INTERNATIONAL DATA SPACES ASSOCIATION

White Paper | Version 1.0 | February 2020

Criteria Catalogue: **Operational Environments**

- ○ Position Paper of members of the IDS Association
- ○ Position Paper of bodies of the IDS Association
- ○ Position Paper of the IDS Association
- ● White Paper of the IDS Association

Publisher

International Data Spaces Association
Anna-Louisa-Karsch-Str. 2
10178 Berlin
Germany

Editor

Sebastian Steinbuss,
International Data Spaces Association

Authors & Contributors

- Nadja Menz, Fraunhofer FOKUS
- Aleksei Resetko, PrivewaterhouseCooper

Cite as

Steinbuss S., Menz N., Resetko A. (2020): Criteria Catalogue. Operational Environments. International Data Spaces Association. https://doi.org/10.5281/zenodo.5675802

IDS CERTIFICATION

Data security and data sovereignty are the fundamental characteristics of the International Data Space. Participants within the International Data Space must therefore use certified software (e.g., a »Connector«) in order to securely exchange data in a sovereign way. Furthermore, data is only exchanged if the exchange takes place between certified participants that operate trustworthy operational environments.

The International Data Space Certification Scheme is of fundamental importance for making this happen. Certification provides a very high degree of transparency. This transparency is achieved by making the certification requirements available to the public. Evaluating the operational environments regarding their fulfilment of the defined levels of security, including infrastructure reliability and process compliance, can achieve the necessary trust.

This document therefore presents the criteria catalogue for the operational environment of a component.

1 Introduction

The operational environment shall provide a sufficiently high degree of trust and security regarding the integrity, confidentiality and availability of information exchanged in the IDS. Nevertheless, the IDS Certification has a flexible setup and provides different levels of certification according to the intended use cases.

One of the International Data Space goals is to evolve towards a global de-facto standard for cross-industrial and cross-company information exchange. Therefore, a low financial and procedural barrier to join the International Data Space is inevitable. To ensure on the one hand a low entry barrier specifically suitable for SME's and on the other hand a scalable certification to meet high information security requirements, three different security levels, with an increasing extent of the security requirements that need to be fulfilled, were defined:

- The Entry Level covers only the basic security requirements that every participant of the International Data Space needs to fulfil. The entry level therefore serves as a low barrier for companies (especially SMEs) interested in trying out International Data Space participation.
- The Member Level covers additional security requirements, ensuring an advanced level of security. This level is suitable for most core participants.
- The Central Level includes special security requirements that are necessary for International Data Space participants providing key services within the International Data Space.

2 Criteria to Certification Level Mapping

ID	Criteria Title	Entry	Member	Central
Asset Management				
A.8.1	Inventory of assets		x	x
A.8.2	Ownership of assets		x	x
A.8.3	Acceptable use of assets		x	x
A.8.4	Return of assets	x	x	x
A.8.5	Classification of information	x	x	x
A.8.6	Labelling of information	x	x	x
A.8.7	Handling of assets			x
A.8.8	Management of removable media			x
A.8.9	Disposal of media	x	x	x
A.8.10	Physical media transfer			x
Business continuity management				
A.17.1	Planning business continuity			x
A.17.2	Verification, updating and testing of the business continuity			x
A.17.3	Supply of the computing centres			x
A.17.4	Planning information security continuity			x
A.17.5	Implementing information security continuity			x
A.17.6	Verify, review and evaluate information security continuity			x
A.17.7	Availability of information processing facilities			x
Communication security				
A.13.1	Technical safeguards	x	x	x
A.13.2	Monitoring of connections	x	x	x
A.13.3	Cross-network access			x
A.13.4	Confidentiality agreement			x
A.13.5	Network controls	x	x	x
A.13.6	Security of network services			x
A.13.7	Segregation in networks			x
A.13.8	Information transfer policies and procedures			x
A.13.9	Agreements on information transfer			x
A.13.10	Electronic messaging			x
A.13.11	Confidentiality or non-disclosure agreements			x
Compliance and data protection				
A.18.1	Identification of applicable legal, contractual and data protection requirements	x	x	x
A.18.2	Planning independent, external audits		x	x
A.18.3	Carrying out independent, external audits		x	x
A.18.4	Identification of applicable legislation and contractual requirements	x	x	x
A.18.5	Intellectual property rights	x	x	x
A.18.6	Protection of records	x	x	x
A.18.7	Privacy and protection of personally identifiable information	x	x	x
Control and monitoring of service providers and suppliers				
A.15.1	Policies for the handling of and security requirements for service providers and suppliers of the organization		x	x
A.15.2	Monitoring of the rendering of services and security requirements for service providers and suppliers of the organization		x	x

ID	Criteria Title	Entry	Member	Central
A.15.3	Information security policy for supplier relationships		x	x
A.15.4	Addressing security within supplier agreements			x
A.15.5	Information and communication technology supply chain			x
A.15.6	Monitoring and review of supplier services		x	x
A.15.7	Managing changes to supplier services			x
Cryptography and key management				
A.10.1	Policy for the use of encryption procedures and key management			x
A.10.2	Policy on the use of cryptographic controls			x
A.10.3	Key management			x
Identity and access management				
A.9.1	Policy for system and data access authorisations		x	x
A.9.2	Administrator authorisations			x
A.9.3	Access to networks and network services	x	x	x
A.9.4	User registration and de-registration		x	x
A.9.5	User access provisioning		x	x
A.9.6	Management of privileged access rights	x	x	x
A.9.7	Management of secret authentication information of users		x	x
A.9.8	Review of user access rights		x	x
A.9.9	Removal or adjustment of access rights	x	x	x
A.9.10	Use of secret authentication information	x	x	x
A.9.11	Information access restriction	x	x	x
A.9.12	Secure log-on procedures	x	x	x
A.9.13	Password management system	x	x	x
A.9.14	Use of privileged utility programs		x	x
A.9.15	Access control to program source code		x	x
Organisation of information security				
A.6.1	Strategic targets regarding information security and responsibility of the top management		x	x
A.6.2	Authorities and responsibilities in the framework of information security		x	x
A.6.3	Separation of functions		x	x
A.6.4	Identification, analysis, assessment and handling of risks	x	x	x
A.6.5	Contact with authorities		x	x
A.6.6	Contact with special interest groups		x	x
A.6.7	Information security in project management		x	x
Personnel				
A.7.1	Security check of the background information			x
A.7.2	Employment agreements	x	x	x
A.7.3	Screening			x
A.7.4	Terms and conditions of employment	x	x	x
A.7.5	Management responsibilities		x	x
A.7.6	Information security awareness, education and training	x	x	x
A.7.7	Disciplinary process		x	x
A.7.8	Termination or change of employment responsibilities	x	x	x
Physical security				
A.11.1	Perimeter protection	x	x	x
A.11.2	Protection against interruptions caused by power failures and other such risks		x	x

