Samen aanjagen van vernieuwing

BIS

Baseline Information security SURF

Author(s)	: CISO team
Version	: see colophon
Date	: February 1, 2024
Feature	: Baseline Information Security SURF (BIS)

Colophon

This document describes the baseline for information security at SURF, the set of minimum security standards that form the basis for data security at SURF: the Baseline Information Security SURF, abbreviated 'BIS'. The BIS is a standard arising from SURF's Information Security Policy.

Document properties

Title	BIS
Subject	Baseline Information Security SURF (BIS)
Document type	Standard
Classification	SURF public
Date	September 3, 2024
Owner	Chief Information Security Officer
Status	2.0

Version management

Version	Date	By	Explanation of change	Determination
1.0	19-10-2021	Alvin Anita, René Ritzen, Rosanne Pouw, Bart Bosman, Sedat Çapkin	Initial document	CISO
1.2	April 2023	CISO team	Definitions, classification renewed, BIS set renewed	CISO
1.3/1.5	July 2023/February 2024	Helma	Intermediate version, concept	-
2.0	03-09-2024	Helma, Sedat, Alvin, Arvid	BIS 2024 based on ISO 27001:2022 et al major	CISO

Table of contents

1 Information security SURF

1.1 Introduction and scope

Information security is the process of determining the required security of information systems in terms of confidentiality, availability and integrity and implementing, maintaining and monitoring a coherent package of associated measures. For determining those security measures, SURF uses the document standard Baseline Information Security SURF (hereinafter referred to as BIS).

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

- SURF information security policy
- ISO 27001 and ISO 27002
- SURF Sector Baseline (surf.sec.nl)
- General Data Processing Regulation
- Other laws and regulations, such as NIS2

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.

Scope

The BIS sets out the security measures (organisational, human-centred, physical and technical) for SURF's information (systems). The BIS applies to the entire SURF organisation, including the services and systems where information is processed. By following these measures, SURF can provide reliable and professional services and information provision.

For definitions, see intranet: information security glossary.

1.2 Roles and responsibility

Roles and responsibilities follow the Three Lines model (3LM) as described in the information security policy. SURF's Executive Board is ultimately responsible for overall security. Line management is responsible for implementing appropriate security measures. The service manager or any assigned process owner is responsible for making decisions on the level of protection required (the risk classification).

SURF provides part of the implementation of the security measures centrally; for the rest, it is the service owner. The BIS makes this distinction and always indicates who is responsible for the implementation of a security measure.

1.3 Evaluation and adjustment

With advances in technology, information security measure sets can quickly become outdated. While the BIS is written as concretely as possible, it only describes the what and not the how. Thus, technical developments have as little impact as possible on the content. Procedures and guidelines for operational implementation are therefore not incorporated in the BIS itself; information on these can be found on the intranet.

This document is reviewed regularly, at least annually, in its entirety and updated as necessary. Changes may be required, for example due to changes in underlying laws and regulations, new or updated policies guidelines, ISO standard or new threats and vulnerabilities, etc. Measures that change are given a raised version number to facilitate comparison.

The annual review also checks whether changes/additions to the measures and (operational) procedures and guidelines are needed. This helps increase practical applicability.

2 Operation of BIS measures

2.1 ISO 27001 controls as a basis

The controls from the ISO 27001 standard consist of 93 management measures (controls) and form the basis of the baseline. The ISO 27002 standard is a specification of the ISO 27001 standard. The ISO 27002 standard helps as a practical guideline to define information security measures for availability, integrity and confidentiality of the information facility.

The list of controls follows this standard and accompanies this document. The appendix contains the controls including concrete measures. The BIS is published on the surf.nl website so that members can see exactly what SURF's security measures entail. From a practical point of view, the list can also be downloaded via the intranet for personal use.

2.2 Selection of measures and hardness determinations

Risk analysis and information classification (BIV) determine which BIS security measures should be taken. See the document 'SURF Information Security Risk Management' (SRI)

Once it is known which classification applies, the relevant measures should be selected. Depending on the context, some measures from the standard set are not applicable); this is the hardness determination: if a control cannot be applicable for a specific case, then the control and the associated, more detailed measures are not applicable. This applies, for example, if a control 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, see 2.3.

2.3 Apply or explain and acceptance

The controller of a service or processing provides a record of the BIS measures that do not apply, cannot yet be fully complied with and why they cannot (yet) be complied with, including an inclusive explanation of the resulting risks.

This is the accountability (aka '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.

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 usually 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 implement appropriate measures or temporary measures that mitigate or reduce the risk until the explains are implemented according to the BIS.

3 Information security frameworks based on classification

For the BIS:

- Line management is responsible for information safety and the security of information (systems).
- Line management sets the level of protection of information in its systems for the BIV aspects of reliability, integrity and confidentiality (basic or high). This is called information classification and suitability classification. For the method of classification, see the document 'SURF Information Security Risk Management'.
- 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 corresponding measures.
- Information security is a cyclical improvement process according to the PDCA (Plan-Do-Check-Act) methodology.

4 BIS - Baseline Information Security SURF - 2024

BIS - Chapter overview

Below is the overview of BIS controls and measures (in accordance with the ISO numbering ISO 27001:2022). The complete list of controls and measures can be found in chapters 5 to 8.

5. Organisational management measure

5.1 Information security policies
5.2 Roles and responsibilities in information security
5.3 Separation of functions
5.4 Management responsibilities
5.5 Contact with government agencies
5.6 Contact with special interest groups
5.7 Information on information security threats
5.8 Information security in project management
5.9 Inventory of information and other related assets
5.10 Accepted use of information and other related business assets
5.11 Return of assets
5.12 Classifying information
5.13 Labelling of information
5.14 Transfer of information
5.15 Access security
5.16 Identity management
5.17 Managing authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.20 Addressing information security in supplier agreements
5.21 Managing information security in the ICT chain
5.22 Monitoring, reviewing and managing changes to supplier services
5.23 Information security for the use of cloud services
5.24 Planning and preparing information security incident management
5.25 Assessing and deciding on information security events
5.26 Responding to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
5.29 Information security during a disruption
5.30 ICT readiness for business continuity
5.31 Legal, statutory, regulatory and contractual requirements
5.32 Intellectual property rights
5.33 Protect registrations
5.34 Privacy and protection of personal data
5.35 Independent assessment of information security
5.36 Compliance with information security policies, rules and standards
5.37 Documented operating procedures

