NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Bundesamt für Sicherheit in der Informationstechnik (BSI) - Standard 200-1 (v1.0)**
Focal Document URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-bsi-200-1-1-0.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4	Management principles	See fDE for details	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1	The tasks and duties of management	The tasks and duties of the management level with regard to information security can be summarised in the following items:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1.1	Assumption of overall responsibility for information security	The topmost management level of every government agency and company is responsible for the organisation working in a targeted and proper manner and is therefore also responsible for assuring information security both on the inside and out. Depending on the country and type of organisation, this can also be governed by various laws. The management level, but also every individual manager, must clearly demonstrate their commitment to their responsibility and must explain the importance of information security to all employees.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
4.1.1	Assumption of overall responsibility for information security	The topmost management level of every government agency and company is responsible for the organisation working in a targeted and proper manner and is therefore also responsible for assuring information security both on the inside and out. Depending on the country and type of organisation, this can also be governed by various laws. The management level, but also every individual manager, must clearly demonstrate their commitment to their responsibility and must explain the importance of information security to all employees.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
4.1.2	Initiating, managing, and supervising information security	A strategy for information security and security objectives must be agreed upon and communicated. The security strategy is based on the business objectives of the company or the role of the government agency. • The impact of security risks on the business operation or on the fulfilment of tasks must be investigated. The management level is the instance making the decisions on how to handle risks. The responsibility for information security remains there. However, the operative task “information security” is typically delegated to an information security officer (ISO). • The organisational framework conditions for information security must be created, responsibilities and authorisations must be assigned and communicated. • Sufficient resources must be made available for information security. The security strategy must comply with the resources that are available. • The security strategy must be reviewed and assessed at regular intervals, e.g. the achievement of the objectives can be monitored with the help of key figures. Identified vulnerabilities and errors must be corrected. For this, an “innovative” working atmosphere must be created and the will for constant improvement must be demonstrated within the organisation. • Employees must be motivated regarding security issues and must consider information security an important aspect of their tasks. For this, appropriate training and awareness-raising measures must be offered, among other things.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
4.1.2	Initiating, managing, and supervising information security	A strategy for information security and security objectives must be agreed upon and communicated. The security strategy is based on the business objectives of the company or the role of the government agency. • The impact of security risks on the business operation or on the fulfilment of tasks must be investigated. The management level is the instance making the decisions on how to handle risks. The responsibility for information security remains there. However, the operative task “information security” is typically delegated to an information security officer (ISO). • The organisational framework conditions for information security must be created, responsibilities and authorisations must be assigned and communicated. • Sufficient resources must be made available for information security. The security strategy must comply with the resources that are available. • The security strategy must be reviewed and assessed at regular intervals, e.g. the achievement of the objectives can be monitored with the help of key figures. Identified vulnerabilities and errors must be corrected. For this, an “innovative” working atmosphere must be created and the will for constant improvement must be demonstrated within the organisation. • Employees must be motivated regarding security issues and must consider information security an important aspect of their tasks. For this, appropriate training and awareness-raising measures must be offered, among other things.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
4.1.2	Initiating, managing, and supervising information security	A strategy for information security and security objectives must be agreed upon and communicated. The security strategy is based on the business objectives of the company or the role of the government agency. • The impact of security risks on the business operation or on the fulfilment of tasks must be investigated. The management level is the instance making the decisions on how to handle risks. The responsibility for information security remains there. However, the operative task “information security” is typically delegated to an information security officer (ISO). • The organisational framework conditions for information security must be created, responsibilities and authorisations must be assigned and communicated. • Sufficient resources must be made available for information security. The security strategy must comply with the resources that are available. • The security strategy must be reviewed and assessed at regular intervals, e.g. the achievement of the objectives can be monitored with the help of key figures. Identified vulnerabilities and errors must be corrected. For this, an “innovative” working atmosphere must be created and the will for constant improvement must be demonstrated within the organisation. • Employees must be motivated regarding security issues and must consider information security an important aspect of their tasks. For this, appropriate training and awareness-raising measures must be offered, among other things.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	8	
