Gap analysis: status of ISO/IEC 27001 implementation

Clause	Mandatory requirements ISO27001:2013	Mandatory requirements ISO22301:2012	Status
4	**Context of the organization**		
4.1	**Understanding the organization and its context**		Fully Implemented
4.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its BCMS. These issues shall be taken into account when establishing, implementing and maintaining the organization's BCMS.	Fully Implemented
Note:	*Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009*		
4.1.a		"The organization shall identify and document the following: a) the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident;"	Fully Implemented
4.1.b		"The organization shall identify and document the following: b) links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy; "	Fully Implemented
4.1.c		*"The organization shall identify and document the following: c) the organization's risk appetite."*	Fully Implemented
		"In establishing the context, the organization shall — articulate its objectives, including those concerned with business continuity, — define the external and internal factors that create the uncertainty that gives rise to risk, — set risk criteria taking into account the risk appetite, and — define the purpose of the BCMS."	Fully Implemented
4.2	**Understanding the needs and expectations of interested parties**		Fully Implemented
4.2	The organization shall determine:	"When establishing its BCMS, the organization shall determine	Fully Implemented
4.2.a	interested parties that are relevant to the information security management system; and	a) its relevant interested parties, and	Fully Implemented
4.2.b	the requirements of these interested parties relevant to information security.	b) their requirements (i.e. their needs and expectations whether stated, implied or obligatory)."	Fully Implemented
Note:	*The requirements of interested parties may include legal and regulatory requirements and contractual obligations.*		
4.2.2		The organization shall establish, implement and maintain a procedure(s) to identify, have access to, and assess the applicable legal and regulatory requirements to which the organization subscribes related to the continuity of its operations, products and services, as well as the interests of relevant interested parties.	Fully Implemented
4.2.2		The organization shall ensure that these applicable legal, regulatory and other requirements to which the organization subscribes are taken into account in establishing, implementing and maintaining its BCMS.	Fully Implemented
4.2.2		The organization shall document this information and keep it up-to-date. New or variations to legal, regulatory and other requirements shall be communicated to affected employees and other interested parties.	Fully Implemented
4.3	**Determining the scope of the information security management system**		Fully Implemented
4.3	The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider:	The organization shall determine the scope of the BCMS, such that the boundaries and applicability of the BCMS can be clearly communicated to relevant internal and external parties.	Fully Implemented
4.3.a	the external and internal issues referred to in 4.1.;		Fully Implemented
4.3.b	the requirements referred to in 4.2; and		Fully Implemented
4.3.c	interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.		Fully Implemented
4.4.	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.		Fully Implemented
4.4.	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.		Fully Implemented
5	**Leadership**		
5.1	**Leadership and commitment**		Fully Implemented
5.1.	Top management shall demonstrate leadership and commitment with respect to the information security management system by:		Fully Implemented
5.1.a	ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;		Fully Implemented
5.1.b	ensuring the integration of the information security management system requirements into the organization's processes;		Fully Implemented
5.1.c	ensuring that the resources needed for the information security management system are available;		Fully Implemented
5.1.d	communicating the importance of effective information security management and of conforming to the information security management system requirements;		Fully Implemented
5.1.e	ensuring that the information security management system achieves its intended outcome(s);		Fully Implemented
5.1.f	directing and supporting persons to contribute to the effectiveness of the information security management system;		Fully Implemented
5.1.g	promoting continual improvement; and		Fully Implemented
5.1.h	supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.		Fully Implemented
5.2	**Policy**		Fully Implemented
5.2.	Top management shall establish an information security policy that:		Fully Implemented
5.2.a	is appropriate to the purpose of the organization;		Fully Implemented
5.2.b	includes information security objectives (see 6.2) or provides the framework for setting information security objectives;		Fully Implemented
5.2.c	includes a commitment to satisfy applicable requirements related to information security; and		Fully Implemented
5.2.d	includes a commitment to continual improvement of the information security management system.		Fully Implemented
5.2.	The information security policy shall:		Fully Implemented
5.2.e	be available as documented information		Fully Implemented