6. People-oriented management measure

6.1 Screening
6.2 Employment contract
6.3 Awareness, education and training on information security
6.4 Disciplinary procedure
6.5 Responsibilities after termination or change of employment
6.6 Confidentiality or non-disclosure agreements
6.7 Working remotely
6.8 Reporting information security events

7. Physical management measure

7.1 Physical security areas
7.2 Physical access security
7.3 Securing offices, rooms and facilities
7.4 Monitoring physical security
7.5 Protect against physical and environmental threats
7.6 Working in secure areas
7.7 'Clear desk' and 'clear screen'
7.8 Placing and protecting equipment
7.9 Securing off-site assets
7.10 Storage media
7.11 Utilities
7.12 Securing cabling
7.13 Maintenance of equipment
7.14 Safe disposal or reuse of equipment

8. Technical management measure

8.1 User equipment
8.2 Special access rights
8.3 Limiting access to information

8.4 Access security on source code

8.5 Secure authentication

8.6 Capacity management

8.7 Protection against malware

8.8 Managing technical vulnerabilities

8.9 Configuration management

8.10 Deleting information

8.11 Masking of data

8.12 Preventing data leaks

8.13 Backup of information

8.14 Redundancy of information processing facilities

8.15 Event registration

8.16 Monitoring activities

8.17 Clock synchronisation

8.18 Use of special system tools

8.19 Installing software on operational systems

8.20 Security of network components

8.21 Security of network services

8.22 Network segmentation

8.23 Applying web filters

8.24 Use of cryptography

8.25 Securing during the development cycle

8.26 Application protection requirements

8.27 Principles for engineering secure systems and system architectures

8.28 Developing secure software

8.29 Testing security during development and acceptance

8.30 Outsourced system development

8.31 Separation of development, test and production environments

8.32 Change management

8.33 Test data

8.34 Protection of information systems during audit

5 BIS - Organisational measures

5. Organisational	BIS ID	Management measure	GFCF	Version
Information security policies	5.01	SURF has published and communicated information security policies adopted by the Executive Board.	BIV Standard	2.0
	5.01.1	SURF has established a baseline of security measures (the BIS, Baseline Information Security SURF) as a concrete implementation of the information security policy.	BIV Standard	
	5.01.2	Services formulate additional information security regulations where appropriate.	IV-High	2.0
	5.01.3	SURF reviews the SURF-wide information security policy once every three years or more often if necessary.	BIV Standard	2.0
	5.01.4	Services check at least once a year whether additional regulations are still up to date or need to be updated.	IV-High	2.0
Roles and responsibilities in information security	5.02	SURF generically describes the roles and responsibilities for information security in the strategic information security policy.	BIV Standard	2.0
	5.02.1	SURF has drawn up a CISO job profile defining the role and responsibilities of the CISO, and a CISO has been appointed according to this profile.	BIV Standard	2.0
	5.02.2	As a service, you describe the roles and corresponding responsibilities for information security (based on the information security policy). You assign these. In this allocation, you take into account what SURF needs as an organisation.	BIV Standard	2.0
Separation of functions	5.03	The service ensures that employees are not given combinations of roles and powers that allow them to manipulate (important or critical) processes, systems or data or make unintentional mistakes without peer control.	BIV Standard	2.0
	5.03.1	Risky tasks are separated in a way that minimises the risk of errors, fraud, theft, etc.	BIV Standard	2.0
	5.03.2	The service describes authorisations that fit a role. To check whether requested authorisations fit an employee's role, the granting of authorisations is recorded. The assignment of those authorisations is described in the authorisation process	BIV Standard	2.0
	5.03.3	The service applies strict separation between management and usage tasks specifically for devices deployed for security, such as firewalls, camera security and alarm systems.	BIV Standard	2.0
	5.03.4	The service applies the four-eye principle when performing critical work. This is specifically important when providing access and granting privileges in systems.	IV-High	2.0
	5.03.5	The service strictly applies segregation of duties when one of tasks is combined with conflicting work.	IV-High	2.0
Management responsibilities	5.04	The board directs that all employees deal with information security according to the SURF policy (and associated procedures).	BIV Standard	2.0
	5.04.1	SURF's board oversees the implementation of the required security measures (according to the Baseline Information Security SURF, the 'BIS').	BIV Standard	2.0

5. Organisational	BIS ID	Management measure	GFCF	Version
	5.04.2	Every team ensures sufficient staffing (capacity) to carry out important tasks and processes also during periods of lower staffing (such as holidays). To this end: a. capacity is monitored so that structural understaffing is signalled and addressed. b . procedures are known in case of unplanned absence of team members c. individuals are identified as SPoF (Single Point of Failure) if they are the only ones capable of performing specific (important) tasks.	BIV Standard	2.0
	5.04.3	The service ensures that vulnerable knowledge (of SPoFs, Single Point of Failure) is secured through knowledge transfer or through external expertise.	BIV Standard	2.0
	5.04.4	Employees can report information security issues anonymously. A whistleblower scheme is available for this purpose.	BIV Standard	2.0
Contact with government agencies	5.05	SURF has and maintains contact with the government where necessary in the field of information security.	BIV Standard	2.0
	5.05.1	SURF has drawn up a list showing which government agencies and regulators are in contact with. This list is updated regularly, at least annually.	BIV Standard	2.0
	5.05.2	SURF has a process for notifying the competent authority with the appropriate information. Changes are notified within two weeks.	BIV Standard	2.0
Contact with special interest groups	5.06	SURF has and maintains contact with stakeholders and experts in the field of information security.	BIV Standard	2.0
	5.06.1	SURF has drawn up a list showing which stakeholders and experts are contacted. This list is updated regularly.	BIV Standard	2.0
Threat information and analysis	5.07	SURF collects information on threats to information security. That information is analysed to adequately inform the organisation about threats in order to respond to them.	BIV Standard	2.0
	5.07.1	The service conducts a risk analysis to understand the information security risks (probability * impact) that exist and periodically updates this analysis.	BIV Standard	2.0
Information security in project management	5.08	With every project or new development, conscious attention is paid to implementing appropriate security measures.	BIV Standard	2.0
	5.08.1	The project team makes a risk assessment (risk analysis and classification) to determine the BIS security measures required. You update this risk analysis in the different project phases.	BIV Standard	2.0
	5.08.2	The project team applies 'Security by Design' and describes in the project plan how it will be implemented.	BIV Standard	2.0
Inventory of information and other related assets	5.09	The service inventories: what information it manages what assets it uses and who owns them This is contained in an inventory list that is regularly renewed.	BIV Standard	2.0
	5.09.1	The service manages its own assets through an Asset Management process.	BIV Standard	2.0
	5.09.2	For each object/asset (including cloud), lifecycle management is arranged with procedures for at least: installation management keeping security up to date phasing out	BIV Standard	2.0