ID	Criteria Title	Entry	Member	Central
A.11.3	Physical security perimeter	x	x	x
A.11.4	Physical entry controls	x	x	x
A.11.5	Securing offices, rooms and facilities	x	x	x
A.11.6	Protecting against external and environmental threats			x
A.11.7	Equipment siting and protection	x	x	x
A.11.8	Supporting utilities			x
A.11.9	Cabling security			x
A.11.10	Security of equipment and assets off-premises	x	x	x
A.11.11	Secure disposal or re-use of equipment		x	x
A.11.12	Unattended user equipment	x	x	x
Procurement, development and maintenance of information systems				
A.14.1	Policies for changes to information systems		x	x
A.14.2	Risk assessment of changes			x
A.14.3	Information security requirements analysis and specification			x
A.14.4	Securing application services on public networks			x
A.14.5	Protecting application services transactions			x
A.14.6	Secure development policy			x
A.14.7	System change control procedures			x
A.14.8	Technical review of applications after operating platform changes			x
A.14.9	Restrictions on changes to software packages			x
A.14.10	Secure system engineering principles			x
A.14.11	Secure development environment			x
A.14.12	Outsourced development			x
A.14.13	System security testing			x
A.14.14	System acceptance testing			x
A.14.15	Protection of test data			x
Safeguards for regular operations				
A.12.1	Capacity management – planning	x	x	x
A.12.2	Capacity management – monitoring		x	x
A.12.3	Protection against malware	x	x	x
A.12.4	Data backup and restoration – concept	x	x	x
A.12.5	Logging and monitoring – concept		x	x
A.12.6	Handling of vulnerabilities, malfunctions and errors – concept	x	x	x
A.12.7	Handling of vulnerabilities, malfunctions and errors – penetration tests	x	x	x
A.12.8	Documented operating procedures			x
A.12.9	Change management		x	x
A.12.10	Capacity management		x	x
A.12.11	Separation of development, testing and operational environments			x
A.12.12	Controls against malware	x	x	x
A.12.13	Information backup		x	x
A.12.14	Event logging		x	x
A.12.15	Protection of log information		x	x
A.12.16	Administrator and operator logs			x
A.12.17	Clock synchronisation			x
A.12.18	Installation of software on operational systems		x	x
A.12.19	Management of technical vulnerabilities		x	x
A.12.20	Restrictions on software installation		x	x

ID	Criteria Title	Entry	Member	Central
A.12.21	Information systems audit controls			x
Security check and verification				
A.18.8	Independent review of information security	x	x	x
A.18.9	Compliance with security policies and standards		x	x
A.18.10	Technical compliance review		x	x
Security Incident Management				
A.16.1	Responsibilities and procedural model	x	x	x
A.16.2	Responsibilities and procedures		x	x
A.16.3	Reporting information security events	x	x	x
A.16.4	Reporting information security weaknesses	x	x	x
A.16.5	Assessment of and decision on information security events		x	x
A.16.6	Response to information security incidents		x	x
A.16.7	Learning from information security incidents		x	x
A.16.8	Collection of evidence		x	x
Security policies and work instructions				
A.5.1	Documentation, communication and provision of policies and instructions	x	x	x
A.5.2	Review and approval of policies and instructions		x	x
A.5.3	Deviations from existing policies and instructions	x	x	x
A.5.4	Policies for information security		x	x
Surrounding parameters				
A.19.1	System description			x
A.19.2	Jurisdiction and data storage, processing and backup locations			x

3 Operational Environment Criteria

3.1 Asset Management

A.8.1: Inventory of assets

- Entry: -
- Member: x
- Central: x

Objective

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

A.8.2: Ownership of assets

- Entry: -
- Member: x
- Central: x

Objective

Assets maintained in the inventory shall be owned.

A.8.3: Acceptable use of assets

- Entry: -
- Member: x
- Central: x

Objective

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

A.8.4: Return of assets

- Entry: x
- Member: x
- Central: x

Objective

All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

A.8.5: Classification of information

- Entry: x
- Member: x
- Central: x

Objective

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

A.8.6: Labelling of information

- Entry: x
- Member: x
- Central: x

Objective

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.8.7: Handling of assets

- Entry: -
- Member: -
- Central: x

Objective

Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.8.8: Management of removable media

- Entry: -
- Member: -
- Central: x

Objective

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

A.8.9: Disposal of media

- Entry: x
- Member: x
- Central: x

Objective

Media shall be disposed of securely when no longer required, using formal procedures.

A.8.10: Physical media transfer

- Entry: -
- Member: -
- Central: x

Objective

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

3.2 Business continuity management

A.17.1: Planning business continuity

- Entry: -
- Member: -
- Central: x

Objective

Strategic establishment and control of a business continuity management (BCM). Planning, implementing and testing business continuity concept as well as incorporating safeguards in order to ensure and maintain operations

Guidance

Based on the business impact analysis, a uniform framework for planning the business continuity and business plan is introduced, documented and applied in order to ensure that all plans (e. g. of the different sites of the organization) are consistent. The planning depends on established standards which is documented comprehensibly in a "statement of applicability".

Business continuity plans and contingency plans take the following aspects into consideration:

• Defined purpose and scope by taking the relevant dependencies into account,

• Accessibility and comprehensibility of the plans for persons who have to take action in line with these plans,

• Ownership by at least one appointed person who is responsible for review, updating and approval,

• Defined communication channels, roles and responsibilities including the notification of the customer,

• Restoration procedures, manual temporary solutions and reference information (by taking the prioritisation into account for the recovery of infrastructure components and services as well as orienting to customers),

• Methods used for the implementation of the plans,

• Continuous improvement process of the plans,

• Interfaces with the security incident management.

A.17.2: Verification, updating and testing of the business continuity

- Entry: -
- Member: -
- Central: x

Objective

Strategic establishment and control of a business continuity management (BCM). Planning, implementing and testing business continuity concept as well as incorporating safeguards in order to ensure and maintain operations

Guidance

The business impact analysis as well as the business continuity plans and contingency plans are

verified, updated and tested at regular intervals (at least once a year) or after essential organisational or environment-related changes. The tests also involve affected customers (tenants) and relevant third parties (e. g. critical suppliers). The tests are documented and results are taken into account for future business continuity safeguards.