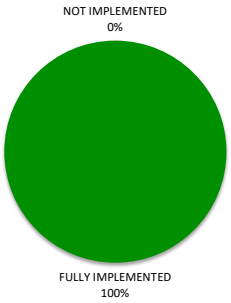
5.2.f	be communicated within the organization; and		Fully Implemented
5.2.g	be available to interested parties, as appropriate.		Fully Implemented
5.3	**Organizational roles, responsibilities and authorities**		Fully Implemented
5.3.	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for:		Fully Implemented
5.3.a	ensuring that the information security management system conforms to the requirements of this International Standard: and		Fully Implemented
5.3.b	reporting on the performance of the information security management system to top management.		Fully Implemented
Note:	*Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.*		
6	**Planning**		
6.1	**Actions to address risks and opportunities**		Fully Implemented
6.1.1	**General**		Fully Implemented
6.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:		Fully Implemented
6.1.1.a	ensure the information security management system can achieve its intended outcome(s);		Fully Implemented
6.1.1.b	prevent, or reduce, undesired effects; and		Fully Implemented
6.1.1.c	achieve continual improvement.		Fully Implemented
6.1.1	The organization shall plan:		Fully Implemented
6.1.1.d	actions to address these risks and opportunities; and		Fully Implemented
6.1.1.e	how to		Fully Implemented
6.1.1.e(1)	integrate and implement the actions into its information security management system processes; and		Fully Implemented
6.1.1.e(2)	evaluate the effectiveness of these actions.		Fully Implemented
6.1.2	**Information Security Risk Assessment**		Fully Implemented
6.1.2.	The organization shall define and apply an information security risk assessment process that:		Fully Implemented
6.1.2.a	establishes and maintains information security risk criteria that include:		Fully Implemented
6.1.2.a(1)	the risk acceptance criteria; and		Fully Implemented
6.1.2.a(2)	criteria for performing information security risk assessments;		Fully Implemented
6.1.2.b	ensures that repeated information security risk assessments produce consistent, valid and comparable results;		Fully Implemented
6.1.2.c	identifies the information security risks:		Fully Implemented
6.1.2.c(1)	apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and		Fully Implemented
6.1.2.c(2)	identify the risk owners;		Fully Implemented
6.1.2.d	analyses the information security risks:		Fully Implemented
6.1.2.d(1)	assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;		Fully Implemented
6.1.2.d(2)	assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and		Fully Implemented
6.1.2.d(3)	determine the levels of risk;		Fully Implemented
6.1.2.e	evaluates the information security risks:		Fully Implemented
6.1.2.e(1)	compare the results of risk analysis with the risk criteria established in 6.1.2. a); and		Fully Implemented
6.1.2.e(2)	prioritize the analysed risks for risk treatment.		Fully Implemented
6.1.2	The organization shall retain documented information about the information securit y risk assessment process.		Fully Implemented
6.1.3	**Information security risk treatment**		Fully Implemented
6.1.3.	The organization shall define and apply an information security risk treatment process to:		Fully Implemented
6.1.3.a	select appropriate information security risk treatment options, taking account of the risk assessment results;		Fully Implemented
6.1.3.b	determine all controls that are necessary to implement the information security risk treatment option(s) chosen;		Fully Implemented
note:	*Organizations can design controls as required, or identify them from any source.*		
6.1.3.c	compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;		Fully Implemented
note:	*Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.*		
note:	*Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.*		
6.1.3.d	produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;		Fully Implemented
6.1.3.e	formulate an information security risk treatment plan; and		Fully Implemented
6.1.3.f	obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.		Fully Implemented
6.1.3.	The organization shall retain documented information about the information security risk treatment process.		Fully Implemented
note:	*The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000[5].*		
6.2	**Information security objectives and planning to achieve them**		Fully Implemented
6.2.	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:		Fully Implemented

	6.2.a	be consistent with the information security policy;		Fully Implemented
	6.2.b	be measurable (if practicable);		Fully Implemented
	6.2.c	take into account applicable information security requirements, and results from risk assessment and risk treatment;		Fully Implemented
	6.2.d	be communicated; and		Fully Implemented
	6.2.e	be updated as appropriate.		Fully Implemented
	6.2.	The organization shall retain documented information on the information security objectives.		Fully Implemented
	6.2.	When planning how to achieve its information security objectives, the organization shall determine:		Fully Implemented
	6.2.f	what will be done;		Fully Implemented
	6.2.g	what resources will be required;		Fully Implemented
	6.2.h	who will be responsible;		Fully Implemented
	6.2.i	when it will be completed; and		Fully Implemented
	6.2.j	how the results will be evaluated.		Fully Implemented
	7	**Support**		
	7.1	**Resources**		Fully Implemented
	7.1.	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.		Fully Implemented
	7.2	**Competence**		Fully Implemented
	7.2.	The organization shall:		Fully Implemented
	7.2.a	determine the necessary competence of person(s) doing work under its control that affects its information security performance;		Fully Implemented
	7.2.b	ensure that these persons are competent on the basis of appropriate education, training, or experience;		Fully Implemented
	7.2.c	where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and		Fully Implemented
	7.2.d	retain appropriate documented information as evidence of competence.		Fully Implemented
	Note:	*Applicable actions may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons*		
	7.3	**Awareness**		Fully Implemented
	7.3.	Persons doing work under the organization's control shall be aware of:		Fully Implemented
	7.3.a	the information security policy;		Fully Implemented
	7.3.b	their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and		Fully Implemented
	7.3.c	the implications of not conforming with the information security management system requirements.		Fully Implemented
	7.4	**Communication**		Fully Implemented
	7.4.	The organization shall determine the need for internal and external communications relevant to the information security management system including:		Fully Implemented
	7.4.a	on what to communicate;		Fully Implemented
	7.4.b	when to communicate;		Fully Implemented
	7.4.c	with whom to communicate;		Fully Implemented
	7.4.d	who shall communicate; and		Fully Implemented
	7.4.e	the processes by which communication shall be effected.		Fully Implemented
	7.5	**Documented Information**		Fully Implemented
	7.5.1	**General**		Fully Implemented
	7.5.1.	The organization's information security management system shall include:		Fully Implemented
	7.5.1.a	documented information required by this International Standard; and		Fully Implemented
	7.5.1.b	documented information determined by the organization as being necessary for the effectiveness of the information security management system.		Fully Implemented
	Note:	*The extent of documented information for an information security management system can differ from one organization to another due to:*		
		the size of organization and its type of activities, processes, products and services;		
		the complexity of processes and their interactions; and		
		the competence of persons.		
	7.5.2	**Creating and updating**		Fully Implemented
	7.5.2.	When creating and updating documented information the organization shall ensure appropriate:		Fully Implemented
	7.5.2.a	identification and description (e.g. a title, date, author, or reference number);		Fully Implemented
	7.5.2.b	format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and		Fully Implemented
	7.5.2.c	review and approval for suitability and adequacy.		Fully Implemented
	7.5.3	**Control of documented information**		Fully Implemented
	7.5.3.	Documented information required by the information security management system and by this International Standard shall be controlled to ensure:		Fully Implemented
	7.5.3.a	it is available and suitable for use, where and when it is needed; and		Fully Implemented
	7.5.3.b	it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).		Fully Implemented
	7.5.3.	For the control of documented information, the organization shall address the following activities, as applicable:		Fully Implemented
	7.5.3.a	distribution, access, retrieval and use;		Fully Implemented
	7.5.3.b	storage and preservation, including the preservation of legibility;		Fully Implemented
	7.5.3.c	control of changes (e.g. version control); and		Fully Implemented
	7.5.3.d	retention and disposition.		Fully Implemented
	7.5.3.	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.		Fully Implemented