5. Organisational	BIS ID	Management measure	GFCF	Versio n
	5.09.3	In the configuration management database (CMDB), any system that scores 'high' in terms of risk in terms of integrity and confidentiality is given a label showing this.	IV-High	2.0
Acceptable use of information and other related assets	5.10	SURF has ICT regulations that set out rules of conduct on how employees should use the organisation's ICT facilities (internet, laptops, e-mail, etc.).	BIV Standard	2.0
	5.10.1	The ICT regulations are accessible to every employee.	BIV Standard	2.0
	5.10.2	Employees are familiar with the existence of (the rules of conduct of) the ICT regulations.	BIV Standard	2.0
	5.10.3	External employees have agreed to the applicable rules of conduct through the contract.	BIV Standard	2.0
Return of assets	5.11	Operating resources provided by SURF to perform tasks are handed in when those tasks cease.	BIV Standard	2.0
Classification of information	5.12	SURF has established an information classification scheme for the BIV (Availability, Integrity, Confidentiality) aspects.	BIV Standard	2.0
	5.12.1	Services determine the required level of protection of their service based on the information classification scheme established by SURF, so that the appropriate BIS security measures can be selected.	BIV Standard	2.0
	5.12.2	The service may be unplanned unavailability for a maximum of 24 hours on an annual basis during regular business hours.	BIV Standard	2.0
	5.12.3	The service may be unavailable during regular business hours for a maximum of about 4 hours unplanned on an annual basis. Sometimes more uptime is required (high+).	B-High	2.0
Labelling of information	5.13	SURF has established a scheme for labelling (the confidentiality) of information.	BIV Standard	2.0
	5.13.1	Services label their information based on the scheme with categories of confidentiality.	BIV Standard	2.0
Transfer of information	5.14	SURF has defined the requirements and conditions under which information may be transferred.	BIV Standard	2.0
	5.14.1	Data in transit is always secured with encryption. For web and mail traffic of sensitive data, the service SURFcerticates or SURFfilesender is used.	BIV Standard	2.0
	5.14.2	The service follows the requirements and conditions for transfer of information as set by SURF.	BIV Standard	2.0
Access security	5.15	SURF has established and implemented procedures for physical and logical access security.	BIV Standard	2.0
Identity management	5.16	Each service manages the entire lifecycle of digital identities.	BIV Standard	2.0
Authentication via organisational identity	5.16.1	The service authenticates end-users of applications that provide access to data through a trusted identity provider. SURF has a clear relationship with individuals who are granted access, for example through contractual agreements. For all users, federated identities are preferably used for authentication on the system.	BIV Standard	2.0
	5.16.2	The service manages user identification and has set up a formal procedure for registering and logging out users for this purpose.	BIV Standard	2.0
	5.16.3	Accounts are assigned and used individually as much as possible. If there is no other way, a group account may be used. This must be justified and recorded by the service owner.	BIV Standard	2.0
Managing authentication information	5.17	A process has been implemented that ensures management of user authentication information. Employees working with this information are instructed on how to do so properly.	BIV Standard	2.0
	5.17.1	SURF makes a password management tool available to employees.	BIV Standard	2.0

5. Organisational	BIS ID	Management measure	GFCF	Version
	5.17.2	The service implements SURF's password policy, with usage rules implemented in such a way that systems enforce them.	BIV Standard	2.0
	5.17.3	Initial and reset passwords are valid for a maximum of 24 hours and the user is required to change them on first use.	BIV Standard	2.0
Access rights	5.18	The service handles access rights to information and assets in the manner prescribed by SURF. This applies to providing, modifying, deleting and assessing those rights.	BIV Standard	2.0
	5.18.1	Persons shall not have access to information systems unless an authorised employee authorises and grants such access.	BIV Standard	2.0
	5.18.2	The application of segregation of duties and allocation of access rights is based on risk assessment.	BIV Standard	2.0
	5.18.3	There is an overview or job profile of who may grant access rights (the 'mandate register').	BIV Standard	2.0
	5.18.4	Previously issued accounts and associated unique identifiers will not be reused....	BIV Standard	2.0
	5.18.5	Access rights are reviewed at least annually.	BIV Standard	2.0
	5.18.6	Deviations with impact are treated as security incidents including notification, follow-up and documentation.	BIV Standard	2.0
	5.18.7	Granted access rights are monitored/reassessed every six months	IV-High	2.0
	5.18.8	SURF grants devices access to the network and services according to the required security level.	BIV Standard	2.0
	5.18.9	Equipment that SURF manages (and has authenticated) can access trusted network zones. Equipment that SURF does not manage (e.g. Bring Your Own Device, BYOD) can only access a network segment with limited (access) rights.	BIV Standard	2.0
Information security in supplier relations	5.19	You ensure adequate management of the information security risks that exist through the use of suppliers for certain products and services.	BIV Standard	2.0
	5.19.1	The service determines how the periodic audit of its suppliers is carried out.	BIV Standard	2.0
Addressing information security in supplier agreements	5.20	With each supplier, you set out in the contract the information security requirements relevant to the supplier relationship.	BIV Standard	2.0
	5.20.1	In procurement processes, the department communicates information security requirements (IIS) to potential suppliers,	BIV Standard	2.0
	5.20.2	In (procurement) contracts where information plays a role, include the security requirements from the request for proposal.	BIV Standard	2.0
	5.20.3	In procurement contracts, you provide performance indicators and associated accountability reports that allow you to monitor the supplier's agreed performance.	BIV Standard	2.0
	5.20.4	In procurement contracts, arrange for regular external audits to check the reliability of the service provided.	BIV Standard	2.0
	5.20.5	When procuring ICT, adhere to standard procurement terms and conditions to ensure confidentiality and/or secrecy.	BIV Standard	2.0
	5.20.6	Before entering into a contract, you have determined, based on a risk assessment, whether the dependency on this supplier is manageable. An integral part of the contract is an elaborated exit strategy.	BIV Standard	2.0
	5.20.7	You enter into a processor agreement with suppliers who process personal data for SURF.	BIV Standard	2.0
	5.20.8	If suppliers need access to SURF's business information, this is done after risk assessment. You make clear agreements about such access and record them.	BIV Standard	2.0

