Disposal of assets - Equipment, information and software may not be taken off site without prior approval.	BIV-Basic
Equipment	11.2.6		Securing off-site equipment and assets - Equipment located off-site must be secured. This should take into account the various risks of working off the organisation's premises.	BIV-Basic
Equipment	11.2.7		Secure removal or reuse of equipment - All equipment components containing storage media should be checked to ensure that sensitive data and licensed software have been removed or reliably securely overwritten prior to removal or reuse.	BIV-Basic
Equipment	11.2.8		Unattended user equipment - Users should ensure that unattended equipment is adequately protected.	BIV-Basic
Equipment	11.2.9		Clear desk and clear screen policies - A clear desk policy for paper documents and removable storage media and a clear screen policy for information processing facilities should be established.	BIV-Basic
Equipment		11.2.9.1	An unattended workplace in an uncontrolled environment is always locked.	BIV-Basic
Equipment		11.2.9.2	Information is automatically made inaccessible with, for example, a screen lock after an inactivity of up to 5 minutes.	BIV-Basic
Equipment		11.2.9.3	Sessions on remote desktops are locked on the remote platform after 15 minutes. Taking over sessions on remote desktops on another client device is only possible via the same secure login procedure used to create the session.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Equipment		11.2.9.4	When using a chip card token to access systems, the access security lock is automatically activated when the token is removed.	BIV-Basic
Equipment		11.2.9.5	Whiteboards, flipcharts and the like in common areas (meeting rooms and flex spaces) should be cleaned after use.	BIV-Basic