A.17.3: Supply of the computing centres

- Entry: -
- Member: -
- Central: x

Objective

Strategic establishment and control of a business continuity management (BCM). Planning, implementing and testing business continuity concept as well as incorporating safeguards in order to ensure and maintain operations

Guidance

The supply of the computing centres (e. g. water, electricity, temperature and moisture control, telecommunications and Internet connection) is secured, monitored and is maintained and tested at regular intervals in order to guarantee continuous effectiveness. It has been designed with automatic fail-safe mechanisms and other redundancies.

Maintenance is performed in compliance with the maintenance intervals and targets recommended by the suppliers as well as only by personnel authorised to do so.

Maintenance protocols including any suspected or detected deficiencies are stored for the duration of the period of time previously agreed upon. After this period of time has expired, the maintenance protocols are destroyed properly and permanently.

A.17.4: Planning information security continuity

- Entry: -
- Member: -
- Central: x

Objective

The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

A.17.5: Implementing information security continuity

- Entry: -
- Member: -
- Central: x

Objective

The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

A.17.6: Verify, review and evaluate information security continuity

- Entry: -
- Member: -
- Central: x

Objective

The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

A.17.7: Availability of information processing facilities

- Entry: -
- Member: -
- Central: x

Objective

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

3.3 Communication security

A.13.1: Technical safeguards

- Entry: x
- Member: x
- Central: x

Objective

Ensuring the protection of information in networks and the corresponding information-processing systems.

Guidance

Based on the results of a risk analysis carried out, the organization has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns (e. g. by MAC spoofing and ARP poisoning attacks) and/or Distributed Denial-of-Service (DDoS) attacks.

A.13.2: Monitoring of connections

- Entry: x
- Member: x
- Central: x

Objective

Ensuring the protection of information in networks and the corresponding information-processing systems.

Guidance

Physical and virtualised network environments are designed and configured in such a way that the connections between trusted and untrusted networks must be restricted and monitored. At defined intervals, it is reviewed whether the use of all services, logs and ports serve a real commercial purpose. In addition, the review also includes the justifications for compensating controls for the use of logs which are considered to be insecure.

A.13.3: Cross-network access

- Entry: -
- Member: -
- Central: x

Objective

Ensuring the protection of information in networks and the corresponding information-processing systems.

Guidance

Each network perimeter is controlled by security gateways. The system access authorisation for cross-network access is based on a security assessment on the basis of the customer requirements.

A.13.4: Confidentiality agreement

- Entry: -
- Member: -
- Central: x

Objective

Ensuring the protection of information in networks and the corresponding information-processing systems.

Guidance

The non-disclosure or confidentiality agreements to be concluded with internal employees, external service providers and suppliers of the organization are based on the requirements of the organization in order to protect confidential data and business details.

The requirements must be identified, documented and reviewed at regular intervals (at least once a year). If the review shows that the requirements have to be adjusted, new non-disclosure or confidentiality agreements are concluded with the internal employees, the external service providers and the suppliers of the organization.

The non-disclosure or confidentiality agreements must be signed by internal employees, external service providers or suppliers of the organization prior to the start of the contract relationship and/or before access to data of the customers is granted.

A.13.5: Network controls

- Entry: x
- Member: x
- Central: x

Objective

Networks shall be managed and controlled to protect information in systems and applications.

A.13.6: Security of network services

- Entry: -
- Member: -
- Central: x

Objective

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

A.13.7: Segregation in networks

- Entry: -
- Member: -
- Central: x

Objective

Groups of information services, users and information systems shall be segregated on networks.

A.13.8: Information transfer policies and procedures

- Entry: -
- Member: -
- Central: x

Objective

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

A.13.9: Agreements on information transfer

- Entry: -
- Member: -
- Central: x

Objective

Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.10: Electronic messaging

- Entry: -
- Member: -
- Central: x

Objective

Information involved in electronic messaging shall be appropriately protected.

A.13.11: Confidentiality or non-disclosure agreements

- Entry: -
- Member: -
- Central: x

Objective

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

3.4 Compliance and data protection

A.18.1: Identification of applicable legal, contractual and data protection requirements

- Entry: x
- Member: x
- Central: x

Objective

Avoiding violations against statutory or contractual duties with respect to information security

Guidance

Legally, regulatory and statutory prescribed requirements, as well as the procedure to comply with these requirements and regulations must be identified, documented and updated regularly by the organization for the its service related to the respective application.

A.18.2: Planning independent, external audits

- Entry: -
- Member: x
- Central: x

Objective

Avoiding violations against statutory or contractual duties with respect to information security

Guidance

Independent audits and assessments of systems or components which contribute to the rendering of the organizations services are planned by the organization in such a way that the following requirements are met:

• There is only read access to software and data.

• Activities which might impair the availability of the systems or components and thus result in a violation of the SLA are carried out outside regular business hours and/or not at load peak times.

• The activities performed are logged and monitored.

A.18.3: Carrying out independent, external audits

- Entry: -
- Member: x
- Central: x

Objective

Avoiding violations against statutory or contractual duties with respect to information security

Guidance

Audits and assessments of processes, IT systems and IT components, provided that they are completely or partially in the organization's area of responsibility and are relevant to the development or operation of the organization's service, are carried out by independent third parties (e. g. certified public auditor) at least once a year in order to identify non-conformities with legally, regulatory and statutory prescribed requirements. The deviations identified are prioritised and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.

A.18.4: Identification of applicable legislation and contractual requirements

- Entry: x
- Member: x
- Central: x

Objective

All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

A.18.5: Intellectual property rights

- Entry: x
- Member: x
- Central: x

Objective

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

A.18.6: Protection of records

- Entry: x

- Member: x
- Central: x

Objective

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

A.18.7: Privacy and protection of personally identifiable information

- Entry: x
- Member: x
- Central: x

Objective

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

3.5 Control and monitoring of service providers and suppliers

A.15.1: Policies for the handling of and security requirements for service providers and suppliers of the organization

- Entry: -
- Member: x
- Central: x

Objective

Ensuring the protection of information which can be accessed by the service providers and/or suppliers of the organization (subcontractors) and monitoring the services and security requirements agreed upon.

Guidance

Policies and instructions for ensuring the protection of information accessed by other third parties (e. g. service providers and/or suppliers of the organization), who contribute significant parts to the development or operation of the organization's service, are documented, communicated and provided according to A.5.1.