5. Organisational	BIS ID	Management measure	GFCF	Version
Managing information security in the ICT chain	5.21	You have put in place a process by which you identify supply chain risks so that you can manage these risks in the supply chain.	BIV Standard	2.0
	5.21.1	You have insight into your supplier's supply chain. The supplier is transparent about how the agreed/required security requirements are passed on to their suppliers.	BIV Standard	2.0
Monitor, review and manage changes to supplier services	5.22	You check whether the supplier fulfils the agreements on security measures. To this end, you make a structural planning for monitoring, assessing and evaluating these agreements.	BIV Standard	2.0
	5.22.1	At least once a year, monitor the performance of your supplier(s) against predefined performance indicators according to the contract.	BIV Standard	2.0
Information security for using cloud services	5.23	The service follows the SURF-wide agreements for purchasing, using and exiting cloud services. This procedure includes a process for managing and terminating the cloud service. The elaboration is in line with SURF's information security requirements.	BIV Standard	2.0
Planning and preparing the management of information security incidents	5.24	SURF has established and communicated a clear process on how to work around security incidents, including a clear description of roles and responsibilities.	BIV Standard	2.0
Assessing and deciding on information security events	5.25	The SIRT determines when an issue is registered as a security incident.	BIV Standard	2.0
	5.25.1	An incident that (potentially) results in a breach of availability, integrity or confidentiality should be reported to the SIRT as soon as possible (within 24 hours as a target).	BIV Standard	2.0
	5.25.2	The SIRT periodically reports to the CISO team on the status and follow-up of incidents.	BIV Standard	2.0
	5.25.3	The SIRT includes information from the CVD procedure in its incident reporting.	BIV Standard	2.0
	5.25.4	Major security incidents, we report as required to the competent authority.	BIV Standard	2.0
Responding to information security incidents.	5.26	Security incidents are picked up and dealt with according to the agreed procedure.	BIV Standard	
	5.26.1	The SIRT follows up security incidents according to the incident procedure and takes care of any escalation.	BIV Standard	2.0
	5.26.2	SURF has an integrated crisis plan. The service refers to this plan in information security continuity plans (for escalation).	BIV Standard	2.0
	5.26.3	SURF tests annually whether the integrated crisis plan is still valid, up-to-date and usable.	BIV Standard	2.0
Learning from information security incidents	5.27	The knowledge gained from analysing security incidents is used to improve security measures and prevent recurrence.	BIV Standard	2.0
	5.27.1	SURF shares analyses of security incidents with relevant partners to prevent recurrence.	BIV Standard	2.0
Collection of evidence	5.28	SURF has established and implemented procedures for dealing with evidence in security incidents.	BIV Standard	2.0
Information security during disruption	5.29	You have a plan by which you can ensure that there is still an appropriate level of information security during a disruption.	BIV-High	2.0

5. Organisational	BIS ID	Management measure	GFCF	Versio n
ICT readiness for business continuity	5.30	The service sets business continuity (of ICT) objectives. These are necessary for a service to continue operating effectively if an ICT-related incident occurs. Services are thus sufficiently able to respond to situations where business continuity and disaster recovery are key.	BIV Standard	2.0
	5.30.1	The service conducts an inventory to identify business-critical (process) components.	BIV Standard	2.0
	5.30.2	The service periodically tests the continuity plans of non-critical systems.	BIV Standard	2.0
	5.30.3	The service annually tests the contingency plans of business-critical systems.	B-High	2.0
Legal, statutory, regulatory and contractual requirements	5.31	The service provides documentation on relevant requirements from laws and regulations, contracts and statutes, among others, and keeps it up to date.	BIV Standard	2.0
	5.31.1	The service describes the approach taken to meet the relevant legal and regulatory requirements.	BIV Standard	2.0
Intellectual property rights	5.32	You consider and protect intellectual property rights.	BIV Standard	2.0
Protecting registrations	5.33	You protect important information about legal obligations and business transactions ('records') from loss, destruction, falsification, unauthorised access, disclosure, etc.	BIV Standard	2.0
	5.33.1	The service clarifies the retention period for each type of information.	BIV Standard	2.0
Privacy and protection of personal data	5.34	SURF ensures adequate protection of privacy and personal data in accordance with laws and regulations.	BIV Standard	2.0
	5.34.1	SURF has appointed a Data Protection Officer (FG). The FG has sufficient mandate to perform the function adequately.	BIV Standard	2.0
	5.34.2	SURF regularly monitors compliance with privacy and data protection requirements and agreements.	BIV Standard	2.0
	5.34.3	The service ensures that it knows and applies SURF's interpretation of personal data processing requirements.	BIV Standard	2.0
Independent assessment of information security	5.35	SURF's approach around information security management and implementation is assessed through internal and external audits as planned or in the event of significant changes.	BIV Standard	2.0
	5.35.1	SURF adopts an annual audit plan that sets out the choices on what type and in what way audits will be carried out.	BIV Standard	2.0
Compliance with information security policies, rules and standards	5.36	SURF regularly monitors compliance with the information security policy and subject-specific agreements and standards.	BIV Standard	2.0
	5.36.1	The CISO periodically reports on information security to the board and management.	BIV Standard	2.0
	5.36.2	Annually, you check compliance with technical security requirements, for example with a security test, pen test or automated vulnerability scans.	BIV Standard	2.0
Documented operating procedures	5.37	Work instructions are available for working with configurations and information processing facilities (system, infratructure) for tasks that are difficult or infrequent.	BIV Standard	2.0
Company procedures for secure use of IT services	5.37.1	Users can see step-by-step how to use a system safely via a manual. The instruction is clear and concrete and the user can easily see whether it is regulations or a handbook/best practice.	BIV Standard	2.0