Note:	*Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.*		
8	**Operation**		
8.1	**Operational planning and control**		Fully Implemented
8.1.	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.		Fully Implemented
8.1.	The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.		Fully Implemented
8.1.	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.		Fully Implemented
8.1.	The organization shall ensure that outsourced processes are determined and controlled.		
8.2	**Operational planning and control**		Fully Implemented
8.2.	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).		Fully Implemented
8.2.	The organization shall retain documented information of the results of the information securit y risk treatment.		Fully Implemented
9	**Performance evaluation**		
9.1	**Monitoring, measurement, analysis and evaluation**		Fully Implemented
9.1.	The organization shall evaluate the information security performance and the effectiveness of the information security management system.		Fully Implemented
9.1.	The organization shall determine:		Fully Implemented
9.1.a	what needs to be monitored and measured, including information security processes and controls;		Fully Implemented
9.1.b	the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;		Fully Implemented
note:	*The methods selected should produce comparable and reproducible results to be considered valid.*		
9.1.c	when the monitoring and measuring shall be performed;		Fully Implemented
9.1.d	who shall monitor and measure;		Fully Implemented
9.1.e	when the results from monitoring and measurement shall be analysed and evaluated; and		Fully Implemented
9.1.f	who shall analyse and evaluate these results.		Fully Implemented
9.1.	The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.		Fully Implemented
9.2	**Internal audit**		Fully Implemented
9.2.	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:		Fully Implemented
9.2.a	conforms to		Fully Implemented
9.2.a(1)	the organization's own requirements for its information security management system; and		Fully Implemented
9.2.a(2)	the requirements of this International Standard;		Fully Implemented
9.2.b	is effectively implemented and maintained.		Fully Implemented
9.2.	The organization shall:		Fully Implemented
9.2.c	plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;		Fully Implemented
9.2.d	define the audit criteria and scope for each audit;		Fully Implemented
9.2.e	select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;		Fully Implemented
9.2.f	ensure that the results of the audits are reported to relevant management; and		Fully Implemented
9.2.g	retain documented information as evidence of the audit programme(s) and the audit results.		Fully Implemented
9.3	**Management Review**		Fully Implemented
9.3.	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.		Fully Implemented
9.3.	The management review shall include consideration of:		Fully Implemented
9.3.a	the status of actions from previous management reviews;		Fully Implemented
9.3.b	changes in external and internal issues that are relevant to the information security management system;		Fully Implemented
9.3.c	feedback on the information security performance, including trends in:		Fully Implemented
9.3.c(1)	nonconformities and corrective actions;		Fully Implemented
9.3.c(2)	monitoring and measurement results;		Fully Implemented
9.3.c(3)	audit results; and		Fully Implemented
9.3.c(4)	fulfilment of information security objectives;		Fully Implemented
9.3.d	feedback from interested parties;		Fully Implemented
9.3.e	results of risk assessment and status of risk treatment plan; and		Fully Implemented
9.3.f	opportunities for continual improvement.		Fully Implemented
9.3.	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.		Fully Implemented
9.3.	The organization shall retain documented information as evidence of the results of management reviews.		Fully Implemented
10	**Improvement**		
10.1	**Nonconformity and corrective action**		Fully Implemented
10.1.	When a nonconformity occurs, the organization shall:		Fully Implemented
10.1.a	react to the nonconformity, and as applicable:		Fully Implemented
10.1.a(1)	take action to control and correct it; and		Fully Implemented

10.1.a(2)	deal with the consequences;		Fully Implemented
10.1.b	evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:		Fully Implemented
10.1.b(1)	reviewing the nonconformity;		Fully Implemented
10.1.b(2)	determining the causes of the nonconformity; and		Fully Implemented
10.1.b(3)	determining if similar nonconformities exist, or could potentially occur;		Fully Implemented
10.1.c	implement any action needed;		Fully Implemented
10.1.d	review the effectiveness of any corrective action taken; and		Fully Implemented
10.1.e	make changes to the information security management system, if necessary.		Fully Implemented
10.1.	Corrective actions shall be appropriate to the effects of the nonconformities encountered.		Fully Implemented
10.1.	The organization shall retain documented information as evidence of:		Fully Implemented
10.1.f	the nature of the nonconformities and any subsequent actions taken, and		Fully Implemented
10.1.g	the results of any corrective action.		Fully Implemented
10.2	**Continual Improvement**		Fully Implemented
10.2.	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	The organization shall continually improve the suitability, adequacy or effectiveness of the BCMS.	Fully Implemented
197	FULLY IMPLEMENTED		100%
0	NOT IMPLEMENTED		0%
197			

Implementation Status ISO27001:2013



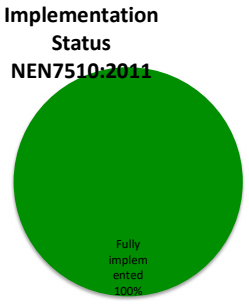
Gap analysis: status of NEN7510 implementation