4.1.2	Initiating, managing, and supervising information security	A strategy for information security and security objectives must be agreed upon and communicated. The security strategy is based on the business objectives of the company or the role of the government agency. • The impact of security risks on the business operation or on the fulfilment of tasks must be investigated. The management level is the instance making the decisions on how to handle risks. The responsibility for information security remains there. However, the operative task “information security” is typically delegated to an information security officer (ISO). • The organisational framework conditions for information security must be created, responsibilities and authorisations must be assigned and communicated. • Sufficient resources must be made available for information security. The security strategy must comply with the resources that are available. • The security strategy must be reviewed and assessed at regular intervals, e.g. the achievement of the objectives can be monitored with the help of key figures. Identified vulnerabilities and errors must be corrected. For this, an “innovative” working atmosphere must be created and the will for constant improvement must be demonstrated within the organisation. • Employees must be motivated regarding security issues and must consider information security an important aspect of their tasks. For this, appropriate training and awareness-raising measures must be offered, among other things.	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	8	
4.1.3	Integration of information security	Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include: • project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned. • incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected. If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
4.1.3	Integration of information security	Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include: • project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned. • incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected. If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.1.3	Integration of information security	Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include: • project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned. • incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected. If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
4.1.3	Integration of information security	Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include: • project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned. • incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected. If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
4.1.3	Integration of information security	Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include: • project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned. • incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected. If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	8	
4.1.3	Integration of information security	Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include: • project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned. • incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected. If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	5	
4.1.4	Setting objectives that can be achieved	Projects frequently fail because the objectives that have been set are unrealistic or too ambitious. This is no different in the field of information security. In order to achieve the reasonable security objective, many small steps and a long-term, continuous process of improvement without high investment costs may, in the beginning, be more efficient than a large-scale project. This way, it may be expedient to initially implement the necessary level of security within selected areas only, and, for instance, using the basic safeguards from IT-Grundschutz regarding the width or the core safeguards ITGrundschutz regarding the depth there. However, using these nuclei as starting points, the security in the organisation must then be increased quickly to the level aimed at.	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	8	
4.1.4	Setting objectives that can be achieved	Projects frequently fail because the objectives that have been set are unrealistic or too ambitious. This is no different in the field of information security. In order to achieve the reasonable security objective, many small steps and a long-term, continuous process of improvement without high investment costs may, in the beginning, be more efficient than a large-scale project. This way, it may be expedient to initially implement the necessary level of security within selected areas only, and, for instance, using the basic safeguards from IT-Grundschutz regarding the width or the core safeguards ITGrundschutz regarding the depth there. However, using these nuclei as starting points, the security in the organisation must then be increased quickly to the level aimed at.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	8	
4.1.4	Setting objectives that can be achieved	Projects frequently fail because the objectives that have been set are unrealistic or too ambitious. This is no different in the field of information security. In order to achieve the reasonable security objective, many small steps and a long-term, continuous process of improvement without high investment costs may, in the beginning, be more efficient than a large-scale project. This way, it may be expedient to initially implement the necessary level of security within selected areas only, and, for instance, using the basic safeguards from IT-Grundschutz regarding the width or the core safeguards ITGrundschutz regarding the depth there. However, using these nuclei as starting points, the security in the organisation must then be increased quickly to the level aimed at.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
4.1.4	Setting objectives that can be achieved	Projects frequently fail because the objectives that have been set are unrealistic or too ambitious. This is no different in the field of information security. In order to achieve the reasonable security objective, many small steps and a long-term, continuous process of improvement without high investment costs may, in the beginning, be more efficient than a large-scale project. This way, it may be expedient to initially implement the necessary level of security within selected areas only, and, for instance, using the basic safeguards from IT-Grundschutz regarding the width or the core safeguards ITGrundschutz regarding the depth there. However, using these nuclei as starting points, the security in the organisation must then be increased quickly to the level aimed at.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