Chapter 12 - Security Operations

Sub-chapter	ISO	ID	Control/measure	Classification
Operating procedures and responsibilities	12.1.1		Documented operating procedures - Operating procedures should be documented and made available to all users who need them.	BIV-Basic
Operating procedures and responsibilities	12.1.2		Change management - Changes in the organisation, business processes, information processing facilities and systems that affect information security must be controlled.	BIV-Basic
Operating procedures and responsibilities		12.1.2.1	The change management procedure addressed at least: a. administration of changes; b. risk assessment of possible consequences of the changes; c . approval procedure for changes.	BIV-Basic
Operating procedures and responsibilities	12.1.3		Capacity management - Resource utilisation should be monitored and tuned, and expectations for future capacity requirements should be established to ensure required system performance.	BIV-Basic
Operating procedures and responsibilities		12.1.3.1	With regard to external links, measures are in place to identify and respond to potential attacks that could negatively affect the availability of information services (e.g. DDoS attacks).	BIV-Basic
Operating procedures and responsibilities		12.1.3.2	IT resources should not structurally exceed 90% utilisation, think network, disk space and CPU capacity. A trend increase in occasional overruns should be monitored 24 hours x 7 days and action taken if necessary.	B-High
Operating procedures and responsibilities	12.1.4		Separation of development, test and production environments - Development, test and production environments should be separated to reduce the risk of unauthorised access to or changes to the production environment.	BIV-Basic
Operating procedures and responsibilities		12.1.4.1	No testing takes place in the production environment. Only with prior approval by the process owner and written record of this, can this be deviated from.	BIV-Basic
Operating procedures and responsibilities		12.1.4.2	Changes to the production environment are always tested before being put into production. Only with prior approval by the process owner and written record of this, can this be deviated from.	BIV-Basic
Protection against malware	12.2.1		Malware management measures - To protect against malware, management measures for detection, prevention and remediation should be implemented, and in conjunction with these, appropriate user awareness should be ensured.	BIV-Basic
Protection against malware		12.2.1.1	File downloading is controlled and limited based on risk and need-of-use.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Protection against malware		12.2.1.2	Users have been educated about the risks of surfing and clicking on unknown links.	BIV-Basic
Protection against malware		12.2.1.3	Software and associated recovery software that detects malware are installed and regularly updated.	BIV-Basic
Protection against malware		12.2.1.4	Computers and media are routinely scanned as a precautionary measure. The scan performed should include: a. scanning all files received over networks or via any form of storage medium for malware before use; b. attachments and downloads before use.	BIV-Basic
Protection against malware		12.2.1.5	The malware scan is performed on different environments, for example on mail servers, desktop computers and when accessing the organisation's network.	BIV-Basic
Backup	12.3.1		Backup of information - Regular backups of information, software and system images should be made and tested in accordance with an agreed backup policy.	BIV-Basic
Backup		12.3.1.1	A backup policy defining and establishing retention and protection requirements is in place	BIV-Basic
Backup		12.3.1.2	Based on an explicit risk assessment, the maximum allowable data loss and the maximum recovery time after an incident were determined.	BIV-Basic
Backup		12.3.1.3	To prevent damage during a disaster, at least one backup copy must be physically stored at a remotel location. The minimum distance from the remotel location to the data centre (main location) is 5 km.	BIV-Basic
Backup		12.3.1.4	The restore procedure is tested at least annually or after a major change to ensure reliability if it needs to be performed in an emergency.	BIV-Basic
Backup		12.3.1.5	The maximum allowable data loss is 1 hour.	B-High
Reporting and monitoring	12.4.1		Log events - Log files of events that record user activities, exceptions and information security events should be created, retained and reviewed regularly.	BIV-Basic
Reporting and monitoring		12.4.1.1	A log line contains at least the event: a. the information necessary to trace the incident back to a natural person with a high degree of certainty; b. the device used; c. the result of the operation (e.g. read, write, modify and delete); d. the date and time of the event.	BIV-Basic
Reporting and monitoring		12.4.1.2	Under no circumstances does a log line contain data that could lead to a security breach.	BIV-Basic
Reporting and monitoring		12.4.1.3	All authentication logs are forwarded to the central logging server	BIV-Basic
Reporting and monitoring		12.4.1.4	The information processing environment is monitored on the basis of a risk assessment, partly based on and the nature of the data and Information Systems to be protected, so that attacks can be detected.	BIV-Basic
Reporting and monitoring		12.4.1.5	Network flow information is sampled and sent to a central data collector.	BIV-Basic
Reporting and monitoring		12.4.1.6	Logging is turned on for all processing of data by the system or applications. This covers all types of processing: read, write, modify and delete.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Reporting and monitoring		12.4.1.7	An automated monitoring system reviews the log files and produces alarms in case of irregularities or situations indicating a potential risk.	IV-High
Reporting and monitoring	12.4.2		Protecting information in log files - Log facilities and information in log files should be protected against falsification and unauthorised access.	BIV-Basic
Reporting and monitoring		12.4.2.1	There is an overview of log files. The log files are generated indicating storage location.	BIV-Basic
Reporting and monitoring		12.4.2.2	For log analysis, log files should be kept for a minimum period of 6 months. Within this period, the availability of log information is guaranteed.	BIV-Basic
Reporting and monitoring		12.4.2.3	Log files are protected against modification or destruction. Access to logs is logged.	BIV-Basic
Reporting and monitoring		12.4.2.4	There is an (independent) internal audit procedure that tests for the unchanged existence of log files at least semi-annually.	IV-High
Reporting and monitoring		12.4.2.5	Improper modification, deletion or attempted deletion of log data shall be reported as soon as possible as a security incident through the information security incident procedure.	IV-High
Reporting and monitoring	12.4.3		Log files of administrators and operators - Activities of system administrators and operators should be recorded and the log files should be protected and reviewed regularly.	BIV-Basic
Reporting and monitoring		12.4.3.1	All actions of system admins are logged.	IV-High
Reporting and monitoring	12.4.4		Clock synchronisation - The clocks of all relevant information processing systems within an organisation or security domain should be synchronised to a single reference time source.	BIV-Basic
Reporting and monitoring		12.4.4.1	It contains the correct time, time zone (local time zone) and date.	BIV-Basic
Reporting and monitoring		12.4.4.2	The system clock and time synchronisation via the SURF NTP (Network Time Protocol) servers are set.	BIV-Basic
Control of operational software	12.5.1		Installing software on operational systems - To control the installation of software on operational systems, procedures should be implemented.	BIV-Basic
Managing technical vulnerabilities	12.6.1		Management of technical vulnerabilities - Information about technical vulnerabilities of Information Systems in use should be obtained in a timely manner, the organisation's exposure to such vulnerabilities should be assessed and appropriate measures should be taken to address the associated risk.	BIV-Basic
Managing technical vulnerabilities		12.6.1.1	Patch management must be in place for every system connected to the SURF network and the software installed on it, regardless of all other security and management measures realised.	BIV-Basic
Managing technical vulnerabilities		12.6.1.2	The department under which the management of the system falls must provide an adequate patch schedule.	BIV-Basic
Managing technical vulnerabilities		12.6.1.3	Each patch is assessed for impact and consequences. Based on this assessment, it is prioritised. Depending on the priority and impact, the installation of the patch is planned. This may result in an immediate rollout of the patch, a rollout during the next	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
			maintenance window or a rollout at a date sometime in the future.	
Managing technical vulnerabilities		12.6.1.4	Security patches should be treated as a priority. This means making an immediate assessment of impact and priority.	BIV-Basic
Managing technical vulnerabilities		12.6.1.5	If a high-priority patch cannot be rolled out quickly, for example on technical grounds, an adequate work-around and/or measures to protect the system or application from vulnerabilities must be put in place for it.	BIV-Basic
Managing technical vulnerabilities		12.6.1.6	As part of system hardening, unnecessary components, services and software on the servers and network elements should be disabled to minimise the risk of technical vulnerabilities and successful attacks. In other words, only the necessary components run on the system.	BIV-Basic
Managing technical vulnerabilities	12.6.2		Restrictions on installing software - Rules should be established and implemented for users to install software.	BIV-Basic
Managing technical vulnerabilities		12.6.2.1	Users can install software on their work environment. Workstations are monitored for installed software and suspicious behaviour.	BIV-Basic
Considerations regarding audits of Information Systems	12.7.1		Management measures regarding audits of Information Systems - Audit requirements and activities involving verification of execution systems should be carefully planned and coordinated to minimise disruption to business processes.	BIV-Basic