ISO /IEC 27001 clause	Mandatory requirement for the ISMS	Status
4	Information Security Management System	
4.1	General requirements	
4.1	The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS	Fully implemented
4.2	Establishing and managing the ISMS	
4.2.1	Establish the ISMS	
4.2.1 (a)	Define the scope and boundaries of the ISMS	Fully implemented
4.2.1 (b)	Define an ISMS policy	Fully implemented
4.2.1 (c)	Define the risk assessment approach	Fully implemented
4.2.1 (d)	Identify the risks	Fully implemented
4.2.1 (e)	Analyse and evaluate the risks	Fully implemented
4.2.1 (f)	Identify and evaluate options for the treatment of risks	Fully implemented
4.2.1 (g)	Select control objectives and controls for the treatment of risks	Fully implemented
4.2.1 (h)	Obtain management approval of the proposed residual risks	Fully implemented
4.2.1 (i)	Obtain management authorization to implement and operate the ISMS	Fully implemented
4.2.1 (j)	Prepare a Statement of Applicability [see the SoA spreadsheet]	Fully implemented
4.2.2	Implement the ISMS	
4.2.2 (a)	Formulate a risk treatment plan	Fully implemented
4.2.2 (b)	Implement the risk treatment plan in order to achieve the identified control objectives	Fully implemented
4.2.2 (c)	Implement controls selected in 4.2.1g to meet the control objectives	Fully implemented
4.2.2 (d)	Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)	Fully implemented
4.2.2 (e)	Implement training and awareness programmes (see 5.2.2)	Fully implemented
4.2.2 (f)	Manage operation of the ISMS	Fully implemented
4.2.2 (g)	Manage resources for the ISMS (see 5.2)	Fully implemented
4.2.2 (h)	Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3a)	Fully implemented
4.2.3	Monitor and review the ISMS	
4.2.3 (a)	Execute monitoring and reviewing procedures and other controls	Fully implemented
4.2.3 (b)	Undertake regular reviews of the effectiveness of the ISMS	Fully implemented
4.2.3 (c)	Measure the effectiveness of controls to verify that security requirements have been met.	Fully implemented
4.2.3 (d)	Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks	Fully implemented
4.2.3 (e)	Conduct internal ISMS audits at planned intervals (see 6)	Fully implemented
4.2.3 (f)	Undertake a management review of the ISMS on a regular basis (see 7.1)	Fully implemented
4.2.3 (g)	Update security plans to take into account the findings of monitoring and reviewing activities	Fully implemented
4.2.3 (h)	Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3)	Fully implemented
4.2.4	Maintain and improve the ISMS	
4.2.4 (a)	Implement the identified improvements in the ISMS.	Fully implemented
4.2.4 (b)	Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3	Fully implemented
4.2.4 (c)	Communicate the actions and improvements to all interested parties	Fully implemented
4.2.4 (d)	Ensure that the improvements achieve their intended objectives	Fully implemented
4.3	Documentation requirements	
4.3.1	General ISMS documentation	
4.3.1 (a)	Documented statements of the ISMS policy (see 4.2.1b) and objectives	Fully implemented
4.3.1 (b)	Scope of the ISMS (see 4.2.1a)	Fully implemented
4.3.1 (c)	Procedures and controls in support of the ISMS	Fully implemented
4.3.1 (d)	Description of the risk assessment methodology (see 4.2.1c)	Fully implemented
4.3.1 (e)	Risk assessment report (see 4.2.1c to 4.2.1g)	Fully implemented
4.3.1 (f)	Risk treatment plan (see 4.2.2b)	Fully implemented
4.3.1 (g)	Procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3c)	Fully implemented
4.3.1 (h)	Records required by this International Standard (see 4.3.3)	Fully implemented
4.3.1 (i)	Statement of Applicability	Fully implemented
4.3.2	Control of documents	
4.3.2	Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:	Fully implemented
4.3.2 (a)	Approve documents for adequacy prior to issue	Fully implemented
4.3.2 (b)	Review and update documents as necessary and re-approve documents	Fully implemented
4.3.2 (c)	Ensure that changes and the current revision status of documents are identified	Fully implemented
4.3.2 (d)	Ensure that relevant versions of applicable documents are available at points of use	Fully implemented
4.3.2 (e)	Ensure that documents remain legible and readily identifiable	Fully implemented
4.3.2 (f)	Ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification	Fully implemented
4.3.2 (g)	Ensure that documents of external origin are identified	Fully implemented
4.3.2 (h)	Ensure that the distribution of documents is controlled	Fully implemented
4.3.2 (i)	Prevent the unintended use of obsolete documents	Fully implemented
4.3.2 (j)	Apply suitable identification to documents if they are retained for any purpose	Fully implemented
4.3.3	Control of records	
4.3.3	Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS …	Fully implemented
4.3.3	Records shall be protected and controlled.	Fully implemented
4.3.3	The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations.	Fully implemented
4.3.3	Records shall remain legible, readily identifiable and retrievable.	Fully implemented
4.3.3	The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.	Fully implemented
4.3.3	Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS.	Fully implemented