4.1.5	Pondering security costs against benefits	One of the most difficult tasks is to ponder the costs for information security against the benefits and risks. It is very important to initially invest in safeguards that are particularly effective or provide protection against especially high risks. Experience shows that the most effective safeguards are not always the most expensive ones. It is therefore absolutely necessary to understand the dependence of the business processes and tasks on information processing so that appropriate safeguards can be selected. At this point, it should be emphasised that information security is only ever achieved by interaction between technical and organisational safeguards. The investments in technology can be read off the budget directly. In order to justify these costs, the security products must be deployed in such a manner that they are of maximum benefit. The products must therefore have been selected for the purpose that they should serve and must be operated in the appropriate manner, i.e. they must be integrated in the holistic security concept and employees must be trained in how to use them. Technical solutions can frequently be replaced by organisational security safeguards. However, experience has shown that it is more difficult to ensure that organisational safeguards are implemented consistently. Furthermore, doing so requires more personnel and thus also places a burden on the resources.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
4.1.6	Role model function	The management level must assume a role model function also when it comes to information security. Among other things, this includes that the management level takes into account all specified security rules, participates in training measures, and supports other managers regarding the execution of their role model function.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.1.6	Role model function	The management level must assume a role model function also when it comes to information security. Among other things, this includes that the management level takes into account all specified security rules, participates in training measures, and supports other managers regarding the execution of their role model function.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
4.1.6	Role model function	The management level must assume a role model function also when it comes to information security. Among other things, this includes that the management level takes into account all specified security rules, participates in training measures, and supports other managers regarding the execution of their role model function.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
4.2	Communication and knowledge	Communication is an important cornerstone regarding the achievement of the set security objectives in all phases of the security process. Misunderstandings and lack of knowledge are the most common causes for security issues. A smooth flow of information regarding security incidents and security safeguards must therefore be assured on all levels and in all departments of an organisation. NOTE: See FDE for additional context	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
4.2	Communication and knowledge	Communication is an important cornerstone regarding the achievement of the set security objectives in all phases of the security process. Misunderstandings and lack of knowledge are the most common causes for security issues. A smooth flow of information regarding security incidents and security safeguards must therefore be assured on all levels and in all departments of an organisation. NOTE: See FDE for additional context	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
4.2	Communication and knowledge	Communication is an important cornerstone regarding the achievement of the set security objectives in all phases of the security process. Misunderstandings and lack of knowledge are the most common causes for security issues. A smooth flow of information regarding security incidents and security safeguards must therefore be assured on all levels and in all departments of an organisation. NOTE: See FDE for additional context	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
4.3	Performance review within the security process	The management level must regularly check the performance and assess the security process (management assessment). If required (e.g. if a number of security incidents occur or there are significant changes to the framework conditions), corresponding audits and assessments must be performed between the regular dates. All results and decisions must be documented in a comprehensible manner [DOC]. The following questions, among other things, should be addressed during the discussion: • Have framework conditions changed resulting in the need to change the approach regarding information security? • Are the security objectives still appropriate? • Is the information security policy still up-to-date? In this, the focus of the performance review regarding the security process is not on auditing individual security safeguards or organisational regulations, but on assessing the situation as a whole. For example, the secure operation of an Internet portal might turn out to be too expensive for a small company. The management level could then, as an alternative, charge a service provider with the administration of the portal. In this situation, it is useful to examine how the security concept and the security organisation have performed to date. In chapter 8 Security concept, various activities are described for reviewing the performance of individual security safeguards. The results gathered there should be taken into account when reviewing the performance of the security strategy. If, for example, it turns out that the security safeguards are ineffective or decidedly expensive, this might give reason to reconsider and adapt the entire security strategy. The following questions should be addressed: • Is the security strategy still appropriate? • Is the security concept appropriate for achieving the set objectives? Are, for instance, the legal requirements fulfilled? • Is the security organisation appropriate for achieving the objectives? Should its position within in the organisation be strengthened or should it be integrated more in the internal processes? • Is there an appropriate relation between the effort – i.e. costs, personnel, materials – required to achieve the security objectives and the business objectives and the role of the organisation?	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