6 BIS - People-focused measures

6. People-oriented	BIS ID	Management measure	GFCF	Version
Screening	6.01	Before a new employee takes up employment, SURF carries out a background check on that person. The check is done in line with applicable laws and regulations and is repeated at regular intervals. The severity of the check fits SURF's requirements and the risks associated with the position or assignment.	BIV-Basic	2.0
	6.01.1	HR checks a new employee's identity, relevant diplomas and certificates on appointment.	BIV-Basic	2.0
	6.01.2	SURF asks the employee to present a valid, applicable Certificate of Good Conduct (VOG) upon commencement of employment and records the check.	BIV-Basic	2.0
	6.01.3	In new situations, if someone is used for sensitive high-risk data processing, it will be checked whether a heavier VOG or other screening measures are needed.	IV-High	2.0
Employment contract	6.02	The employment contract specifies the information security responsibilities for employee and organisation. Employees are specifically made aware of these, including when there is a job change.	BIV-Basic	2.0
	6.02.1	Employees are explained where to find the information security agreements and instructions that apply to them. Access to this information is easy.	BIV-Basic	2.0
	6.02.2	SURF provides new employees with the employment conditions regulations as part of the signed employment agreement.	BIV-Basic	2.0
Information security awareness, education and training	6.03	SURF ensures that employees in the field of information security have or receive appropriate, relevant to their function: awareness level education and training regular updates on organisational policies and policies/procedures .	BIV-Basic	2.0
	6.03.1	Employees have a responsibility to protect company information. Everyone knows the rules and obligations regarding information security and any special requirements for specific environments.	BIV-Basic	2.0
	6.03.2	Employees receive in-service training on information security from SURF, e.g. awareness activities, training courses, presentations and campaigns.	BIV-Basic	2.0
	6.03.3	Employees receive an introduction 'information security' as part of onboarding. This is done no later than three months after joining the company.	BIV-Basic	2.0
	6.03.4	For safe working at the workplace, at least the following aspects have been implemented: a. awareness programmes address behavioural aspects of safe mobile working; b. for SURF equipment, users sign a user agreement in which they declare to be aware of the dangers of mobile working and declare to use the equipment safely.	BIV-Basic	2.0
	6.03.5	SURF ensures that employees receive education on working safely online, so that they know the risks of digital working and online behaviour (e.g. clicking on unfamiliar links) and how to deal with them.	BIV-Basic	2.0
	6.03.6	Managers regularly draw employees' attention to the importance of information security and privacy training and actively encourage them to attend it periodically. Managers ensure that their employees are familiar with the ICT Regulations (AUP).	BIV-Basic	2.0

6. People-oriented	BIS ID	Management measure	GFCF	Versio n
	6.03.7	Employees who have access to strictly confidential information receive explicit instruction from their manager on how to handle it, what their responsibility is and that they will be monitored accordingly.	IV-High	2.0
	6.03.8	Directors undertake demonstrable education and training so that they are able to identify cybersecurity risks and assess risk management approaches.	BIV base	2.0
Disciplinary procedure	6.04	SURF has established and communicated a disciplinary procedure. This can be followed if employees knowingly breach information security. Attention is drawn to this in the conditions of employment.	BIV-Basic	2.0
	6.04.1	In other relevant documents besides the ICT Regulations (AUP) and the Code of Conduct, SURF draws employees' attention to possible disciplinary measures.	BIV-Basic	2.0
	6.04.2	Employees whose job or role brings them into contact with sensitive data processing operations are alerted by their manager that the role they perform requires extra care to apply security policies and measures and that disciplinary action is more likely to be taken in case of deliberate breach due to the nature of the processing operations.	IV-High	2.0
Responsibilities after termination or change of employment	6.05	SURF has established a procedure on how responsibilities and rights are transferred or remain in force upon change or termination of employment. Employees receive instructions from SURF on responsibilities around information security that remain in force after job change or termination. This procedure is evaluated annually.	BIV-Basic	2.0
	6.05.1	If your employment changes or ends, apply the procedure established by SURF for transferring responsibilities and rights.	BIV-Basic	2.0
Confidentiality or non-disclosure agreement	6.06	SURF has an established model confidentiality agreement that contains agreements on the protection of information. This is applied and signed by staff and other external parties where relevant.	BIV-Basic	2.0
Working remotely	6.07	SURF takes security measures to protect information accessed and processed outside SURF's physical locations when staff work remotely.	BIV-Basic	2.0
Reporting information security events	6.08	SURF ensures that employees can easily report suspicious events or (possible) incidents.	BIV-Basic	2.0
	6.08.1	Employees know how to deal with security incidents.	BIV-Basic	2.0
	6.08.2	A procedure for Coordinated Vulnerability Disclosure (CVD) has been published and established.	BIV-Basic	2.0
	6.08.3	The service reports security incidents to the SIRT as soon as possible, at least within 24 hours of becoming aware of them.	BIV-Basic	2.0
	6.08.4	The service owner is responsible for resolving security incidents (or having them resolved).	BIV-Basic	2.0

7 BIS - Physical measures

Section	BIS ID	Management measure	GFCF	Version
Physical security areas	7.01	Within SURF, areas have been designated that should be secured with physical access measures because they provide access to information and assets.	BIV-Basis	2.0
Physical access security	7.02	Physical access to secure zones places in buildings with information and assets is protected appropriately for each zone.	BIV-Basis	2.0