5	Management responsibility	
5.1	Management commitment	
5.1	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:	Fully implemented
5.1 (a)	Establishing an ISMS policy	Fully implemented
5.1 (b)	Ensuring that ISMS objectives and plans are established	Fully implemented
5.1 (c)	Establishing roles and responsibilities for information security	Fully implemented
5.1 (d)	Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement	Fully implemented
5.1 (e)	Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1)	Fully implemented
5.1 (f)	Deciding the criteria for accepting risks and the acceptable levels of risk	Fully implemented
5.1 (g)	Ensuring that internal ISMS audits are conducted (see 6)	Fully implemented
5.1 (h)	Conducting management reviews of the ISMS (see 7)	Fully implemented
5.2	Resource management	
5.2.1	Provision of resources	
5.2.1	The organization shall determine and provide the resources needed to:	Fully implemented
5.2.1 (a)	Establish, implement, operate, monitor, review, maintain and improve an ISMS	Fully implemented
5.2.1 (b)	Ensure that information security procedures support the business requirements	Fully implemented
5.2.1 (c)	Identify and address legal and regulatory requirements and contractual security obligations	Fully implemented
5.2.1 (d)	Maintain adequate security by correct application of all implemented controls	Fully implemented
5.2.1 (e)	Carry out reviews when necessary, and to react appropriately to the results of these reviews	Fully implemented
5.2.1 (f)	Where required, improve the effectiveness of the ISMS	Fully implemented
5.2.2	Training, awareness and competence	
5.2.2	The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:	Fully implemented
5.2.2 (a)	Determining the necessary competencies for personnel performing work effecting the ISMS	Fully implemented
5.2.2 (b)	Providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs	Fully implemented
5.2.2 (c)	Evaluating the effectiveness of the actions taken	Fully implemented
5.2.2 (d)	Maintaining records of education, training, skills, experience and qualifications (see 4.3.3)	Fully implemented
5.2.2	The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.	Fully implemented
6	Internal ISMS audit	
6	The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:	Fully implemented
6 (a)	Conform to the requirements of this International Standard and relevant legislation or regulations	Fully implemented
6 (b)	Conform to the identified information security requirements	Fully implemented
6 (c)	Are effectively implemented and maintained	Fully implemented
6 (d)	Perform as expected.	Fully implemented
6	An audit programme shall be planned	Fully implemented
6	The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8).	Fully implemented
7	Management review of the ISMS	
7.1	General	
7.1	Management shall review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness	Fully implemented
7.2	Review input	
7.2	The input to a management review shall include:	Fully implemented
7.2 (a)	Rsults of ISMS audits and reviews	Fully implemented
7.2 (b)	Feedback from interested parties	Fully implemented
7.2 (c)	Techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness	Fully implemented
7.2 (d)	Status of preventive and corrective actions	Fully implemented
7.2 (e)	Vulnerabilities or threats not adequately addressed in the previous risk assessment	Fully implemented
7.2 (f)	Results from effectiveness measurements	Fully implemented
7.2 (g)	Follow-up actions from previous management reviews	Fully implemented
7.2 (h)	Any changes that could affect the ISMS	Fully implemented
7.2 (i)	Recommendations for improvement	Fully implemented
7.3	Review output	
7.3	The output from the management review shall include any decisions and actions related to the following:	Fully implemented
7.3 (a)	Improvement of the effectiveness of the ISMS	Fully implemented
7.3 (b)	Update of the risk assessment and risk treatment plan	Fully implemented
7.3 (c)	Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS	Fully implemented
7.3 (d)	Resource needs	Fully implemented
7.3 (e)	Improvement to how the effectiveness of controls is being measured	Fully implemented
8	ISMS improvement	
8.1	Continual improvement	
8.1	The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).	Fully implemented
8.2	Corrective action	
8.2	The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action shall define requirements for:	Fully implemented
8.2 (a)	Identifying nonconformities	Fully implemented
8.2 (b)	Determining the causes of nonconformities	Fully implemented
8.2 (c)	Evaluating the need for actions to ensure that nonconformities do not recur	Fully implemented
8.2 (d)	Determining and implementing the corrective action needed	Fully implemented
8.2 (e)	Recording results of action taken (see 4.3.3)	Fully implemented
8.2 (f)	Reviewing of corrective action taken	Fully implemented
8.3	Preventive action	