Chapter 13 - Communication security

Sub-chapter	ISO	ID	Control/measure	Classification
Network security management	13.1.2		Network services security - Eise for security mechanisms, service levels and management for all network services should be identified and included in agreements on network services. This applies both to services provided internally and to outsourced services.	BIV-Basic
Network security management		13.1.2.1	Data traffic entering or leaving the organisation is monitored against and analysed for malicious elements with detection facilities, such as the National Detection Network, deployed on the basis of a risk assessment, partly based on the nature of the data and Information Systems to be protected.	BIV-Basic
Network security management		13.1.2.2	Connection to corporate networks (including wireless) is possible only after authentication.	BIV-Basic
Network security management		13.1.2.3	For external access to internal networks, a VPN server equipped with Multi Factor Authentication is used.	BIV-Basic
Network security management		13.1.2.4	For wireless connections such as Wi-Fi and for wired connections outside the controlled area, encryption means are used.	BIV-Basic
Network security management		13.1.2.5	New threats detected by the detection solution mentioned in 13.1.2.1, taking into account the applicable legal frameworks, are preferably reported by automated	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
			mechanisms (threat intelligence sharing) and handled by internal SURF CERT/SOC.	
Network security management		13.1.2.6	Network traffic is filtered both incoming and outgoing. Filtering is deployed based on the nature of the data and information systems to be protected and partly on the basis of a risk assessment.	BIV-Basic
Network security management	13.1.3		Security mechanisms, service levels and management requirements for all network services should be identified and included in agreements on network services. This applies both to services provided internally and to outsourced services.	BIV-Basic
Network security management		13.1.3.1	Each VLAN has a defined security protection level.	BIV-Basic
Network security management		13.1.3.1	The security of the IT systems is based on defined security levels according to a structured VLAN classification.	BIV-Basic
Information transport	13.2.1		Information transport policies and procedures - To protect information transport, which is done through all types of communication facilities, formal transport policies, procedures and management measures should be in place.	BIV-Basic
Information transport	13.2.2		Information transport agreements - Agreements should cover the secure transport of business information between the organisation and external parties.	BIV-Basic
Information transport	13.2.3		Electronic messages - Information contained in electronic messages should be appropriately protected.	BIV-Basic
Information transport		13.2.3.1	The security of electronic messages is subject to the established standards against malware, phishing, eavesdropping and modification such as SPF, DKIM, DMARC and encryption.	BIV-Basic
Information transport		13.2.3.2	E-mail messages are automatically scanned for the presence of spam messages and viruses and other malicious software.	BIV-Basic
Information transport		13.2.3.3	Data in transit should always be encrypted. Use SURF certificates for web and e-mail traffic of sensitive data. Sensitive data include digital documents from which users can derive rights.	BIV-Basic
Information transport		13.2.3.4	The ICT Resources Use Regulations (also known as the Acceptable Use Policy) describe how staff should handle ICT resources (internet, laptops, e-mail, etc.).	BIV-Basic
Information transport	13.2.4		Confidentiality or non-disclosure agreement - Requirements for confidentiality or non-disclosure agreements that reflect the organisation's information protection needs should be established, regularly reviewed and documented.	BIV-Basic