The corresponding controls are used to mitigate risks which may result from the potential access to information of the customers. The following aspects are at least to be taken into account for this:

- Definition and description of minimum security requirements with regard to the information processed, which are based on recognised industry standards such as ISO/IEC 27001,
- Legal and regulatory requirements, including data protection, intellectual property right, copyright, handling of meta data as well as a description as to how they are ensured (e. g. site of data processing and liability, see surrounding parameters for transparency),
- Requirements for incident and vulnerability management (especially notifications and collaborations when eliminating malfunctions),
- Disclosure and contractual obligation to the minimum security requirements also to subcontractors if they do not only contribute insignificant parts to the development or operation of the organization's service (e. g. service provider of the computing centre).

The definition of the requirements is integrated into the risk management of the organization.

According to requirement A.6.4, they are checked at regular intervals for their appropriateness.

A.15.2: Monitoring of the rendering of services and security requirements for service providers and suppliers of the organization

- Entry: -
- Member: x
- Central: x

Objective

Ensuring the protection of information which can be accessed by the service providers and/or

suppliers of the organization (subcontractors) and monitoring the services and security requirements agreed upon.

Guidance

Procedures for the regular monitoring and review of agreed services and security requirements of third parties (e.g. service providers and/or suppliers of the organization) who contribute essential parts to the development or operation of the organizations service are established.

The safeguards include at least the following aspects:

- Regular review of service reports (e. g. SLA reports) if they are provided by third parties,
- Review of security-relevant incidents, operational disruptions or failures and interruptions that are related to the service,
- Unscheduled reviews after essential changes to the requirements or environment. The essentiality must be assessed by the organization and documented comprehensibly for audits.

Identified deviations are subjected to a risk analysis according to requirement A.6.4 in order to effectively address them by mitigating safeguards in a timely manner.

A.15.3: Information security policy for supplier relationships

- Entry: -
- Member: x
- Central: x

Objective

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A.15.4: Addressing security within supplier agreements

- Entry: -
- Member: -
- Central: x

Objective

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

A.15.5: Information and communication technology supply chain

- Entry: -
- Member: -
- Central: x

Objective

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A.15.6: Monitoring and review of supplier services

- Entry: -
- Member: x
- Central: x

Objective

Organizations shall regularly monitor, review and audit supplier service delivery

A.15.7: Managing changes to supplier services

- Entry: -
- Member: -
- Central: x

Objective

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account

of the criticality of business information, systems and processes involved and re-assessment of risks.

3.6 Cryptography and key management

A.10.1: Policy for the use of encryption procedures and key management

- Entry: -
- Member: -
- Central: x

Objective

Guaranteeing the appropriate and effective use of cryptography in order to protect the security of information.

Guidance

Policies and instructions with technical and organisational safeguards for encryption procedures and key management are documented, communicated and provided according toA.5.1, in which the following aspects are described:

• Using strong encryption procedures (e. g. AES) and the use of secure network protocols that correspond to the state of the art (e. g. TLS, IPsec, SSH),

• Risk-based regulations for the use of encryption which are compared to schemes for the classification of information and take the communication channel, type, strength and quality of the encryption into account,

• Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys,

• Taking the relevant legal and regulatory obligations and requirements into consideration.

A.10.2: Policy on the use of cryptographic controls

- Entry: -
- Member: -
- Central: x

Objective

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.10.3: Key management

- Entry: -
- Member: -
- Central: x

Objective

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

3.7 Identity and access management

A.9.1: Policy for system and data access authorisations

- Entry: -
- Member: x
- Central: x

Objective

Securing the authorisation and authentication of users of the organization (usually privileged user) and its customer in order to prevent unauthorised access.

Guidance

A role and rights concept based on the business and security requirements of the organization as well as a policy for the management of system and data access authorisations are documented, communicated and provided according to A.5.1 and address the following areas:

• Granting and change (provisioning) of data access authorisations on the basis of the "least-privilege principle") and as is necessary for performing the required tasks ("need-to-know principle"),

• Separation of functions between operative and controlling functions (also referred to as "separation of duties"),

• Separation of functions in the administration of roles, approval and granting of data access authorisations,

• Regular review of granted authorisations,

• Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship,

• Requirements for the approval and documentation of the management of system and data access authorisations.

A.9.2: Administrator authorisations

- Entry: -
- Member: -
- Central: x

Objective

Securing the authorisation and authentication of users of the organization (usually privileged user) and its customer in order to prevent unauthorised access.

Guidance

Granting and change of data access authorisations for internal and external users with administrative or extensive authorisations under the responsibility of the organization comply with the policy or the management of system and data access authorisations (see A.9.2) or a separate policy. The authorisations are granted in a personalised manner and as is necessary for performing the corresponding tasks ("need-to-know principle"). Organisational and/or technical safeguards make sure that granting these authorisations does not result in undesired, critical combinations which violate the principle of the separation of duties (e. g. assigning authorisations for the administration of both the database and the operating system). If this is not possible in certain selected cases, appropriate, compensating controls are established in order to identify any misuse of these authorisations (e. g. logging and monitoring by an SIEM (security information and event management) solution).

A.9.3: Access to networks and network services

- Entry: x
- Member: x
- Central: x

Objective

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

A.9.4: User registration and de-registration

- Entry: -
- Member: x
- Central: x

Objective

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.5: User access provisioning

- Entry: -
- Member: x
- Central: x

Objective

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

A.9.6: Management of privileged access rights

- Entry: x
- Member: x
- Central: x

Objective

The allocation and use of privileged access rights shall be restricted and controlled.

A.9.7: Management of secret authentication information of users

- Entry: -
- Member: x
- Central: x

Objective

The allocation of secret authentication information shall be controlled through a formal management process.

A.9.8: Review of user access rights

- Entry: -
- Member: x
- Central: x

Objective

Asset owners shall review users' access rights at regular intervals.

A.9.9: Removal or adjustment of access rights

- Entry: x
- Member: x
- Central: x

Objective

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9.10: Use of secret authentication information

- Entry: x
- Member: x
- Central: x

Objective

Users shall be required to follow the organization's practices in the use of secret authentication information.

A.9.11: Information access restriction

- Entry: x
- Member: x
- Central: x

Objective

Access to information and application system functions shall be restricted in accordance with the access control policy.

A.9.12: Secure log-on procedures

- Entry: x
- Member: x
- Central: x

Objective

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure

A.9.13: Password management system

- Entry: x
- Member: x
- Central: x

Objective

Password management systems shall be interactive and shall ensure quality passwords.

A.9.14: Use of privileged utility programs

- Entry: -
- Member: x
- Central: x

Objective

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.9.15: Access control to program source code

- Entry: -
- Member: x
- Central: x

Objective

Access to program source code shall be restricted.

3.8 Organisation of information security

A.6.1: Strategic targets regarding information security and responsibility of the top management

- Entry: -
- Member: x
- Central: x

Objective

Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.