Section	BIS ID	Management measure	GFCF	Version
Securing offices, rooms and facilities	7.03	SURF has established and implemented physical access security policies with the aim of protecting staff, facilities, etc. from potential hazards.	BIV-Basis	2.0
	7.03.1	Physical access to areas and rooms at SURF is secured through identification, authentication, and authorisation (IAM). Where necessary, logging of access takes place.	BIV-Basic	2.0
	7.03.2	For access to secure areas, everyone is given an access pass so that legitimate presence can be demonstrated.	BIV-Basic	2.0
	7.03.3	A key plan is in place to manage keys or access passes giving access to secure areas.	BIV-Basic	2.0
Monitoring physical security	7.04	SURF building(s) and site(s) are constantly monitored for unauthorised physical access.	BIV-Basic	2.0
Protect against physical and environmental threats	7.05	ICT infrastructure is appropriately protected against physical threats, such as fire or flooding.	BIV-Basic	2.0
Working in secure areas	7.06	SURF has described and implemented security measures for working in secure areas.	BIV-Basic	2.0
Clear desk and clear screen	7.07	SURF has established and communicated clear rules for working safely in the workplace ('clear desk' and 'clear screen').	BIV-Basic	2.0
	7.07.1	If a device is inactive for a certain time, access is automatically locked. For example, consider screen locking after five minutes of inactivity.	BIV-Basic	2.0
	7.07.2	Taking over a session remotely can only be done via the same secure login procedure used to create the session. A remote session locks automatically after five minutes of inactivity.	BIV-Basic	2.0
	7.07.3	If a physical token (such as a yubikey or chip card) for accessing a system is removed, this automatically locks access to that system.	BIV-Basic	2.0
Equipment placement and protection.	7.08	Equipment is placed in a safe place and protected.	BIV-Basic	2.0
Off-site asset security.	7.09	SURF ensures that ICT resources are protected when they are outside the SURF building/premises. Consider, for example, encryption of the hard disk of laptops and the possibility of erasing information remotely.	BIV-Basic	2.0
Storage media	7.10	You ensure adequate security of removable storage media such as USB sticks, external hard drives, in accordance with the classification of the data stored. This applies to the entire life cycle from commissioning, transport to destruction.	BIV-Basic	2.0
	7.10.1	Keep removable media in stock and removable media with confidential information in a place only accessible to authorised persons.	BIV-Basic	2.0
	7.10.2	You do not use removable media for external exchange of information.	BIV-Basic	2.0
	7.10.3	Printers require authentication for printing information.	BIV-Basic	2.0
	7.10.4	SURF asks for a certificate of destruction if an external party needs to destroy a device or erase the information on removable media.	BIV-Basic	2.0
	7.10.5	Removable media are adequately destroyed, e.g. by burning or shredding.	IV-High	2.0
	7.10.6	If transportation of equipment with information is required, choose a courier or carrier that is sufficiently reliable.	IV-High	2.0
Utilities	7.11	SURF protects information systems from power outages and other disruptions caused by disruptions in utilities.	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Version
Protection of cabling	7.12	Cables in use for transmitting data or supporting information services SURF protects from interception, disruption or damage.	BIV-Basic	2.0
Equipment maintenance	7.13	To ensure continuous availability and integrity of appature, this equipment is maintained as prescribed.	BIV-Basic	2.0
	7.13.1	In the maintenance contract with the equipment supplier, it is agreed that: support will be provided during office hours the response time will be a maximum of 4 hours within office hours	BIV-Basic	2.0
	7.13.2	In the maintenance contract with the equipment supplier, it is agreed: that 24/7 support is provided that the response time is a maximum of 2 hours or replacement components must be on site	B-High	2.0
Safe removal or reuse of equipment	7.14	SURF checks before destruction and/or reuse that components of equipment with storage media have been adequately erased/overwritten to ensure that sensitive data and licensed software cannot be retrieved.	BIV-Basic	2.0