8.3	The organization shall determine action to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:	Fully implemented
8.3 (a)	Identifying potential nonconformities and their causes	Fully implemented
8.3 (b)	Evaluating the need for action to prevent occurrence of nonconformities	Fully implemented
8.3 (c)	Determining and implementing preventive action needed	Fully implemented
8.3 (d)	Recording results of action taken (see 4.3.3)	Fully implemented
8.3 (e)	Reviewing of preventive action taken	Fully implemented
8.3	The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks	Fully implemented
	NEN7510-specific clauses	
4.1	Waar mogelijk integreren organisaties hun ISMS met de processen voor borging van kwaliteit en patiëntveiligheid en houden zij rekening met de richtlijnen genoemd in 4.3 t.m. 4.6.	Fully implemented
6.1.3	Organisaties die patiëntgegevens verwerken behoren de verantwoordelijkheden voor de beveiliging van patiëntgegevens eenduidig toe te wijzen.	Fully implemented
7.2.2	Alle informatiesystemen die patiëntgegevens verwerken behoren de gebruikers, bijvoorbeeld via een inlogboodschap, te wijzen op de vertrouwelijkheid van de gegevens die via het systeem toegankelijk zijn. Documenten met patiëntgegevens behoren van het kenmerk "vertrouwelijk" te zijn voorzien.	Fully implemented
8.1.3	Een organisatie die patiëntgegevens verwerkt behoort in de aanstellingsvoorwaarden van medewerkers, vrijwilligers of contractanten die patiëntgegevens verwerken of gaan verwerken een verklaring op te nemen over de geheimhouding en zorgvuldigheid die daarbij is vereist vanuit het informatiebeveiligingsbeleid van de organisatie.	Fully implemented
8.2.2	Een organisatie die patiëntgegevens verwerkt behoort ervoor te zorgen dat opleiding en training inzake informatiebeveiliging zijn geregeld voor alle medewerkers bij aanvang van het dienstverband en dat regelmatige opfrissing van de kennis is voorzien.	Fully implemented
9.2.5	Een organisatie die patiëntgegevens verwerkt behoort te zorgen voor toestemming voor elk gebruik buiten de instelling van medische apparaten die gegevens registreren en/of doorgeven, met inbegrip van apparatuur die, al of niet permanent, in gebruik is bij ambulante medewerkers en mogelijk tot hun vaste uitrusting behoort.	Fully implemented
10.5.1	Een organisatie, die patiëntgegevens verwerkt, behoort van alle patiëntgegevens back-upkopieën te maken en in een veilige omgeving op te slaan om de beschikbaarheid te waarborgen.	Fully implemented
10.7.3	Media met patiëntgegevens behoren fysiek te worden beveiligd. Op de staat en locatie van media met patiëntgegevens behoort controle te worden uitgeoefend.	Fully implemented
10.9.3	Openbaar beschikbare zorginformatie (te onderscheiden van patiëntgegevens) behoort systematisch te worden gearchiveerd. Van openbaar beschikbare zorginformatie behoort de bron of auteur te zijn vermeld.	Fully implemented
10.10.3	De logging van informatiesystemen voor het verwerken van patiëntgegevens behoort te zijn beveiligd en niet te manipuleren.	Fully implemented
10.10.6	Zorginformatiesystemen die tijdkritische zorgactiviteiten ondersteunen behoren te voorzien in synchronisatie om mogelijke tijdverschillen tussen verschillende registraties van activiteiten te signaleren en daarvoor te corrigeren.	Fully implemented
11.1.1	Een organisatie die patiëntgegevens verwerkt, behoort een toegangsbeleid ten aanzien van deze gegevens te hanteren. Het toegangsbeleid behoort te voldoen aan professionele, ethische, wettelijke en patiëntgerelateerde eisen en tevens tegemoet komen aan de eisen die het werk van zorgprofessionals stelt en speciale aandacht besteden aan de beschikbaarheid van gegevens bij het verlenen van acute zorg.	Fully implemented
11.2.1	Een organisatie die patiëntgegevens verwerkt, behoort te waarborgen dat toegang tot systemen die patiëntgegevens verwerken deel uitmaakt van een formele gebruikersregistratieprocedure. Deze procedure behoort te waarborgen dat de mate van vereiste authenticatie bij een gebruiker in overeenstemming is met het resulterende niveau van toegang.	Fully implemented
11.5.2	Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken.	Fully implemented
12.2.1	Informatiesystemen die patiëntgegevens verwerken moeten alle patiëntgegevens gecontroleerd van de juiste patiëntidentificatie voorzien.	Fully implemented
12.2.4	Informatiesystemen behoren bij het presenteren van patiëntgegevens altijd voldoende identificerende gegevens te tonen om het de zorgverlener mogelijk te maken vast te stellen dat de patiëntgegevens de patiënt in kwestie betreffen.	Fully implemented
12.4.2	Er behoren geen tot personen herleidbare patiëntgegevens te worden gebruikt als testgegevens.	
14.1.2	Organisaties die patiëntgegevens verwerken behoren een continuïteitsstrategie vast te stellen, te documenteren, in te voeren en te onderhouden. Hierin behoort voor ieder bedrijfsproces een maximaal toegelaten uitvalduur (MUD) en een maximaal toelaatbaar verlies aan gegevens (MGV) te worden vastgesteld.	Fully implemented
15.1.3	Organisaties die patiëntgegevens verwerken behoren ervoor te zorgen dat tot een persoon herleidbare gegevens niet langer worden bewaard dan noodzakelijk en dat het risico van onbedoelde openbaarmaking van persoonsgegevens waar mogelijk wordt beperkt door vernietigen van de gegevens, danwel door anonimiseren of pseudonimiseren. Zie NPR-ISO/TS 25237:2008 [30].	Fully implemented
15.1.4	Behoudens wettelijke uitzonderingen, behoort een zorginstelling toestemming te hebben van de patiënt voor het uitwisselen van zijn gegevens.	Fully implemented

Count		Proportion
137	Fully implemented	100%
0	Partially implemented	0%
0	Not implemented	0%
137	Total	



Statement of Applicability of ISO27001:2013

Version	201701
Date Approved	15-Feb-17
By	Director of Operations

Annex A ref	Control title	Control Description	Applicability
		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.5.1.2	Review of the policies 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
		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**	
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Applicable
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
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Applicable
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Applicable
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
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.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.7 Human resource security	
A.7.1	**Prior to employment**	**To ensure that employees and contractors understand their responsibilities and are suit-able 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
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
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
A.7.2.2	Information security awareness, education and training	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.	Applicable
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.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, communicated to the employee or contractor and enforced.	Applicable
		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.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Applicable
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
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
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.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.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable
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.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Applicable
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Applicable
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.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.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.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.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Applicable
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.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Applicable
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.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.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.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.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Applicable
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.9.4.5	Access control to program source code	Access to program source code shall be restricted.	Applicable
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
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
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
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
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Applicable
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
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Applicable

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
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
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Applicable
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Applicable
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Applicable
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
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
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Applicable
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Applicable
		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
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.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Applicable
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Applicable
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
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
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 information security events shall be produced, kept and regularly reviewed.	Applicable
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Applicable
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
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 single reference time source.	Applicable
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
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 measures taken to address the associated risk.	Applicable
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Applicable
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 operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Applicable
		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
A.13.1.2	Security of network services	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.	Applicable
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Applicable
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
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Applicable
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Applicable
A.13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Applicable
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
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 dispute and unauthorized disclosure and modification.	Applicable
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
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
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
A.14.2.3	Technical review of applications after operating platform changes	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.	Applicable
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
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
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
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Applicable
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Applicable
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
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
		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
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
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
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
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
		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.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Applicable
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 systems or services.	Applicable
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.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Applicable
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.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.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.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.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
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
		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
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
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
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
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Applicable
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.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.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Applicable

