Statement of Applicability of ISO27001:2013

Version	1.2
Date Approved	6-nov-17
Author	Harmen Thiewes (ISO)

Annex A ref	Control title	Control Description	Applicability	Implemented control	Justification
			A.5 Information security policies		
A.5.1.	**Management direction for information security**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**			
A.5.1.1.	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	**Applicable**	A formal information security policy has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.5.1.2.	Review of the poli- cies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	**Applicable**	All policies and controls and subjected to periodical reviews.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
			A.6 Organization of information security		
A.6.1	**Internal Organization**	**To establish a management framework to initiate and control the implementation and operation of information security within the organization.**			
A.6.1.1.	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	**Applicable**	Security is part of all roles in the organization. All responisiblities have been described in job descriptions and are maintained. Segregation of duties is implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.6.1.2.	Segregation of duties	Conf licting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	**Applicable**	Security is part of all roles in the organization. All responisiblities have been described in job descriptions and are maintained. Segregation of duties is implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.6.1.3.	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	**Applicable**	Is part of security officers role.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.6.1.4.	Contact with special interest groups	Appropriate contacts with special interest groups or other special- ist security forums and professional associations shall be maintained.	**Applicable**	Is part of security officers role.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.6.1.5.	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	**Applicable**	Security by design is integrated into project managment methodology.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.6.2	**Mobile devices and teleworking**	**To ensure the security of teleworking and use of mobile devices.**			
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	**Applicable**	A formal policy has been implemented and is maintained (gouden regels en gedragsregels en Intune).	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	**Applicable**	A formal policy has been implemented and is maintained (gouden regels en gedragsregels en Intune).	Control has been selected after analysis based on risk assessment and the PinkWeb context.
			A.7 Human resource security		
A.7.1	**Prior to employment**	**To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.**			

A.7.1.1.	Screening	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.	Applicable	Screening and background checks are part of the procedures for all personell.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.7.1.2.	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.	Applicable	Responsibilities are part of the 'personeelsgids' which forms an integral part of the employment of an employee.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.7.2	**During employment**	**To ensure that employees and contractors are aware of and fulfil their information security responsibilities.**			
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Applicable	All responisiblities have been described in job descriptions and are maintained. Special proceduers for third parties have been designed and implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contrac- tors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Applicable	Formal awareness campagnes are held and continuously monitored. A formal procedure 'in dienst' is in place and explicitely linked to awareness instruction.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary processin place to take action against employees who have committed aninformation security breach.	Applicable	A formal disciplinary proces has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.7.3	**Termination and change of employment**	**To protect the organization’s interests as part of the process of changing or terminating employment.**			
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, com- municated to the employee or contractor and enforced.	Applicable	Are formal procedure "uit dienst" is in place and explicitely linked to access control policy.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8 Asset management					
A.8.1	**Responsibility for assets**	**To identify organizational assets and define appropriate protection responsibilities.**			
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Applicable	A formal asset managment policy and procedure has been implemented and is maintained.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Applicable	All assets have been asigned owners, with adequate responsibilities and rights.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Applicable	An acceptable use policy has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Applicable	Are formal procedure "uit dienst" is in place and is explicitely linked to asset management.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.2	**Information classification**	**To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.**			
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Applicable	A formal policy and procedure for the guidelines of classification has implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable	A set of procedures for the handling and labelling of all assets has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and imple- mented in accordance with the information classification scheme adopted by the organization.	Applicable	A set of procedures for the handling and labelling of all assets has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.3	**Media handling**	**To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.**			
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Applicable	A formal policy has been implemented and is maintained (gouden regels, gedragsregels, documentclassificatie, operations manual).	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Applicable	A formal policy has been implemented and is maintained (gouden regels, gedragsregels, documentclassificatie, operations manual).	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Applicable	A formal policy has been implemented and is maintained (gouden regels, gedragsregels, documentclassificatie, operations manual).	Control has been selected after analysis based on risk assessment and the PinkWeb context.
			A.9 Access control		
A.9.1	**Business requirements of access control**	**To limit access to information and information processing facilities.**			
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.2	**User access management**	**To ensure authorized user access and to prevent unauthorized access to systems and services.**			
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Applicable	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.9.2.6	Removal or adjustment of access rights	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.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.3	**User responsibilities**	**To make users accountable for safeguarding their authentication information.**			
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.4	**System and application access control**	**To prevent unauthorized access to systems and applications.**			
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	**Applicable**	A formal access control policy and access control list has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
			A.10 Cryptography		
A.10.1	**Cryptographic controls**	**To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.**			
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	**Applicable**	See operations manual. PinkWeb uses SLL and VPN where approriate.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	**Applicable**	See operations manual. PinkWeb uses SLL and VPN where approriate.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
			A.11 Physical and environmental security		
A.11.1	**Secure areas**	**To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.**			
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.1.4	Protecting against external and enviromental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2	**Equipment**	**To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.**			

A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or support- ing information services shall be protected from interception, interference or damage.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.11.2.7	Secure disposal or re- use of equipment	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.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.11.2.9	Clear desk and clear screen policy	A clean desk policy for papers and removable storage media that contain sensitive information and a clear screen policy for information processing facilities shall be adopted.	**Applicable**	Physcial security is devided over two locations: the office and the data centre. Security of both locations is part of the operations manual and stricktly adherred. The datacentre responsiblities have been outsourced and are monitored by PinkWeb to ensure compliance. The datacentre itself is ISO27001 certified.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12 Operations security					
A.12.1	**Operational procedures and responsibilities**	**To ensure correct and secure operations of information processing facilities.**			
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	**Applicable**	Part of the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	**Applicable**	A change management procedure is implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required sys- tem performance.	**Applicable**	Part of the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be sepa- rated to reduce the risks of unauthorized access or changes to the operational environment.	**Applicable**	PinkWeb has implemented a separation between development, testing, acceptance and operational enviroment (OTAP).	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.2	**Protection from malware**	**To ensure that information and information processing facilities are protected against malware.**			
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	**Applicable**	The operations manual describes the implemented methods, such as virus scanners, anti spam etc. Also part of awareness.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.3	**Backup**	**To protect against loss of data.**			