8 BIS - Technical measures

Section	BIS ID	Management measure	GFCF	Version
User endpoint devices	8.01	Business information on end-users' managed devices must be adequately protected.	BIV-Basic	2.0
	8.01.1	Mobile devices (such as a laptop, tablet and smartphone) are set up so that: the device is managed and secured via MDM the device is protected with access security the data on the built-in storage devices is protected with encryption the device is part of patch management and hardening SURF can remotely erase business data from the device (when connection is active) Compliance with the points in paragraphs 1 to 6 is reviewed periodically	BIV-Basic	2.0
Special access rights	8.02	You minimise the allocation and use of special powers/permissions.	BIV-Basic	2.0
Session management for access with special rights	8.02.1	The access of users whose operational and administrative tasks require more permissions in the ICT infrastructure is regulated through a Privileged Access Management (PAM) system with separate accounts so that the intended access is not available as an end user. You check annually whether these issued authorisations are still correct.	BIV-Basic	2.0
	8.02.2	Every quarter, you check whether the powers/permissions issued are still correct.	IV-High	2.0
Limiting access to information	8.03	You ensure restriction of access to systems and information according to access security regulations.	BIV-Basic	2.0
	8.03.1	The service prevents users from accessing data they do not need, for example by separating ("logically" or physically isolating) environments and data.	BIV-Basic	2.0
	8.03.2	Users can only access and process the information they need to perform their tasks. In systems and applications, the principles of 'Least Privilege' and 'Need-to-Know' are used as a starting point.	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Version
Access protection on source code	8.04	You protect read and write access to programme source code, development tools and software libraries appropriately.	BIV-Basic	2.0
	8.04.1	There is protection against unwanted and unauthorised changes to shared open source code.	BIV-Basic	2.0
Secure authentication	8.05	You implement an appropriate form of authentication based on the access management policy. The required form of authentication may be stricter depending on the role (think admins or developers).	BIV-Basic	2.0
	8.05.1	Multifactor authentication is mandatory for access to all systems and applications (cloud/on-premises).	BIV-Basic	2.0
	8.05.2	Access to systems and applications and internal company data is only possible through the internal trusted zone	BIV-Basic	2.0
	8.05.3	You give external suppliers access to the network only when necessary. You record in advance how, for what and for how long the rights are granted, and you log the access.	BIV-Basic	2.0
Capacity management	8.06	You describe the capacity requirements for processing, data storage and file storage and monitor system performance accordingly, so that you can make adjustments if capacity reaches a critical point.	BIV-Basic	2.0
	8.06.1	Measures are in place so that we identify and respond appropriately to possible attacks, such as a DDoS attack.	BIV-Basic	2.0
	8.06.2	ICT resources (network and disk space and CPU capacity) are structurally no more than 90% in use. There is 24/7 monitoring for increases in occasional overruns so that action can be taken if necessary.	B-High	2.0
Protection against malware	8.07	You have good malware protection in place, supported by appropriate user awareness.	BIV-Basic	2.0
	8.07.1	You scan all received files for malware before use. You also perform regular malware scans.	BIV-Basic	2.0
	8.07.2	SURF and/or the service scans e-mail messages for spam, viruses and other malicious software. This is done automatically.	BIV-Basic	2.0
	8.07.3	The ability to download files is restricted based on risk and need-of-use. Downloading is monitored so that action can be taken.	BIV-Basic	2.0
	8.07.4	Software that detects malware and associated recovery software are installed and regularly updated.	BIV-Basic	2.0
	8.07.5	The service uses the standards set by SURF against: malware phishing eavesdropping (encryption) modification (SPF, DKIM, DMARC, security settings)	BIV-Basic	2.0
Managing technical vulnerabilities	8.08	You gather information about technical vulnerabilities so that you can take measures to secure systems, data and hardware appropriately.	BIV-Basic	2.0
Registration and resolution of vulnerabilities	8.08.1	You provide automated vulnerability scans on your system. You record the results in an overview including the status of handling. In doing so, you take into account the regulations of the Patch Management procedure.	BIV-Basic	2.0
Automated vulnerability scanning	8.08.2	You perform an automated vulnerability scan on the ICT systems at least once a month. This is done from a separate account that can be distinguished in monitoring.	BIV-Basic	2.0
Automated application vulnerability scanning	8.08.3	You perform an automated vulnerability scan on the application/(web) application at least once a quarter. This is done from a separate account that can be distinguished in monitoring.	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Versio n
	8.08.4	You ensure that you set up patch management for all hardware and software. You do this using the regulations according to the SURF-wide procedure Patch management.	BIV-Basic	2.0
	8.08.5	If you cannot roll out a high-priority security patch on time, you report this to the SIRT. Furthermore, in the meantime, you take measures or a work-around to protect the system/application from abuse of vulnerabilities.	BIV-Basic	2.0
	8.08.6	You apply hardening to systems: only the necessary components run. Superfluous components, services and software are disabled.	BIV-Basic	2.0
Configuration management	8.09	The service documents and establishes configuration settings of hardware, software, services and networks. This also applies to security configurations. You regularly check whether the settings need to be adjusted.	BIV-Basic	2.0
Basic configuration	8.09.1	The service works with a best practice or standard for system security configuration.	BIV-Basic	2.0
	8.09.2	You monitor whether configuration settings are not changed unintentionally or without authorisation. This is preferably done automatically.	BIV-Basic	
Erasing information	8.10	When digital information is no longer needed, it is deleted. You take into account (maximum) retention periods.	BIV-Basic	2.0
Masking information	8.11	You apply data masking where necessary to provide for the principles of least-privilege/need-to-know.	BIV-Basic	2.0
Data leakage prevention	8.12	If you process sensitive information, make sure you have measures in place on the systems, networks and devices used that prevent data leaks through detection.	BIV-Basic	2.0
Backup of information	8.13	The service regularly backs up and tests information, software and images according to the agreed procedure for backups.	BIV-Basic	2.0
	8.13.1	A procedure for backup and recovery (restore) has been established in which you describe the requirements for storing, protecting and testing the backups.	BIV-Basic	2.0
	8.13.2	You test restoring data from backups at least annually, and you test it anyway after a major change to ensure that your backup is reliable in an emergency.	BIV-Basic	2.0
	8.13.3	To avoid damaging the backup during a disaster, at least one copy of the backup should be kept in another location (off-site).	BIV-Basic	2.0
	8.13.4	You have done a risk assessment and determined based on that: what is the maximum allowable data loss what is the maximum recovery time after an incident.	BIV-Basic	2.0
	8.13.5	The maximum allowable data loss after an incident is one hour.	B-High	2.0
Redundancy of information processing facilities	8.14	To meet availability requirements, information processing facilities must have sufficient redundancy.	BIV-Basic	2.0
	8.14.1	The maximum recovery time after an incident, disaster or information processing facility failure is 2 hours (within regular business hours).	B-High	2.0
Logging	8.15	You provide log files that record and log activities, exceptions, errors and other relevant events. The log files are protected from modification or deletion and their contents are analysed regularly.	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Version
	8.15.1	All types of processing - reading, writing, updating, deleting, exporting - of data in systems and applications are logged.	BIV-Basic	2.0
	8.15.2	At a minimum, a log line contains the event: the information necessary to trace the incident back to a natural person with a high degree of certainty; the device used; the result of the operation (e.g. read, write, modify and delete); the date and time of the event.	BIV-Basic	2.0
	8.15.3	You prevent log lines from containing information that could compromise security (such as a plaintext password).	BIV-Basic	2.0
	8.15.4	You forward all authentication logs to the IS/SecOps central logging server. You sample network flow information and send it to a central logging server.	BIV-Basic	2.0
	8.15.5	You provide an up-to-date overall view of the various log files with their storage location.	BIV-Basic	2.0
	8.15.6	Keep log files for at least six months. Within that period, the availability of log information remains guaranteed for possible log analysis. Access to log files is also logged.	BIV-Basic	2.0
	8.15.7	There is an (independent) internal audit procedure that tests semi-annually whether log files are unchanged.	IV-High	2.0
	8.15.8	Modification, deletion or attempted deletion of log data shall be reported as soon as possible as a security incident to the SIRT.	IV-High	2.0
	8.15.9	All actions of system admins are logged.	IV-High	2.0
Monitoring activities	8.16	SURF monitors networks, systems and applications for anomalous behaviour, enabling timely response to alerts. Measures are in place to evaluate potential incidents.	BIV-Basic	2.0
Account monitoring	8.16.1	Monthly report/register for the active accounts: the number of exclusions the account status (with, where relevant, the account end date and/or account closure date)	BIV-Basic	2.0
	8.16.2	You implement an automated log file monitoring system that notifies you when it detects irregularities or potential risks.	IV-High	2.0
Detection and prevention of data exfiltration	8.16.3	To limit unwanted copying and downloading of data, the service dectects large spikes in network usage/bandwidth. Administrators and/or users receive notification/a warning when large amounts of information are downloaded.	IV-High	2.0
Session and identity monitoring	8.16.4	Through session and identity monitoring (based on context and behaviour) detect or prevent unauthorised user activities	IV-High	2.0
Network intrusion detection and prevention systems	8.16.5	We know what we consider to be normal network and application traffic as a baseline. This allows us to detect and block deviations from this baseline. Based on this baseline, critical ICT services are monitored with network intrusion detection and prevention systems.	IV-High	2.0
Clock synchronisation	8.17	You ensure that the system clocks of information processing systems are synchronised with a SURF-approved time source.	BIV-Basic	2.0
	8.17.1	The system contains the correct time, time zone (local time zone) and date.	BIV-Basic	2.0
Use of special system tools	8.18	Users seek approval for deploying special system tools that can limit or bypass security measures.	BIV-Basic	2.0
	8.18.1	The service logs the use of special system tools.	BIV-Basic	2.0
Installing software on operational systems	8.19	To safely install software on devices and systems, the team drafts regulations that are followed.	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Versio n
	8.19.1	Users can install software on their work environment. IS monitors the work environment, installed software and suspicious behaviour.	BIV-Basic	2.0
Network security	8.20	SURF ensures protection of information in systems and applications by securing and managing networks and network devices.	BIV-Basic	2.0
Network access control	8.20.1	A user is only granted access to the network on the basis of appropriate identification and authentication. Unidentified users are not given access to the network (at most to the guest network).	BIV-Basic	2.0
Security of network services	8.21	SURF has determined the service level and security measures required for all network services. This is monitored.	BIV-Basic	2.0
	8.21.1	SURF monitors and analyses incoming and outgoing data traffic to detect malicious elements. This is done with facilities such as the National Detection Network, which is deployed on the basis of a risk assessment. This is done based on the nature of the data and information systems to be protected.	BIV-Basic	2.0
	8.21.2	SURF filters incoming and outgoing network traffic, with deployment being determined on the basis of a risk assessment. This is done according to the nature of the data and information systems to be protected.	BIV-Basic	2.0
	8.21.3	Users and devices may only connect to the corporate network (wired and wireless) after authentication/approval.	BIV-Basic	2.0
	8.21.4	To access the internal network from a remote location, we use a VPN server with multi-factor authentication (MFA).	BIV-Basic	2.0
	8.21.5	Connections (wired and wireless) outside the trusted zone are encrypted.	BIV-Basic	2.0
	8.21.6	New threats detected by the detection solution (see 8.21.1) are reported and handled by the SIRT. This is preferably done through automated mechanisms (threat intelligence sharing) and the applicable legal frameworks are taken into account.	BIV-Basic	2.0
Network segmentation	8.22	In SURF's networks, groups of information services, systems and users are separated from each other.	BIV-Basic	2.0
	8.22.1	When using VLANs, you include all VLANs in an overview. You make it clear how the VLANs are secured (access, separation, links).	BIV-Basic	2.0
	8.22.2	The security of ICT facilities is based on the formulated security level according to a structured VLAN classification.	BIV-Basic	2.0
Applying web filters	8.23	The organisation applies web filters so that access to certain external websites can be blocked if they potentially expose users to malicious content.	BIV-Basic	2.0
Use of cryptography	8.24	SURF has established basic rules as regulations for effective use of cryptography and management of cryptographic keys. These rules are applied.	BIV-Basic	2.0
	8.24.1	You apply standard strong encryption methods according to appropriate norms and standards, including those of the Standardisation Forum.	BIV-Basic	2.0
	8.24.2	The service lays down the following rules for cryptography for its own service: when and what you use encryption for; who is responsible for implementation; who is responsible for key management; which standards you use as a basis for encryption and how the standards of the Standardisation Forum are applied; how you determine the level of protection;	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Versio n
		for communication between organisations, you make mutual agreements.		
	8.24.3	You use a SURF-approved CA (certificate-authority), preferably SURF Certificates.	BIV-Basic	2.0
	8.24.4	To manage cryptographic keys, use the principles of ISO 11770 (part 3). This standard deals specifically with security techniques for information security.	BIV-Basic	2.0
Securing during the development cycle	8.25	The team applies predetermined rules for the safe development of software and systems.	BIV-Basic	2.0
	8.25.1	When developing web applications, you take appropriate measures for security, using the OWASP Secure Development as a starting point.	BIV-Basic	2.0
	8.25.2	Testing and development of software and systems is carried out on the basis of the OTAP methodology.	BIV-Basic	2.0
Application security requirements	8.26	Before developing or buying applications, you draw up requirements for information security. You record these requirements (with the service owner or in the contract with the supplier).	BIV-Basic	2.0
Secure system architecture and technical principles	8.27	Technical principles have been established for designing secure information systems. You regularly check whether the principles are still in line with the current situation.	BIV-Basic	2.0
Server and application infrastructure not shared	8.27.1	IT services run in their own virtual environment, so vulnerabilities in one service do not give access to other services.	BIV-Basic	2.0
Secure encryption	8.28	If you develop software (even if you get someone else to do it for SURF), apply your secure coding principles.	BIV-Basic	2.0
Testing security during development and acceptance	8.29	During software development and testing, you check whether the information security meets the predetermined requirements for that security.	BIV-Basic	2.0
Penetration tests	8.29.1	The service conducts regular pen tests. The frequency required depends on the risk analysis. In any case, a pen test follows in these situations: before commissioning new ICT after major updates after major changes This is done by a trusted party (preferred supplier).	BIV-Basic	2.0
	8.29.2	Before putting a system or application into use, you perform an acceptance test. This test is described in advance and follows a structured test method and is preferably automated.	BIV-Basic	2.0
Outsourced system development	8.30	You provide direction and control of outsourced system or software development. You monitor the activities and assess whether they meet the security requirements set.	BIV-Basic	2.0
	8.30.1	In a tender process, you determine in advance what level of protection is required by means of a classification. That classification makes it clear which mandatory security measures you must request from the supplier.	BIV-Basic	2.0
Separation of development, test and production environments	8.31	The development, test and production environments are separate and secure.	BIV-Basic	2.0
	8.31.1	You may not test in the production environment unless the service owner gives prior written permission.	BIV-Basic	2.0
	8.31.2	You test changes before putting them into production. You may only deviate from this if the service owner gives written permission in advance.	BIV-Basic	2.0