4.3	Performance review within the security process	The management level must regularly check the performance and assess the security process (management assessment). If required (e.g. if a number of security incidents occur or there are significant changes to the framework conditions), corresponding audits and assessments must be performed between the regular dates. All results and decisions must be documented in a comprehensible manner [DOC]. The following questions, among other things, should be addressed during the discussion: • Have framework conditions changed resulting in the need to change the approach regarding information security? • Are the security objectives still appropriate? • Is the information security policy still up-to-date? In this, the focus of the performance review regarding the security process is not on auditing individual security safeguards or organisational regulations, but on assessing the situation as a whole. For example, the secure operation of an Internet portal might turn out to be too expensive for a small company. The management level could then, as an alternative, charge a service provider with the administration of the portal. In this situation, it is useful to examine how the security concept and the security organisation have performed to date. In chapter 8 Security concept, various activities are described for reviewing the performance of individual security safeguards. The results gathered there should be taken into account when reviewing the performance of the security strategy. If, for example, it turns out that the security safeguards are ineffective or decidedly expensive, this might give reason to reconsider and adapt the entire security strategy. The following questions should be addressed: • Is the security strategy still appropriate? • Is the security concept appropriate for achieving the set objectives? Are, for instance, the legal requirements fulfilled? • Is the security organisation appropriate for achieving the objectives? Should its position within in the organisation be strengthened or should it be integrated more in the internal processes? • Is there an appropriate relation between the effort – i.e. costs, personnel, materials – required to achieve the security objectives and the business objectives and the role of the organisation?	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
4.3	Performance review within the security process	The management level must regularly check the performance and assess the security process (management assessment). If required (e.g. if a number of security incidents occur or there are significant changes to the framework conditions), corresponding audits and assessments must be performed between the regular dates. All results and decisions must be documented in a comprehensible manner [DOC]. The following questions, among other things, should be addressed during the discussion: • Have framework conditions changed resulting in the need to change the approach regarding information security? • Are the security objectives still appropriate? • Is the information security policy still up-to-date? In this, the focus of the performance review regarding the security process is not on auditing individual security safeguards or organisational regulations, but on assessing the situation as a whole. For example, the secure operation of an Internet portal might turn out to be too expensive for a small company. The management level could then, as an alternative, charge a service provider with the administration of the portal. In this situation, it is useful to examine how the security concept and the security organisation have performed to date. In chapter 8 Security concept, various activities are described for reviewing the performance of individual security safeguards. The results gathered there should be taken into account when reviewing the performance of the security strategy. If, for example, it turns out that the security safeguards are ineffective or decidedly expensive, this might give reason to reconsider and adapt the entire security strategy. The following questions should be addressed: • Is the security strategy still appropriate? • Is the security concept appropriate for achieving the set objectives? Are, for instance, the legal requirements fulfilled? • Is the security organisation appropriate for achieving the objectives? Should its position within in the organisation be strengthened or should it be integrated more in the internal processes? • Is there an appropriate relation between the effort – i.e. costs, personnel, materials – required to achieve the security objectives and the business objectives and the role of the organisation?	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	8	
4.4	Continuous improvement of the security process	The results of the performance review must be used consistently to make appropriate corrections. This might mean that the security objectives, the security strategy, or the security concept must be changed and the security organisation must be adapted to the requirements. It may make sense to subject the business processes and the IT environment to fundamental changes or to discontinue or outsource business processes if, for instance, their secure operation cannot be guaranteed using the available resources. If major changes are required and more comprehensive improvements must be implemented, this will result in a return to the planning phase, thus completing the management cycle.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
4.4	Continuous improvement of the security process	The results of the performance review must be used consistently to make appropriate corrections. This might mean that the security objectives, the security strategy, or the security concept must be changed and the security organisation must be adapted to the requirements. It may make sense to subject the business processes and the IT environment to fundamental changes or to discontinue or outsource business processes if, for instance, their secure operation cannot be guaranteed using the available resources. If major changes are required and more comprehensive improvements must be implemented, this will result in a return to the planning phase, thus completing the management cycle.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5	Resources for information security	Maintaining a particular level of security always requires financial, personnel, and time-related resources that must be made available in sufficient quantities by the management level. If set objectives cannot be achieved due to a lack of resources, it is not the fault of the persons responsible for the implementation, but rather the fault of the superiors who have set unrealistic objectives or have not provided the necessary resources. In order to fulfil the set objectives, it is important that an initial costbenefit estimation is performed already when the objectives are defined. In the course of the security process, this aspect should continue to play a decisive role so that, on the one hand, resources are not wasted, and, on the other, the investments necessary for achieving an appropriate level of security are guaranteed. Frequently, only technical solutions are associated with IT security. However, this is too shortsighted. This is another reason for better using the term information security instead of IT security. First and foremost, it is important to emphasise that investing in human resources is often more effective than investing in security technology. Technology alone does not solve any problems; it must always be integrated in the organisational framework conditions. The examination of the effectiveness and appropriateness of security safeguards must also be ensured by providing sufficient resources. In practice, the internal security experts frequently do not have enough time to analyse all the influencing factors and framework conditions that are relevant to security (e.g. statutory requirements or technical questions). To some extent, they lack the relevant basic principles. It always makes sense to consult external experts if questions and issues cannot be clarified or solved using one's own means. This must be documented by the internal security experts so that the management level provides the necessary resources. A prerequisite for secure IT operations is a company that functions well. Sufficient resources must therefore be made available for operations. Typical problems encountered during IT operations (scarce resources, overburdened administrators, or an unstructured and poorly maintained IT environment) must generally be solved so that the actual security safeguards can be implemented effectively and efficiently.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