Guidance

A security policy with security objectives and strategic parameters for achieving these objectives is documented. The security objectives are derived from the corporate objectives and business processes, relevant laws and regulations as well as the current and future expected threat environment with respect to information security. The strategic targets

constitute essential framework conditions which in further policies and instructions are specified in more detail (see A.5.1).

The security policy is adopted by the top management and communicated to all concerned internal and external parties of the organization (e. g. customers, subcontractors).

A.6.2: Authorities and responsibilities in the framework of information security

- Entry: -
- Member: x
- Central: x

Objective

Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.

Guidance

Responsibilities shared between the organization and its customers, duties to cooperate as well as interfaces for the reporting of security incidents and malfunctions are defined, documented, assigned depending on the respective business model and the contractual duties and communicated to all concerned internal and external parties (e. g. customers, subcontractors of the organization). On the part of the organization, at least the following roles (or comparable equivalents) are described in the security policy or associated policies and corresponding responsibilities assigned:

• Head of IT (CIO)

• IT Security Officer (CISO)

• Representative for the handling of IT security incidents (e. g. Head of CERT)

Changes to the responsibilities and interfaces are communicated internally and externally in such a timely manner that all internal and external parties concerned (e. g. customers) are able to respond to them appropriately with organisational and technical safeguards, before the change becomes effective.

A.6.3: Separation of functions

- Entry: -
- Member: x
- Central: x

Objective

Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.

Guidance

Organisational and technical controls are established in order to ensure the separation of roles and responsibilities (also referred to the "segregation of duties") which are incompatible with respect to the confidentiality, integrity and availability of information of the customers. Controls for the separation of functions are established in the following areas in particular:

• Administration of roles, granting and assignment of access authorisations for users under the responsibility of the organization,

• Development and implementation of changes to the organization's service,

• Maintenance of the physical and logical IT infrastructure relevant to the organization's service (networks, operating systems, databases) and the IT applications if they are in the organization's area of responsibility according to the contractual agreements with the its customers.

Operative and controlling functions should not be performed by one and the same person at the same time to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. If it is not possible to achieve a segregation of duties for organisational or technical reasons, appropriate compensating controls are established in order to prevent or uncover improper activities.

A.6.4: Identification, analysis, assessment and handling of risks

- Entry: x
- Member: x
- Central: x

Objective

Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.

Guidance

The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the organization's service are done at least once a year in order to take internal and external changes and influencing factors into account. The identified risks are comprehensibly documented, assessed and provided with mitigating safeguards according to the safeguards of the risk management.

A.6.5: Contact with authorities

- Entry: -
- Member: x
- Central: x

Objective

Appropriate contacts with relevant authorities shall be maintained.

A.6.6: Contact with special interest groups

- Entry: -
- Member: x
- Central: x

Objective

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.7: Information security in project management

- Entry: -
- Member: x
- Central: x

Objective

Information security shall be addressed in project management, regardless of the type of the project.

3.9 Personnel

A.7.1: Security check of the background information

- Entry: -
- Member: -
- Central: x

Objective

Making sure that employees, service providers and suppliers understand their tasks, that they are aware of their responsibility with regard to information security and that the assets of the organisation are protected if the tasks are modified or completed.

Guidance

The background of all internal and external employees of the organization with access to data of the customers or of the shared IT infrastructure is checked according to the local legislation and regulation by the organization prior to the start of the employment relationship. To the extent permitted by law, the security check includes the following areas:

• Verification of the person by means of the identity card,

• Verification of the curriculum vitae,

• Verification of academic titles and degrees,

• Request of a police clearance certificate for sensitive posts in the company

A.7.2: Employment agreements

- Entry: x
- Member: x
- Central: x

Objective

Making sure that employees, service providers and suppliers understand their tasks, that they are aware of their responsibility with regard to information security and that the assets of the organisation are protected if the tasks are modified or completed.

Guidance

Employment agreements include the obligations of the organization's internal and external employees to comply with relevant laws, regulations and provisions regarding information security. The security policy as well as the policies and instructions for information security derived from this are added to the employment agreement documents. Corresponding compliance is confirmed by the employee by a written statement before they can access the data of the organization's customers or the (shared) IT infrastructure.

A.7.3: Screening

- Entry: -
- Member: -
- Central: x

Objective

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

A.7.4: Terms and conditions of employment

- Entry: x
- Member: x
- Central: x

Objective

The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.

A.7.5: Management responsibilities

- Entry: -
- Member: x
- Central: x

Objective

Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

A.7.6: Information security awareness, education and training

- Entry: x
- Member: x
- Central: x

Objective

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

A.7.7: Disciplinary process

- Entry: -
- Member: x
- Central: x

Objective

There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

A.7.8: Termination or change of employment responsibilities

- Entry: x
- Member: x
- Central: x

Objective

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

3.10 Physical security

A.11.1: Perimeter protection

- Entry: x
- Member: x
- Central: x

Objective

Preventing unauthorised physical site access and protection against theft, damage, loss and failure of operations.

Guidance

The perimeter of premises or buildings which house sensitive or critical information, informationsystems or other network infrastructure are protected in a physically solid manner and by means of appropriate security safeguards that conform to the current state of the art.

A.11.2: Protection against interruptions caused by power failures and other such risks

- Entry: -
- Member: x
- Central: x

Objective

Preventing unauthorised physical site access and protection against theft, damage, loss and failure of operations.

Guidance

Precautions against the failure of supply services such as power, cooling or network connections are taken by means of suitable safeguards and redundancies in coordination with safeguards for operational reliability. Power and telecommunication supply lines which transport data or supply information systems must be protected against interception and damage.

A.11.3: Physical security perimeter

- Entry: x
- Member: x
- Central: x

Objective

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

A.11.4: Physical entry controls

- Entry: x
- Member: x
- Central: x

Objective

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.11.5: Securing offices, rooms and facilities

- Entry: x
- Member: x
- Central: x

Objective

Physical security for offices, rooms and facilities shall be designed and applied.

A.11.6: Protecting against external and environmental threats

- Entry: -
- Member: -
- Central: x

Objective

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A.11.7: Equipment siting and protection

- Entry: x
- Member: x
- Central: x

Objective

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.11.8: Supporting utilities

- Entry: -
- Member: -
- Central: x

Objective

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.11.9: Cabling security

- Entry: -
- Member: -
- Central: x

Objective

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

A.11.10: Security of equipment and assets off-premises

- Entry: x
- Member: x
- Central: x

Objective

Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

A.11.11: Secure disposal or re-use of equipment

- Entry: -
- Member: x
- Central: x

Objective

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

A.11.12: Unattended user equipment

- Entry: x
- Member: x
- Central: x

Objective

Users shall ensure that unattended equipment has appropriate protection.