Section	BIS ID	Management measure	GFCF	Versio n
Change management	8.32	You follow a change management procedure when making changes to information processing systems.	BIV-Basic	2.0
Emergency	8.32.1	When a change needs to be implemented immediately, we refer to it as an 'emergency change'. To ensure that this can take place with minimal impact on systems and applications, it must be done in a standardised way. For this purpose, an emergency procedure is established for change management. This procedure is documented, authorised and known.	B-High	2.0
	8.32.2	The change management procedure shall address at least: a. the administration of changes; b. a risk assessment of possible consequences of the changes; c. a change approval procedure.	BIV-Basic	2.0
	8.32.3	A generally accepted framework such as FitSM or ITIL is used for change management.	BIV-Basic	2.0
Test information	8.33	Test data should be appropriately selected, protected and managed.	BIV-Basic	2.0
	8.33.1	You do not use production data in the test environment The test environment is subject to the same security measures as the production environment.	BIV-Basic	2.0
	8.33.2	If the use of production data in a test environment is unavoidable, this data is minimised and preferably anonymised or pseudonymised.	BIV-Basic	2.0
Protection of information systems during audits	8.34	To ensure the smooth running of audits (such as a pen test) and avoid impact on production systems, the investigation is limited to what is necessary. The management responsible makes proper arrangements with the tester in this respect.	BIV-Basic	2.0