5	Resources for information security	Maintaining a particular level of security always requires financial, personnel, and time-related resources that must be made available in sufficient quantities by the management level. If set objectives cannot be achieved due to a lack of resources, it is not the fault of the persons responsible for the implementation, but rather the fault of the superiors who have set unrealistic objectives or have not provided the necessary resources. In order to fulfil the set objectives, it is important that an initial costbenefit estimation is performed already when the objectives are defined. In the course of the security process, this aspect should continue to play a decisive role so that, on the one hand, resources are not wasted, and, on the other, the investments necessary for achieving an appropriate level of security are guaranteed. Frequently, only technical solutions are associated with IT security. However, this is too shortsighted. This is another reason for better using the term information security instead of IT security. First and foremost, it is important to emphasise that investing in human resources is often more effective than investing in security technology. Technology alone does not solve any problems; it must always be integrated in the organisational framework conditions. The examination of the effectiveness and appropriateness of security safeguards must also be ensured by providing sufficient resources. In practice, the internal security experts frequently do not have enough time to analyse all the influencing factors and framework conditions that are relevant to security (e.g. statutory requirements or technical questions). To some extent, they lack the relevant basic principles. It always makes sense to consult external experts if questions and issues cannot be clarified or solved using one's own means. This must be documented by the internal security experts so that the management level provides the necessary resources. A prerequisite for secure IT operations is a company that functions well. Sufficient resources must therefore be made available for operations. Typical problems encountered during IT operations (scarce resources, overburdened administrators, or an unstructured and poorly maintained IT environment) must generally be solved so that the actual security safeguards can be implemented effectively and efficiently.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	8	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
6	Involving employees in the security process	Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security. If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilitieschange, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards). Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
7	The security process	The management level must define the security objectives knowing all of the relevant framework conditions, the environmental analysis, and based on the business objectives of the company or the role of the government agency and must create the prerequisites for their implementation. The approach is planned with a security strategy to establish a continuous security process. The strategy is implemented with the help of a security concept and a security organisation. In the following, we shall therefore describe the relevant management activities for each lifecycle phase. Due to the broad range and the better overview, the activities relevant to the security concept will be described in a separate chapter.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
7	The security process	The management level must define the security objectives knowing all of the relevant framework conditions, the environmental analysis, and based on the business objectives of the company or the role of the government agency and must create the prerequisites for their implementation. The approach is planned with a security strategy to establish a continuous security process. The strategy is implemented with the help of a security concept and a security organisation. In the following, we shall therefore describe the relevant management activities for each lifecycle phase. Due to the broad range and the better overview, the activities relevant to the security concept will be described in a separate chapter.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
7.1	Planning of the security process	NOTE: See FDE for additional context	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.2	Establishing a security organisation [DOC]	Planning and executing a security process includes defining organisational structures (e.g. departments, groups, centres of expertise) as well as roles and duties. There are different options for organising the structure of information security management. In this, staff arrangements depend on the size of the respective organisation, the existing resources, and the desired level of security. The process of scheduling the resources for supporting information security must be performed such that the agreed level of security can actually be achieved. When defining roles within the framework of information management, the following basic rules must be observed: 1. The overall responsibility for information security remains with the management level. 2. At least one person has to be appointed who promotes and coordinates the information security process, typically as information security officer (ISO). 3. Every employee is equally responsible for their original task and for maintaining information security at his/her workplace and in his/her environment. In order to secure direct access to the organisation's management, the role of the ISO should be organised as an executive department. At management level, the information security role should be clearly assigned to one responsible manager whom the ISO directly reports to.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	8	