3.11 Procurement, development and maintenance of information systems

A.14.1: Policies for changes to information systems

- Entry: -
- Member: x
- Central: x

Objective

Complying with the security targets in case of new developments and procurement of information systems as well as changes.

Guidance

Policies and instructions with technical and organisational safeguards for the proper management of changes to information systems for the development or operation of the organization's service, including middleware, databases, operating systems and network components are documented, communicated and provided according to A.5.1. At least the following aspects are to be taken into account in this respect:

• Criteria for the classification and prioritisation of changes and related requirements for the type and scope of tests to be carried out and permits to be obtained,

• Requirements for the notification of affected organization's customers according to the contractual agreements,

• Requirements for the documentation of tests as well as for the application and permit of changes,

• Requirements for the documentation of changes to the system, operating and user documentation.

A.14.2: Risk assessment of changes

- Entry: -
- Member: -
- Central: x

Objective

Complying with the security targets in case of new developments and procurement of information systems as well as changes.

Guidance

The principal of a change performs a risk assessment beforehand. All configuration objects which might be affected by the change are assessed with regard to potential impacts. The result of the risk assessment is documented appropriately and comprehensively.

A.14.3: Information security requirements analysis and specification

- Entry: -
- Member: -
- Central: x

Objective

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

A.14.4: Securing application services on public networks

- Entry: -
- Member: -
- Central: x

Objective

Information involved in application services passing over public

networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification

A.14.5: Protecting application services transactions

- Entry: -
- Member: -
- Central: x

Objective

Information involved in application service transactions shall be

protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A.14.6: Secure development policy

- Entry: -
- Member: -
- Central: x

Objective

Rules for the development of software and systems shall be established and applied to developments within the organization.

A.14.7: System change control procedures

- Entry: -
- Member: -
- Central: x

Objective

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

A.14.8: Technical review of applications after operating platform changes

- Entry: -
- Member: -
- Central: x

Objective

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

A.14.9: Restrictions on changes to software packages

- Entry: -
- Member: -
- Central: x

Objective

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

A.14.10: Secure system engineering principles

- Entry: -
- Member: -
- Central: x

Objective

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

A.14.11: Secure development environment

- Entry: -
- Member: -
- Central: x

Objective

Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

A.14.12: Outsourced development

- Entry: -
- Member: -
- Central: x

Objective

The organization shall supervise and monitor the activity of outsourced system development.

A.14.13: System security testing

- Entry: -
- Member: -
- Central: x

Objective

Testing of security functionality shall be carried out during development.

A.14.14: System acceptance testing

- Entry: -
- Member: -
- Central: x

Objective

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

A.14.15: Protection of test data

- Entry: -
- Member: -
- Central: x

Objective

Test data shall be selected carefully, protected and controlled.

3.12 Safeguards for regular operations

A.12.1: Capacity management – planning

- Entry: x
- Member: x
- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid capacity bottlenecks. The procedures include forecasts of future capacity requirements in order to identify use trends and master system overload risks.

A.12.2: Capacity management – monitoring

- Entry: -
- Member: x
- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of organization's services are defined. Thus, the organization ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.

A.12.3: Protection against malware

- Entry: x
- Member: x
- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

The logical and physical IT systems which the organization uses for the development and rendering of the organization's service as well as the network perimeters which are subject to the organization's area of responsibility are equipped with anti-virus protection and repair programs which allow for a signature- and behaviour-based detection and removal of malware. The programs are updated according to the contractual agreements concluded with the manufacturer(s), but at least once a day.

A.12.4: Data backup and restoration – concept

- Entry: x
- Member: x
- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

Policies and instructions with technical and organisational safeguards in order to avoid losing data are documented, communicated and provided according to A.5.1. They provide reliable procedures for the regular backup (backup as well as snapshots, where applicable) and restoration of data. The scope, frequency and duration of the retention comply with the contractual agreements concluded with the organization's customers as well as the organization's business requirements. Access to the data backed up is limited to authorised personnel. Restoration procedures include control mechanisms that ensure that restorations are carried out only after they have been approved by persons authorised to do so according to the contractual agreements with the organization's customers or the internal policies of the organization.

A.12.5: Logging and monitoring – concept

- Entry: -
- Member: x
- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to A.5.1 in order to log events on all assets which are used for the development or operation of the organization's service and to store them in a central place. The logging includes defined events which may impair the security and availability of the organization's service, including logging the activation, stopping and pausing of different logs. In case of unexpected or unusual events, the logs are checked by authorised personnel due to special events in order to allow for a timely examination of malfunctions and security incidents as well as for the initiation of suitable safeguards.

A.12.6: Handling of vulnerabilities, malfunctions and errors – concept

- Entry: x
- Member: x

- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to A.5.1 in order to ensure the prompt identification and addressing of vulnerabilities over all levels of the organization's service, for which they are responsible. The safeguards include among other things:

• Regular identification and analysis of vulnerabilities,

• Regular follow-up of safeguards in order to address identified safeguards (e. g. installation of security updates according to internal target specifications).

A.12.7: Handling of vulnerabilities, malfunctions and errors – penetration tests

- Entry: x
- Member: x
- Central: x

Objective

Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

Guidance

The organization has penetration tests performed by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to documented test methods and include the infrastructure components defined to be critical to the secure operation of the organization's service, which were identified as such as part of a risk analysis. Type, scope, time/period of time and results are documented comprehensibly for an independent third party. Determinations from the penetration tests are assessed and, in case of medium or high criticality regarding the confidentiality, integrity or availability of the organization's service, followed up and remedied. The assessment of the criticality and the mitigating safeguards for the individual determinations are documented.

A.12.8: Documented operating procedures

- Entry: -
- Member: -
- Central: x

Objective

Operating procedures shall be documented and made available to all users who need them.

A.12.9: Change management

- Entry: -
- Member: x
- Central: x

Objective

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

A.12.10: Capacity management

- Entry: -
- Member: x
- Central: x

Objective

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

A.12.11: Separation of development, testing and operational environments

- Entry: -
- Member: -
- Central: x

Objective

Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

A.12.12: Controls against malware

- Entry: x
- Member: x
- Central: x

Objective

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A.12.13: Information backup

- Entry: -
- Member: x
- Central: x

Objective

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A.12.14: Event logging

- Entry: -
- Member: x
- Central: x

Objective

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.15: Protection of log information

- Entry: -
- Member: x
- Central: x

Objective

Logging facilities and log information shall be protected against tampering and unauthorized access.