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

Statement of Applicability of Cloud Controls

Version	201701
Date Approved	15-Feb-17
By	Director of Operations

Annex A ref	Control title	Control Description	Applicability
		CloudControls	
CC-MULTI	**Multi Tenancy**	**To ensure that activities of one customer will not negatively affect services of another customer**	
CC-MULTI-01	Cloud provider capacity management	Cloud provider will ensure enough capacity is available, taking peaks in usage and multi tenancy into account.	Applicable
CC-MULTI-02	Acceptable activities other customers	Acceptable use with regard to other customers: A customer acceptable use policy will be defined. Prohibited activities in the customer acceptable use policy include illegal activities and activities that threaten the performance of other customers. Immediate action is taken when cloud provider becomes aware acceptable use policy is contravened.	Applicable
CC-MULTI-03	Isolation failure risk	Isolation failure risk in virtualization technology and storage is frequently reviewed and is managed to a minimum.	Applicable
CC-MULTI-04	Network segregation	It is possible to completely separate the environments of a single customer on the network level, sniffing and ip spoofing should be impossible. It should be possible to firewall the customer environment.	Applicable
CC-MULTI-05	Control over hardware in case of subpoena's	Subpoena of other customer: In a subpoena situation the cloud provider commits to make a commercially reasonable effort to resist within the limits of applicable law any confiscation of hardware or data from customers that are not subpoenaed. Procedures are in place allowing the safe extraction of customer assets upon subpoena.	Applicable
CC-OUTS	**Outsourcing: Management information and control**	**To ensure the services are clearly defined and delivered and the customer is always informed properly regarding the terms and conditions as well as the delivery and use of the environment and can act accordingly.**	
CC-OUTS-01	Clear agreements	All terms of business are clearly described and communicated. SLAs between the client and the service organization clearly describe the scope of the stack and application of the SLA.	Applicable
CC-OUTS-39	Changes to agreements	The risk of the provider changing the SLA, Terms of Business or the rest of the agreement against the customers' whishes is mitigated.	Applicable
CC-OUTS-02	Portability of services	Short term contracts are possible, customer virtual assets are exportable and transportable in an industry-accepted format. Sufficient access to the environment or data will be granted in order to implement migration.	Applicable
CC-OUTS-03	Customer risk assessment	Provider should provide information on request regarding the potential for: law enforcement driven confiscation, provider termination, vendor lock-in, change in ownership, financial instability.	Applicable
CC-OUTS-04	Cloud provider compliance with SLA	Procedures regarding the fulfillment of SLA agreements are defined, implemented and will be internally communicated. Upon a change in policies or SLA fulfillment which negatively affect the compliance with the SLA, the clients are promptly informed. The cloud provider will get a reasonable period to bring the SLA delivery back into compliance. If the SLA delivery is not brought back in compliance a compensation is offered to the affected clients. If compliance with the SLA can not be achieved because of a change of law the relevant points of non-compliance will be deemed permissible.	Applicable
CC-OUTS-05	Breach of uptime commitment	A robust committed uptime breach remedy and compensation system is in place. Availability is defined as pingable from outside the network. Key product components being unavailable also implies a service is down. Scheduled downtime is reported in advance.	Applicable
CC-OUTS-06	Information on audits and control over non compliance measures	Cloud provider should communicate audit policy, controls and results. Reports should not include information which might lead to compromise. If an audit reveals the provider is not in compliance with the standards it is committed to, the relevant customers are informed. The cloud provider will get a reasonable period to bring the standard back in compliance. If the standard is not brought back into compliance customers should be compensated. If a change in the law makes it impossible to get back into compliance the relevant point of non-compliance will be deemed permissible.	Applicable
CC-OUTS-07	Extreme provisioning requests	The customer is informed of extreme provisioning requests. Extreme provisioning requests made by mistake or by malicious insiders of the client organization (Economic Denial of Service or EDOS) can be revoked if noticed within a reasonable timeframe. It is possible to cap cost by agreement.	Applicable
CC-OUTS-08	Control over assets at cloud provider termination	An arrangement should be in place ensuring access to data and assets in case the service organization would unexpectedly seize its activities.	Applicable
CC-OUTS-09	Canceling of services	No frivolous canceling of customer contracts: The cloud provider may only cancel a customer contract on short notice if required by law, the services are not paid for or breaches of the fair use policy are ignored. The customer is warned ahead of time if possible and there is a procedure that needs to be followed in these circumstances.	Applicable
CC-OUTS-10	Control over interruption of services	The cloud provider may only suspend a customers' service when it is forced to. The cloud provider may only willingly interrupt the service if required by law, services are not paid for, a breach of the fair use policy is not remedied or the services or other customers are threatened. The customer is warned ahead of time if possible and there is a procedure that needs to be followed in these circumstances.	Applicable
CC-OUTS	**Outsourcing: Legal Process**	**To ensure the customer is always informed properly regarding the legal aspects of the service and any legal action is taken according to predefined procedures**	