7.2	Establishing a security organisation [DOC]	Planning and executing a security process includes defining organisational structures (e.g. departments, groups, centres of expertise) as well as roles and duties. There are different options for organising the structure of information security management. In this, staff arrangements depend on the size of the respective organisation, the existing resources, and the desired level of security. The process of scheduling the resources for supporting information security must be performed such that the agreed level of security can actually be achieved. When defining roles within the framework of information management, the following basic rules must be observed: 1. The overall responsibility for information security remains with the management level. 2. At least one person has to be appointed who promotes and coordinates the information security process, typically as information security officer (ISO). 3. Every employee is equally responsible for their original task and for maintaining information security at his/her workplace and in his/her environment. In order to secure direct access to the organisation's management, the role of the ISO should be organised as an executive department. At management level, the information security role should be clearly assigned to one responsible manager whom the ISO directly reports to.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
7.2	Establishing a security organisation [DOC]	Planning and executing a security process includes defining organisational structures (e.g. departments, groups, centres of expertise) as well as roles and duties. There are different options for organising the structure of information security management. In this, staff arrangements depend on the size of the respective organisation, the existing resources, and the desired level of security. The process of scheduling the resources for supporting information security must be performed such that the agreed level of security can actually be achieved. When defining roles within the framework of information management, the following basic rules must be observed: 1. The overall responsibility for information security remains with the management level. 2. At least one person has to be appointed who promotes and coordinates the information security process, typically as information security officer (ISO). 3. Every employee is equally responsible for their original task and for maintaining information security at his/her workplace and in his/her environment. In order to secure direct access to the organisation's management, the role of the ISO should be organised as an executive department. At management level, the information security role should be clearly assigned to one responsible manager whom the ISO directly reports to.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
7.2	Establishing a security organisation [DOC]	Planning and executing a security process includes defining organisational structures (e.g. departments, groups, centres of expertise) as well as roles and duties. There are different options for organising the structure of information security management. In this, staff arrangements depend on the size of the respective organisation, the existing resources, and the desired level of security. The process of scheduling the resources for supporting information security must be performed such that the agreed level of security can actually be achieved. When defining roles within the framework of information management, the following basic rules must be observed: 1. The overall responsibility for information security remains with the management level. 2. At least one person has to be appointed who promotes and coordinates the information security process, typically as information security officer (ISO). 3. Every employee is equally responsible for their original task and for maintaining information security at his/her workplace and in his/her environment. In order to secure direct access to the organisation's management, the role of the ISO should be organised as an executive department. At management level, the information security role should be clearly assigned to one responsible manager whom the ISO directly reports to.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
7.3	Implementation of the information security policy	A security concept must be drawn up in order to achieve the set security objectives. For greater clarity, a separate chapter has been provided to explain how a security concept can be planned and implemented and how the level of information security can be maintained and improved. The results of the check of the security safeguards are then integrated in the performance review of the security process and are assessed by the management level.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
7.3	Implementation of the information security policy	A security concept must be drawn up in order to achieve the set security objectives. For greater clarity, a separate chapter has been provided to explain how a security concept can be planned and implemented and how the level of information security can be maintained and improved. The results of the check of the security safeguards are then integrated in the performance review of the security process and are assessed by the management level.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
7.4	Maintaining information security	Establishing information security is not a project with a limited time span, but a continuous process. The appropriateness and effectiveness of all elements of the information security management system must be checked at regular intervals. This means that not only individual security safeguards must be checked, but also that the security strategy must be reviewed on a regular basis. The implementation of the security safeguards should be evaluated at regular intervals by means of internal audits. These also serve the purpose of collecting and evaluating the experiences made in dayto-day practice. In addition to audits, it is also necessary to perform drills and awareness-raising measures, since this is the only manner of determining whether all the specified procedures and the conduct in cases of emergency will actually have the desired effect. Findings regarding vulnerabilities and opportunities for improvements must lead to consequences within the security organisation without any exception. Moreover, it is important that future developments both regarding the technology used and the business processes and organisational structures are perceived at an early stage so that potential threats can be identified in time, provisions can be made and security safeguards can be implemented. If significant changes in business processes or organisational structures are looming, the information security management must become involved here. The ISO must become active in a proactive manner: Even if the involvement of the information security management is already planned for in the organisation's regulations, it should not wait to become involved as planned, but should become involved in the relevant processes of its own accord in good time. It is important that none of the audits are carried out by those individuals who were involved in the planning and design of the security objectives, because it is difficult to find one's own mistakes. Depending on the size of the organisation it might be useful to consult external auditors to avoid the situation in which employees become blinkered to their own work. The maintenance of information security is also an important point for small and medium-sized organisations. Although the audits will be less extensive than in large organisations, they must not be omitted in any case. Within the context of the annual management assessment, the topmost management level must also check whether there are new legal stipulations that must be taken into consideration or whether other framework conditions have changed.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