A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Applicable	PinkWeb has an information backup policy in place. The policy is described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.4	**Logging and monitoring**	**To record events and generate evidence.**			
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and infor- mation security events shall be produced, kept and regularly reviewed.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a sin- gle reference time source.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.5	**Control of operational software**	**To ensure the integrity of operational systems.**			
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.6	**Technical vulnerability management**	**To prevent exploitation of technical vulnerabilities.**			
A.12.6.1	Management of technical vulnerabilities	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 meas- ures taken to address the associated risk.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.12.7	**Information systems audit considerations**	**To minimise the impact of audit activities on operational systems.**			
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of opera- tional systems shall be carefully planned and agreed to minimise disruptions to business processes.	Applicable	Procedures have been designed and are in place. The measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
			A.13 Communications security		
A.13.1	**Network security management**	**To ensure the protection of information in networks and its supporting information processing facilities.**			
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Applicable	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.13.1.2	Security of network services	Security mechanisms, service levels and management require- ments of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Applicable	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Applicable	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.13.2	**Information transfer**	**To maintain the security of information transferred within an organization and with any external entity.**			
A.13.2.1	Information transfer policies and procedures	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	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements ref lecting the organization’s needs for the protection of informa- tion shall be identified, regularly reviewed and documented.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14 System acquisition, development and maintenance					
A.14.1	**Security requirements of information systems**	**To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.**			
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dis- pute and unauthorized disclosure and modification.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthoized message duplication or replay.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2	**Security in development and support processes**	**To ensure that information security is designed and implemented within the development lifecycle of information systems.**			
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applica- tions shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.14.3	**Test data**	**To ensure the protection of data used for testing.**			
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	**Applicable**	Measures are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.15 Supplier relationships					
A.15.1	**Information security in supplier relationships**	**To ensure protection of the organization’s assets that is accessible by suppliers.**			
A.15.1.1	Information security policy for supplier relationships	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.	**Applicable**	Security is part of all contracts. All contracts and agreements are reviewed periodically.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.15.1.2	Addressing security within supplier agreements	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.	**Applicable**	Security is part of all contracts. All contracts and agreements are reviewed periodically.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	**Applicable**	Security is part of all contracts. All contracts and agreements are reviewed periodically.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.15.2	**Supplier service delivery management**	**To maintain an agreed level of information security and service delivery in line with supplier agreements.**			
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	**Applicable**	Part of the security officers role. A policy has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.15.2.2	Managing changes to supplier services	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.	**Applicable**	Part of the security officers role. A policy has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.16 Information security incident management					
A.16.1	**Management of information security incidents and improvements**	**To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.**			
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	**Applicable**	A formal Information security incident management has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	**Applicable**	All roles in the organisation have been clearly instructed to report any and all information security events. Part of awareness.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.16.1.3	Reporting information security weaknesses	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 sys- tems or services.	Applicable	All roles in the organisation have been clearly instructed to report any and all information security weaknesses. Part of awareness.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Applicable	A formal Information security incident management has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Applicable	A formal Information security incident management has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Applicable	A formal Information security incident management has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Applicable	A formal Information security incident management has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.17 Information security aspects of business continuity management					
A.17.1	**Information security continuity**	**Information security continuity shall be embedded in the organization’s business continuity management systems.**			
A.17.1.1	Planning information security continuity	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.	Applicable	A business continuity plan has been established. Also formal methods for the prevention of potential calamities have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.17.1.2	Implementing information security continuity	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.	Applicable	A business continuity plan has been established. Also formal methods for the prevention of potential calamities have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.17.1.3	Verify, review and evaluate information security continuity	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.	Applicable	Business continuity plans are tested and updates periodically.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.17.2	**Redundancies**	**To ensure availability of information processing facilities.**			
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Applicable	Measure are described in the operations manual.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18 Compliance					
A.18.1	**Compliance with legal and contractual requirements**	**To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.**			
A.18.1.1	Identification of applicable legislation and contractual requirements	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.	Applicable	All relevant statuatory, regulatory and contractual requirements have been identified, documented are kept up to date.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18.1.2	Intellectual property rights	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.	Applicable	Formal policies for the protection of intellectual property rights has been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Applicable	Formal procedures for the protection of organisational records have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Applicable	Formal policies to protect data and privacy according to relevant legislation, regulations and contracual clausses have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Applicable	Where relevant cryptographic controls have been implemented are a subject to relevant laws and regulations.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18.2	**Information security reviews**	**To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.**			
A.18.2.1	Independent review of information security	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.	Applicable	A formal audit plan and and audit procedures have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18.2.2	Compliance with security policies and standards	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.	Applicable	A formal audit plan and and audit procedures have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	Applicable	A formal audit plan and and audit procedures have been implemented.	Control has been selected after analysis based on risk assessment and the PinkWeb context.

Count			
114	Applicable	This control is definitely needed to mitigate unacceptable risks (default response!)	100%
0	Not Applicable	This control is not needed, usually because management believes the corresponding risks are acceptable (justify in the comments)	0%
114			