Chapter 14 - Acquisition, development and maintenance of information systems

Sub-chapter	ISO	ID	Control/measure	Classification
Security requirements for Information Systems	14.1.1		Analysis and specification of information security requirements - Information security-related requirements should be included in the requirements for new Information Systems or extensions of existing Information Systems.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Security requirements for Information Systems		14.1.1.1	For new Information Systems and changes to existing Information Systems, an explicit risk assessment must be carried out to determine the security requirements, based on SURF's baseline.	BIV-Basic
Security requirements for Information Systems	14.1.2		Secure applications on public networks - Information that is part of executive services and exchanged over public networks should be protected against fraudulent activities, contract disputes and unauthorised disclosure and modification.	BIV-Basic
Security requirements for Information Systems		14.1.2.1	See measure 13.2.3.3 (Make use of SURF certificates)	BIV-Basic
Security requirements for Information Systems	14.1.3		Protecting application transactions - Information forming part of application transactions must be protected to prevent incomplete transmission, incorrect routing, unauthorised modification of messages, unauthorised disclosure, unauthorised duplication or playback.	BIV-Basic
Security requirements for Information Systems		14.1.3.1	See measure 13.2.3.3 (Make use of SURF certificates)	BIV-Basic
Security in development and support processes	14.2.1		Policy for secure development - Rules for developing software and systems should be established and applied to development activities within the organisation.	BIV-Basic
Security in development and support processes		14.2.1.1	Security by Design is the starting point for the development of software and systems.	BIV-Basic
Security in development and support processes		14.2.1.2	Testing and development of software and systems is carried out on the OTAP principle.	BIV-Basic
Security in development and support processes	14.2.2		Change management procedures related to systems - Changes to systems within the development life cycle should be controlled through the use of formal change management procedures.	BIV-Basic
Security in development and support processes		14.2.2.1	A generally accepted framework such as FitSM or ITIL is used for change management.	BIV-Basic
Security in development and support processes	14.2.3		Technical assessment of applications after control platform changes - If control platforms have changed, business-critical applications should be assessed and tested to ensure there is no adverse impact on the organisation's operations or security.	BIV-Basic
Security in development and support processes	14.2.4		Restrictions on changes to software packages - Changes to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.	BIV-Basic
Security in development and support processes	14.2.5		Principles for engineering secure systems - Principles for engineering secure systems should be established, documented, maintained and applied for all operations concerning the implementation of Information Systems.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Security in development and support processes		14.2.5.1	See control 14.2.1.1 (Security by Design)	BIV-Basic
Security in development and support processes	14.2.6		Secure development environment - Organisations should establish and appropriately secure secure development environments for system development and integration operations that cover the entire system development lifecycle.	BIV-Basic
Security in development and support processes		14.2.6.1	See control 14.2.1.2 (OTAP)	BIV-Basic
Security in development and support processes	14.2.7		Outsourced software development - Outsourced system development should be supervised and monitored by the organisation.	BIV-Basic
Security in development and support processes		14.2.7.1	A prerequisite for outsourcing processes is an explicit risk assessment. The necessary resulting security measures are imposed on the supplier.	BIV-Basic
Security in development and support processes	14.2.8		Testing system security - Security functionality should be tested during development activities.	BIV-Basic
Security in development and support processes	14.2.9		System acceptance testing - For new Information Systems, upgrades and new versions, programmes for conducting acceptance testing and related criteria should be established.	BIV-Basic
Security in development and support processes		14.2.9.1	A system or application is subjected to a predefined acceptance test.	BIV-Basic
Security in development and support processes		14.2.9.2	Structured testing methodologies such as TMap, for example, are used for acceptance testing of systems. The tests are preferably automated.	BIV-Basic
Test data	14.3.1		Protection of test data - Test data must be carefully chosen, protected and controlled.	BIV-Basic
Test data		14.3.1.1	Production data should not be used as test data. The same measures apply to the test environment as in the production environment.	BIV-Basic
Test data		14.3.1.2	If it is unavoidable that production data are used in a test environment, they should be anonymised or pseudonymised.	BIV-Basic