7.4	Maintaining information security	Establishing information security is not a project with a limited time span, but a continuous process. The appropriateness and effectiveness of all elements of the information security management system must be checked at regular intervals. This means that not only individual security safeguards must be checked, but also that the security strategy must be reviewed on a regular basis. The implementation of the security safeguards should be evaluated at regular intervals by means of internal audits. These also serve the purpose of collecting and evaluating the experiences made in dayto-day practice. In addition to audits, it is also necessary to perform drills and awareness-raising measures, since this is the only manner of determining whether all the specified procedures and the conduct in cases of emergency will actually have the desired effect. Findings regarding vulnerabilities and opportunities for improvements must lead to consequences within the security organisation without any exception. Moreover, it is important that future developments both regarding the technology used and the business processes and organisational structures are perceived at an early stage so that potential threats can be identified in time, provisions can be made and security safeguards can be implemented. If significant changes in business processes or organisational structures are looming, the information security management must become involved here. The ISO must become active in a proactive manner: Even if the involvement of the information security management is already planned for in the organisation's regulations, it should not wait to become involved as planned, but should become involved in the relevant processes of its own accord in good time. It is important that none of the audits are carried out by those individuals who were involved in the planning and design of the security objectives, because it is difficult to find one's own mistakes. Depending on the size of the organisation it might be useful to consult external auditors to avoid the situation in which employees become blinkered to their own work. The maintenance of information security is also an important point for small and medium-sized organisations. Although the audits will be less extensive than in large organisations, they must not be omitted in any case. Within the context of the annual management assessment, the topmost management level must also check whether there are new legal stipulations that must be taken into consideration or whether other framework conditions have changed.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7.4	Maintaining information security	Establishing information security is not a project with a limited time span, but a continuous process. The appropriateness and effectiveness of all elements of the information security management system must be checked at regular intervals. This means that not only individual security safeguards must be checked, but also that the security strategy must be reviewed on a regular basis. The implementation of the security safeguards should be evaluated at regular intervals by means of internal audits. These also serve the purpose of collecting and evaluating the experiences made in dayto-day practice. In addition to audits, it is also necessary to perform drills and awareness-raising measures, since this is the only manner of determining whether all the specified procedures and the conduct in cases of emergency will actually have the desired effect. Findings regarding vulnerabilities and opportunities for improvements must lead to consequences within the security organisation without any exception. Moreover, it is important that future developments both regarding the technology used and the business processes and organisational structures are perceived at an early stage so that potential threats can be identified in time, provisions can be made and security safeguards can be implemented. If significant changes in business processes or organisational structures are looming, the information security management must become involved here. The ISO must become active in a proactive manner; Even if the involvement of the information security management is already planned for in the organisation's regulations, it should not wait to become involved as planned, but should become involved in the relevant processes of its own accord in good time. It is important that none of the audits are carried out by those individuals who were involved in the planning and design of the security objectives, because it is difficult to find one's own mistakes. Depending on the size of the organisation it might be useful to consult external auditors to avoid the situation in which employees become blinkered to their own work. The maintenance of information security is also an important point for small and medium-sized organisations. Although the audits will be less extensive than in large organisations, they must not be omitted in any case. Within the context of the annual management assessment, the topmost management level must also check whether there are new legal stipulations that must be taken into consideration or whether other framework conditions have changed.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