A.12.16: Administrator and operator logs

- Entry: -
- Member: -
- Central: x

Objective

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

A.12.17: Clock synchronisation

- Entry: -
- Member: -
- Central: x

Objective

The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

A.12.18: Installation of software on operational systems

- Entry: -
- Member: x
- Central: x

Objective

Procedures shall be implemented to control the installation of software on operational systems.

A.12.19: Management of technical vulnerabilities

- Entry: -
- Member: x
- Central: x

Objective

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A.12.20: Restrictions on software installation

- Entry: -
- Member: x
- Central: x

Objective

Rules governing the installation of software by users shall be established and implemented.

A.12.21: Information systems audit controls

- Entry: -
- Member: -
- Central: x

Objective

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

3.13 Security check and verification

A.18.8: Independent review of information security

- Entry: x
- Member: x
- Central: x

Objective

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

A.18.9: Compliance with security policies and standards

- Entry: -
- Member: x
- Central: x

Objective

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

A.18.10: Technical compliance review

- Entry: -
- Member: x
- Central: x

Objective

Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

3.14 Security Incident Management

A.16.1: Responsibilities and procedural model

- Entry: x
- Member: x
- Central: x

Objective

Ensuring a consistent and consistent approach regarding the monitoring, recording, assessment, communication and escalation of security incidents.

Guidance

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to A.5.1 in order to ensure a fast, effective and proper response to all known security incidents. On the part of the organization, at least roles must be filled, requirements for the classification, prioritisation and escalation of security incidents defined and interfaces with the incident management and the business continuity management created.

In addition to this, the organization has established a "computer emergency response team" (CERT), which contributes to the coordinated solution of specific security incidents. Customers affected by security incidents are informed in a timely manner and appropriate form.

A.16.2: Responsibilities and procedures

- Entry: -
- Member: x
- Central: x

Objective

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.3: Reporting information security events

- Entry: x
- Member: x
- Central: x

Objective

Information security events shall be reported through appropriate management channels as quickly as possible.

A.16.4: Reporting information security weaknesses

- Entry: x
- Member: x
- Central: x

Objective

Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

A.16.5: Assessment of and decision on information security events

- Entry: -
- Member: x
- Central: x

Objective

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

A.16.6: Response to information security incidents

- Entry: -
- Member: x
- Central: x

Objective

Information security incidents shall be responded to in accordance with the documented procedures.

A.16.7: Learning from information security incidents

- Entry: -
- Member: x
- Central: x

Objective

Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

A.16.8: Collection of evidence

- Entry: -
- Member: x
- Central: x

Objective

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

3.15 Security policies and work instructions

A.5.1: Documentation, communication and provision of policies and instructions

- Entry: x
- Member: x
- Central: x

Objective

Providing policies and instructions with respect to the security claim and to support the business requirements.

Guidance

Policies and instructions for information security or related topics derived from the security policy are documented in an uniform structure. They are communicated and made available to all internal and external employees of the organization properly and adequately. Policies are versioned and approved by top management of the organization. The policies and instructions describe at least the following aspects:

• Goals

• Scopes of application

• Roles and responsibilities, including requirements for the qualification of the personnel and the establishment of substitution arrangements,

• Coordination of different company departments,

• Security architecture and safeguards for the protection of data, IT applications and IT infrastructures which are managed by the organization or third parties as well as

• Safeguards for the compliance with legal and regulatory requirements (compliance).

A.5.2: Review and approval of policies and instructions

- Entry: -
- Member: x
- Central: x

Objective

Providing policies and instructions with respect to the security claim and to support the business requirements.

Guidance

The policies and instructions for information security are reviewed with respect to their appropriateness and effectiveness by specialists of the organization who are familiar with the topic at least once a year to ensure their continuing suitability, adequacy and effectiveness. At least the following aspects are taken into account in the review:

• Organisational changes at the organization,

• Current and future expected threat environment regarding information security as well as

• Legal and technical changes in the organization's environment.

Revised policies and instructions are approved by committees or bodies of the organization authorised to do so before they become valid.

A.5.3: Deviations from existing policies and instructions

- Entry: x

- Member: x
- Central: x

Objective

Providing policies and instructions with respect to the security claim and to support the business requirements.

Guidance

Exceptions of policies and instructions for information security are approved by committees or bodies of the organization authorised to do so in a documented form. The appropriateness of approved exceptions and the assessment of the risks resulting from this are reviewed by specialists of the organization who are familiar with the topic against the backdrop of the current and future expected threat environment regarding information security at least once a year.

A.5.4: Policies for information security

- Entry: -
- Member: x
- Central: x

Objective

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

3.16 Surrounding parameters

A.19.1: System description

- Entry: -
- Member: -
- Central: x

Objective

The general organisational and legal framework conditions and targets are described comprehensibly and accurately for a third party expert in order to assess the general suitability of the service for the desired application.

Guidance

In their system description, the organization provides comprehensible and transparent specifications regarding the organization's service, which allow an expert third party to assess the general suitability of the organization's service for the desired application. The system description describes the following aspects:

• Type and scope of the organization's services rendered according to the service level agreement which is typically based on a contract concluded with the its customers,

• Principles, procedures and safeguards for rendering (development and/or operation) the organization's service, including the controls established,

• Description of the infrastructure, network and system components used for the development and operation of the organization's service,

• Handling of significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical IT systems,

• Roles and responsibilities of the organization and the its customer, including the duties to cooperate and corresponding controls at the organization's customer,

• Functions assigned or outsourced to subcontractors.

A.19.2: Jurisdiction and data storage, processing and backup locations

- Entry: -
- Member: -
- Central: x

Objective

The general organisational and legal framework conditions and targets are described comprehensibly and accurately for a third party expert in order to assess the general suitability of the service for the desired application.

Guidance

In service level agreements, their process documentation or comparable documentation, the organization provides comprehensible and transparent specifications regarding its jurisdiction as well as with respect to data storage, processing and backup locations, which allow an expert third party to assess the general suitability of the organization's service for the customer application. This also holds true if data of the organization's customer is processed, stored and backed up by subcontractors of the organization.

Data of the customer shall only be processed, stored and backed up outside the contractually agreed locations only with the prior express written consent of the customer.

4 Summary

For further details, see the spreadsheet Certification Criteria - Participants v1.0.0 in Jive[1].

[1] https://industrialdataspace.jiveon.com/docs/DOC-1799

How To: IDS Certification Process

Participants and core components within the IDS ecosystem shall provide sufficiently high degree of security regarding the integrity and confidentiality of the data being processed in the IDS. Therefore, a certification of participants and core components is mandatory. Involved partners are the applicant, evaluation facility and the certification body.