Chapter 15 - Supplier relations

Sub-chapter	ISO	ID	Control/measure	Classification
Information security in supplier relations	15.1.1		Information security policy for supplier relationships - Information security requirements to reduce risks associated with the supplier's access to the	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
			organisation's assets should be agreed and documented with the supplier.	
Information security in supplier relations		15.1.1.1	Information security requirements (availability, integrity and confidentiality) are named in calls for tender where information (provision) is involved.	BIV-Basic
Information security in supplier relations		15.1.1.2	Control measures for supplier access to business information are established based on explicit risk assessment.	BIV-Basic
Information security in supplier relations		15.1.1.3	Processor agreements are concluded with all suppliers who process personal data as processors for or on behalf of the organisation, setting out all legally required agreements.	BIV-Basic
Information security in supplier relations	15.1.2		Inclusion of security aspects in supplier agreements - All relevant information security requirements should be identified and agreed with any supplier that accesses, processes, stores, communicates or provides IT infrastructure elements for the benefit of the organisation's information.	BIV-Basic
Information security in supplier relations		15.1.2.1	The security requirements from the call for tender are explicitly included in the (procurement) contracts where information plays a role.	BIV-Basic
Information security in supplier relations		15.1.2.2	Procurement contracts explicitly include performance indicators and related accountability reports.	BIV-Basic
Information security in supplier relations		15.1.2.3	Procurement contracts explicitly include the possibility of an external audit to check the reliability of the service provided. An audit is not necessary if the contractor demonstrates through certification that the desired reliability of the service is guaranteed.	BIV-Basic
Information security in supplier relations		15.1.2.4	To ensure confidentiality or secrecy, standard terms and conditions of procurement are used in IT procurement.	BIV-Basic
Information security in supplier relations		15.1.2.5	Before a contract is concluded, a risk assessment determines whether the dependence on a supplier is manageable. An integral part of the contract is an explicit elaboration of the exit strategy.	BIV-Basic
Information security in supplier relations		15.1.2.6	Procurement contracts will explicitly include the possibility of an external audit to test the reliability of the service provided. An audit is not necessary if the contractor demonstrates through certification that the desired reliability of the service is guaranteed.	IV-High
Information security in supplier relations	15.1.3		Information and communication technology supply chain - Agreements with suppliers should include requirements that address information security risks associated with the information and communication technology services and products supply chain.	BIV-Basic
Information security in supplier relations		15.1.3.1	Suppliers must disclose their supply chain and be transparent about the measures they have taken to extend the requirements imposed on them to their suppliers.	BIV-Basic
Management of supplier services	15.2.1		Monitoring and assessing supplier services - Organisations should regularly monitor, assess and audit supplier services.	BIV-Basic
Management of supplier services		15.2.1.1	At least once a year, suppliers' information security performance is assessed against predefined performance indicators, as included in the contract.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Management of supplier services	15.2.2		Management of changes in supplier services - Changes in supplier services including maintaining and improving existing information security policies, procedures and control measures should be, managed, taking into account affected systems and processes, reassessment of risks and how critical business information is.	BIV-Basic