7.4	Maintaining information security	Establishing information security is not a project with a limited time span, but a continuous process. The appropriateness and effectiveness of all elements of the information security management system must be checked at regular intervals. This means that not only individual security safeguards must be checked, but also that the security strategy must be reviewed on a regular basis. The implementation of the security safeguards should be evaluated at regular intervals by means of internal audits. These also serve the purpose of collecting and evaluating the experiences made in dayto-day practice. In addition to audits, it is also necessary to perform drills and awareness-raising measures, since this is the only manner of determining whether all the specified procedures and the conduct in cases of emergency will actually have the desired effect. Findings regarding vulnerabilities and opportunities for improvements must lead to consequences within the security organisation without any exception. Moreover, it is important that future developments both regarding the technology used and the business processes and organisational structures are perceived at an early stage so that potential threats can be identified in time, provisions can be made and security safeguards can be implemented. If significant changes in business processes or organisational structures are looming, the information security management must become involved here. The ISO must become active in a proactive manner; Even if the involvement of the information security management is already planned for in the organisation's regulations, it should not wait to become involved as planned, but should become involved in the relevant processes of its own accord in good time. It is important that none of the audits are carried out by those individuals who were involved in the planning and design of the security objectives, because it is difficult to find one's own mistakes. Depending on the size of the organisation it might be useful to consult external auditors to avoid the situation in which employees become blinkered to their own work. The maintenance of information security is also an important point for small and medium-sized organisations. Although the audits will be less extensive than in large organisations, they must not be omitted in any case. Within the context of the annual management assessment, the topmost management level must also check whether there are new legal stipulations that must be taken into consideration or whether other framework conditions have changed.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
7.5	Continuous improvement of information security	Ultimately, the review of the security process is intended to improve the process. The results should therefore be used to assess the effectiveness and efficiency of the selected security strategy and, if necessary, to adapt it. The security strategy must also be reviewed in the case of changes to the security objectives or framework conditions.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
7.5	Continuous improvement of information security	Ultimately, the review of the security process is intended to improve the process. The results should therefore be used to assess the effectiveness and efficiency of the selected security strategy and, if necessary, to adapt it. The security strategy must also be reviewed in the case of changes to the security objectives or framework conditions.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8	
7.5	Continuous improvement of information security	Ultimately, the review of the security process is intended to improve the process. The results should therefore be used to assess the effectiveness and efficiency of the selected security strategy and, if necessary, to adapt it. The security strategy must also be reviewed in the case of changes to the security objectives or framework conditions.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	
8	Security concept	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1	Creating a security concept	NOTE: See FDE for additional context	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
8.2	Implementation of the security concept	NOTE: See FDE for additional context	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
8.3	Performance review of the security concept	NOTE: See FDE for additional context	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
8.4	Continuous improvement of the security concept	Regularly reviewing the performance of the security concept serves for remedying errors and vulnerabilities identified and for optimising security safeguards with regard to their efficiency. One important item involves improving the practical feasibility of technical safeguards and organisational procedures so as to increase the acceptance of the security safeguards. Likewise, the formulation of suitable security safeguards should time and again be considered as to whether it is easily comprehensible and understandable.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
8.4	Continuous improvement of the security concept	Regularly reviewing the performance of the security concept serves for remedying errors and vulnerabilities identified and for optimising security safeguards with regard to their efficiency. One important item involves improving the practical feasibility of technical safeguards and organisational procedures so as to increase the acceptance of the security safeguards. Likewise, the formulation of suitable security safeguards should time and again be considered as to whether it is easily comprehensible and understandable.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8	
8.4	Continuous improvement of the security concept	Regularly reviewing the performance of the security concept serves for remedying errors and vulnerabilities identified and for optimising security safeguards with regard to their efficiency. One important item involves improving the practical feasibility of technical safeguards and organisational procedures so as to increase the acceptance of the security safeguards. Likewise, the formulation of suitable security safeguards should time and again be considered as to whether it is easily comprehensible and understandable.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	
9	Certification of the ISMS	NOTE: See FDE for additional context	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
9	Certification of the ISMS	NOTE: See FDE for additional context	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
10	The ISMS based on BSI IT-Grundschutz	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.1	Introduction	NOTE: See FDE for additional context	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.2	The security process in accordance with IT-Grundschutz	All common methods, best practice examples, and information security management standards barely differ regarding the information they provide with regard to the security process or the duties of the management. The greatest differences lie in the manner in which the security concept is specifically developed, i.e. how the risk assessment is formulated and how the security safeguards are selected. Therefore, the basic approach for developing a security concept in accordance with IT-Grundschutz will be explained here.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.2.1	Integrated risk assessment in IT-Grundschutz	NOTE: See FDE for additional context	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.2.2	Security concept	NOTE: See FDE for additional context	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control