The certification process is divided into the following three stages:

1 THE APPLICATION STAGE

The main goal of this stage is the successful start of the IDS certification process. It starts with the applicant triggering the certification process. The applicant must contact an approved evaluation facility to carry out the evaluation according to the IDS certification schema. The choice of the evaluation facility lies with applicant. The applicant must provide the necessary evidence for the certification body to confirm the application. If the applicant is accepted, the evaluation procedure will be opened and there will be a Kick-Off with all involved partners.
IDS_Ready evaluators: www.internationaldataspaces.org/the-principles/evaluation-facilities/
Contact email: certiication@internationaldataspaces.org

2 THE EVALUATION STAGE

The main goal of this stage is the evaluation of a participant or IDS core component based on the defined certification criteria. The evaluation facility is responsible for carrying out the detailed technical and / or organizational evaluation work during the certification.
The evaluation facility documents the detailed results in an evaluation report. If deviations have been identified, implementing the corrective actions is the responsibility of the applicant. Afterwards, a re-examination is necessary. The evaluation is monitored by the certification body to ensure the correct implementation and execution of the IDS certification scheme.
Certification Criteria – Participants: industrialdataspace.jiveon.com/docs/DOC-1799
Certification Criteria – Components: industrialdataspace.jiveon.com/docs/DOC-2223

3 THE CERTIFICATION STAGE

The main goal of this stage is the examination of the evaluation report by the certification body as well as the process for issuing the certificate if the result is positive.
The certification body receives the evaluation report from the evaluation facility and is responsible for the final decision about the award or denial of the certificate. If the decision is positive, the applicant will be confirmed as being IDS compliant. The certification body issues the certificate.
Requirements for IDS Evaluation Facilities: industrialdataspace.jiveon.com/docs/DOC-1710

Whitepaper 2018: bit.ly/2lIRo5z
Webinar on YouTube: bit.ly/2kBGAG5

Related Documents

IDS Reference Architecture Model Version 3.0
April 2019

White Paper Certification Version 2.0
April 2019

IDSA Webinar: Trust in the IDS based on the certification of participants and components
January 2019

IDS Certification: Criteria for Participants
(internal)

IDS Certification: Criteria for Core Components
(internal)

IDS Certification: Code of Conduct
(internal)

IDS Certification: Approval Scheme for Evaluation Facilities
(internal)

OUR MEMBERS


Aalto University
ADVANEO
agrarmarkt informatik
Allianz
Atos
Audi
bill-X Collect. Manage. Execute.
Boehringer Ingelheim
Brainport Industries
bdr BUNDESDRUCKEREI
CAICT
SUPERCLUSTER
CDQ SHARING DATA EXCELLENCE
cea
Cefriel POLITECNICO DI MILANO
iti Information Technologies Institute
CHALMERS UNIVERSITY OF TECHNOLOGY
COSMOPlat
Cybus
CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
DAIMLER
DATAHEAD
DATATRONIQ
DB SCHENKER
Deloitte.
Deutsche Bank
DGZfP
DHBW Duale Hochschule Baden-Württemberg Ravensburg
Digital Green
DIMECC
DR. SCHNEIDER UNTERNEHMENSGRUPPE
eccenca command your data!
EcoDataCenter
ELDORADO
ENGIE
ENGINEERING
8760 Fastems
fir an der RWTH Aachen
FIWARE
Leibniz Universität Hannover
Fraunhofer
GateHouse Logistics
EDGE CLOUD
GESIS
Google
HITACHI Inspire the Next
HUAWEI
i2cat
iav
IBM
ILVO Instituut voor Landbouw-, Visserij- en Voedingsonderzoek
imec
Imperial College London
Institut Mines-Télécom
INDUSTRY 2025 INDUSTRIE INDUSTRIA
INNOPAY
innovalia ASSOCIATION
Insight
Irish Manufacturing Research
ITI INVESTIGATE TO INNOVATE
Klarrio
komsa DIE BESSERE VERBINDUNG
LOSEC LEADERS IN SECURITY
Lobster
Logata Digital Solutions
LOGENIOS
minnosphere
msg
nexedi
nicos AG
olmogo data ownership solutions


orbiter

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ

pi-lar GmbH

POLITECNICO
MILANO 1863

pwc

QuinScape

realworldsystems

RI
SE

REWE
GROUP

RITTAL

SALZGITTERAG
Stahl und Technologie

SAP

SCHAEFFLER

SETLOG
The Smart Connective

SICK
Sensor Intelligence.

SIEMENS
Ingenuity for life

Signal
Solutions

SINTEF

SMEV AG
Smart Mobility Evolution

TARC

tecnalia
Inspiring Business

IK4 TEKNIKER


mtc
Manufacturing Technology Centre

thyssenkrupp

TNO innovation for life

TÜV NORD GROUP

TÜV
SÜD

UNIKLINIK
RWTH AACHEN

UNiSCON
Sealed Cloud Technologies

UNITY
CONSULTING & INNOVATION

universität
Witten/Herdecke

University of Amsterdam

UNIVERSITY
OF TWENTE.

vastuu group

VDMA

VOLKSWAGEN
AKTIENGESELLSCHAFT

VTT

WELOTEC
a byte smarter

WeTech
IDS-China

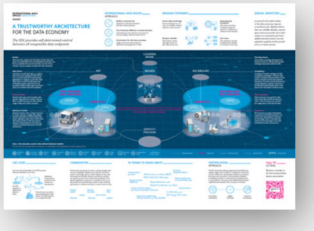
ZVEI:
Die Elektroindustrie

OVERVIEW PUBLICATIONS

Reference Architecture Model

Executive Summary

Image Brochure



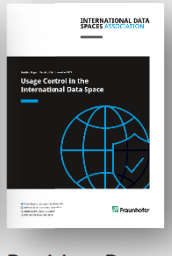
Infographic

Use Case Brochures

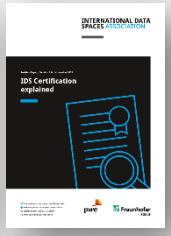
Study on Data Exchange

Position Paper Implementing the European Data Strategy

Position Paper GDPR Requirements and Recommendations



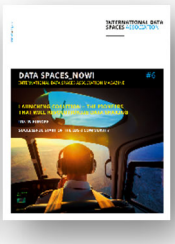
Position Paper Usage Control in the IDS



Position Paper IDS Certification Explained

White Paper Certification

Sharing data while keeping data ownership



Magazine Data Spaces_Now!

For these and further downloads: www.internationaldataspaces.org/info-package

Code available at: https://github.com/industrial-data-space

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association