Chapter 16 - Information security incident management

Sub-chapter	ISO	ID	Control/measure	Classification
Management of information security incidents and improvements	16.1.1		Responsibilities and procedures - Board responsibilities and procedures should be established to ensure a prompt, effective and orderly response to information security incidents.	BIV-Basic
Management of information security incidents and improvements	16.1.2		Information security event reporting - Information security events should be reported through the appropriate management levels as soon as possible.	BIV-Basic
Management of information security incidents and improvements		16.1.2.1	All security incidents are reported to SURF-IRT.	BIV-Basic
Management of information security incidents and improvements		16.1.2.2	The SURF-IRT team follows up on security incidents according to the applicable incident procedure and ensures the necessary escalations.	BIV-Basic
Management of information security incidents and enhancements		16.1.2.3	All employees and contractors have demonstrably familiarised themselves with the security incident procedure.	BIV-Basic
Management of information security incidents and improvements		16.1.2.4	Incidents are reported to the SURF-IRT (SIRT) as soon as possible, but in any case within 24 hours of becoming known.	BIV-Basic
Management of information security incidents and improvements		16.1.2.5	The process owner is responsible for resolving security incidents.	BIV-Basic
Management of information security incidents and improvements		16.1.2.6	The follow-up of incidents is reported periodically to the person in charge.	BIV-Basic
Management of information security incidents and improvements		16.1.2.7	Information derived from the procedure for coordinated vulnerability disclosure (formerly 'responsible disclosure', is part of incident reporting.	BIV-Basic
Management of information security incidents and improvements	16.1.3		Reporting information security weaknesses - Employees and contractors using the organisation's Information systems and services should be required to record and report information security weaknesses observed or perceived in systems or services.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Management of information security incidents and enhancements		16.1.3.1	A procedure for coordinated vulnerability disclosure has been published and set up (for heen 'responsible disclosure').	BIV-Basic
Management of information security incidents and enhancements	16.1.4		Assessment and decision-making on information security events - Information security events should be assessed, judging whether they should be classified as information security incidents.	BIV-Basic
Management of information security incidents and enhancements		16.1.4.1	Information security incidents that have resulted in a suspected or possible intentional breach of the availability, confidentiality or integrity of information processing systems must be reported as soon as possible (within 24 hours) to SURF-IRT (SIRT). SIRT, together with the responsible department, then makes an impact analysis of the incident and defines necessary remedial measures.	BIV-Basic
Management of information security incidents and enhancements	16.1.5		Information security incident response - Information security incidents should be responded to in accordance with documented procedures.	BIV-Basic
Management of information security incidents and improvements	16.1.6		Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	BIV-Basic
Management of information security incidents and enhancements		16.1.6.1	Security incidents are analysed with the aim of learning and preventing future security incidents.	BIV-Basic
Management of information security incidents and enhancements		16.1.6.2	Security incident analyses are shared with relevant partners to prevent recurrence and future incidents.	BIV-Basic
Management of information security incidents and enhancements	16.1.7		Collection of evidence - The organisation must define and implement procedures for identifying, collecting, obtaining and retaining information that can serve as evidence.	BIV-Basic

Chapter 17 - Information security aspects of business continuity management

Sub-chapter	ISO	ID	Control/measure	Classification
Information security continuity	17.1		Information security aspects of business continuity management have been implemented.	BIV-Basic
Information security continuity	17.1.1		Information security continuity plans - The organisation must establish its requirements for information security and for continuity of information security management in adverse situations, e.g. a crisis or disaster.	BIV-Basic
Information security continuity		17.1.1	A crisis plan should be in place and be part of the information security continuity plans.	BIV-Basic
IInformation security continuity	17.1.2		Implement information security continuity - The organisation must establish, document, implement and maintain processes, procedures and control measures to ensure the required level of continuity for information security during an adverse situation.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classification
Information security continuity	17.1.3		Information security continuity verification, assessment and evaluation - The organisation must regularly verify the control measures established and implemented for information security continuity to ensure that they are sound and effective during adverse situations.	BIV-Basic
Information security continuity		17.1.3.1	Continuity plans of business-critical systems are tested annually for validity and usability. Continuity plans of other systems are tested biannually for validity and usability.	BIV-Basic
Information security continuity		17.1.3.2	By performing an explicit risk assessment, the business-critical process components and their associated reliability requirements are identified.	BIV-Basic
Information security continuity		17.1.3.3	The service of the mission-critical components is restored within a week in case of calamities at least.	BIV-Basic
Information security continuity		17.1.3.4	The crisis plan are tested annually for validity, timeliness and usability.	BIV-Basic
Redundant components	17.2.1		Availability of information processing facilities - Information processing facilities should be implemented with sufficient redundancy to meet availability requirements.	BIV-Basic
Redundant components		17.2.1.1	The maximum recovery time after an incident, disaster or information processing facility failure is 4 hours.	B-High

Chapter 18 - Compliance

Sub-chapter	ISO	ID	Control/measure	Classification
Compliance with legal and contractual requirements	18.1.1		Establish applicable legislation and contractual requirements - All relevant statutory, regulatory, contractual requirements and the organisation's approach to meeting them should be explicitly established, documented and kept up to date for each information system and the organisation.	BIV-Basic
Compliance with legal and contractual requirements	18.1.2		Intellectual property rights - To ensure compliance with legal, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products, appropriate procedures should be implemented.	BIV-Basic
Compliance with legal and contractual requirements	18.1.3		Protect records - Records must be protected against loss, destruction, falsification, unauthorised access and unauthorised release in accordance with legal, regulatory, contractual and business requirements.	BIV-Basic
Compliance with legal and contractual requirements		18.1.3.1	The retention period for each type of information has been clarified.	BIV-Basic
Compliance with legal and contractual requirements	18.1.4		Privacy and protection of personal data - Privacy and protection of personal data should be ensured, where applicable, in accordance with relevant laws and regulations.	BIV-Basic
Compliance with legal and contractual requirements		18.1.4.1	In line with the AVG, every organisation has a Data Protection Officer (FG) with sufficient mandate to perform his/her function.	BIV-Basic
Compliance with legal and contractual requirements		18.1.4.2	Organisations regularly check compliance with privacy rules and information processing and procedures within its area of responsibility against relevant policies, standards and other security requirements.	BIV-Basic

Sub-chapter	ISO	ID	Control/measure	Classificati on
Compliance with legal and contractual requirements	18.1.5		Requirements for the use of cryptographic management measures - Cryptographic management measures should be applied in accordance with all relevant agreements, laws and regulations.	BIV-Basic
Compliance with legal and contractual requirements		18.1.5.1	Cryptographic control measures should explicitly adhere to international standards.	BIV-Basic
Information security assessments	18.2.1		Independent assessment of information security - The organisation's approach to managing information security and its implementation (e.g. management objectives, management measures, policies, processes and procedures for information security), should be independently assessed at planned intervals or as soon as significant changes occur.	BIV-Basic
Information security assessments		18.2.1.1	There is an information security information system (ISMS) that demonstrably covers the entire PDCA cycle (plan-do-check-act) in a structured manner.	BIV-Basic
Information security assessments		18.2.1.2	There is an established audit plan in which annual choices are made for which systems what type of security audits are carried out.	BIV-Basic
Information security assessments	18.2.2		Compliance with security policies and standards - The board should regularly assess compliance with information processing and procedures within its area of responsibility against relevant policies, standards and other security requirements.	BIV-Basic
Information security assessments		18.2.2.1	Information security is reported in the P&C cycle. Service owner to process owner, process owner to board.	BIV-Basic
Information security assessments	18.2.3		Assessment of technical compliance - Information systems should be regularly assessed for compliance with the organisation's information security policies and standards.	BIV-Basic
Information security assessments		18.2.3.1	Information systems are checked annually for technical compliance with security standards and risks regarding actual security. This can be done, for example, through (automated) vulnerability analyses or pen tests.	IV-High