CC-OUTS-11	Data location and applicable jurisdictions	Customer can determine jurisdiction where data is stored. It should be communicated which governments and jurisdictions can lay claim to a customers' data, also in situations where the data is transferred from one part of the provider network to another.	Applicable
CC-OUTS-12	Evidence collection	There should be a policy for retaining evidence and information on this policy should be provided. Automated collection of evidence is implemented. Data chain of custody is maintained. Virtual assets also have chain of custody.	Applicable
CC-OUTS-13	Customer investigations	Supporting customer investigations: Cloud provider will cooperate in any incident investigation by the customer including the handing over of relevant logs (subject to privacy commitments).	Applicable
CC-OUTS-14	Review of agreements and law	All relevant contracts, NDA requirements and law should be reviewed periodically.	Applicable
CC-OUTS-15	Disclosure of relevant legislation and regulatory contacts	Cloud provider should communicate legislation relevant to the service that could impact the services of the customer. Cloud provider should also provide details on supervisory authority, court of jurisdiction and contact details. Customer shall be informed about jurisdiction of transport within the provider network.	Applicable
CC-OUTS-16	Secure data ownership	Customer data always remains owned by the customer. Provider should communicate intellectual property rights that it claims.	Applicable
CC-OUTS-17	Legal response	Cloud provider commits to make a commercially reasonable effort to resist any cease and desist or subpoena procedure if the customer so requires within the limits of applicable law. If informing the customer of a legal request or demand is not allowed cloud provider will assume client would want to resist such request.	Applicable
CC-OUTS	**Outsourcing: Infrastructure design**	**To ensure the customer is always informed properly regarding the architecture and implementation of the service.**	
CC-OUTS-21	Information regarding availability and performance	The expected level of performance, level of redundancy and expected recovery times at every level of the processing layer, data storage, the internal network and the transit connections are available A backup policy is established and communicated. Datacenter locations should be communicated. Information on datacenter security, resilience and recovery policies should be available	Applicable
CC-OUTS-22	Information on resiliency management	Disaster recovery plans and availability enhancing measures should be shared with customers when relevant.	Applicable
CC-OUTS-23	Changes in technology and change management	Procedures should be established and implemented regarding the provisioning of information on changes to the information system. Cloud provider should communicate its controls for the procurement of new information systems and enhancements. Provider will endeavor to keep existing technologies used by customers available.	Applicable
CC-OUTS	**Outsourcing: Security Process**	**To ensure security is managed effectively according to the relevant standards and the customer is always informed properly regarding the security aspects of the service**	
CC-OUTS-24	Information on security status and policy changes	Provider management should ensure that security status and requirements can be communicated to customers. Customers should be informed about security policy changes with material impact.	Applicable
CC-OUTS-25	Security weaknesses	Security weaknesses and their mitigation are audited. Reports should not include information which might lead to compromise.	Applicable
CC-OUTS-26	Conflicting roles	Provider should develop and disclose policy with respect to conflicting roles, and address specific conflicting roles in the auditing process.	Applicable
CC-OUTS-27	Customer responsibility regarding incidents	Customers should be made aware of their responsibilities regarding incident management and a procedure for customer imput is in place.	Applicable
CC-OUTS-28	Customer vulnerability assessment	Cloud provider should provide the possibility for vulnerability assessment by customers and provide information on the policy regarding vulnerability assessment.	Applicable
CC-OUTS	**Outsourcing: Operational process**	**To ensure the customer is always properly informed regarding the operational status of the service and disturbances to the service.**	
CC-OUTS-29	Information on incidents	A policy is available to inform customers in the case of a breach of privacy, a security breach or technical failure that could affect the customer. Fault logs policy should be communicated and logs made available to customers on request.	Applicable
CC-OUTS-30	Information regarding SLA performance and service usage	Detailed reporting on SLA performance, used and billable resources.	Applicable
CC-OUTS-31	Information and planning regarding maintenance and information on outages	There is a procedure to communicate with customers in the case of maintenance and outages. Maintenance will be planned in order to minimize customer impact.	Applicable
CC-OUTS-32	Information on degraded services	Outage reporting: If service was interrupted or degraded a detailed report will be provided on the reason and mitigation measures if relevant.	Applicable
CC-OUTS-33	User manuals	Cloud provider should provide explanation pertaining to the relevant services the provider offers.	Applicable
CC-OUTS	**Outsourcing: Connecting to the service**	**To ensure customer information is appropriately protected while connecting to the service.**	
CC-OUTS-34	Management Interface Protection	Public facing web applications and API's related to the cloud service are secured. Connections are made on the basis of strong passwords and encrypted connections.	Applicable
CC-OUTS-35	Customer payment data	Sensitive customer data is encrypted. Measures are implemented to prevent storage and visibility of sensitive financial information.	Applicable

CC-OUTS-36	Management interface access functionality and policies	Customer management interfaces have a role based access model with individual access only, logging and extra checks in the case of data destruction. It should be possible for the authorized customer to change access rights to the customer management interface. Information should be provided on management interface access procedures so the customer can develop its own policies. On client contract termination, all access rights are revoked directly after the contract end date. Reductions in access are implemented immediately and across all applications the customer can access. Information on the use of customer access rights will be provided on demand.	Applicable
CC-OUTS-37	Management Interface Availability	Availability measures for the management interface should be in place.	Applicable
CC-OUTS-38	Customer personnel authorisation	Requests from customer personnel are only executed if that person has been authorized based on his service portfolio and SLA.	Applicable
CC-AVAIL	**Availability**	**To ensure the customer is appropriately protected against malfunction or loss of infrastructure or support.**	
CC-AVAIL-01	Support and spare parts	There is sufficient access to support and spare parts with respect to externally acquired software and hardware.	Applicable
CC-AVAIL-02	Redundancy of core systems	Provider data and core systems: Core provider systems are redundant. A multiple location storage and backup policy for system management data is developed and implemented. Reporting or mitigation mechanisms are in place upon lack of backups or backup-failure.	Applicable
CC-AVAIL-03	Failure isolation	Site redundancy: Failure of one physical site will not result in other sites failing. An alternate processing site is available for core IT functions.	Applicable
CC-AVAIL-04	Employee single point of failure	Risk to single employees is minimised. Skills are not unique and knowledge is documented.	Applicable
CC-AVAIL-05	Datacenter protection	The datacenter environment is controlled with power and air control systems set up redundantly.	Applicable
CC-AVAIL-06	Redundant internet connectivity	The network should be set up redundantly with multiple transit gateways. Measures to divert, mitigate or stop Distributed Denial of Service attacks are implemented. DNS setup is redundant and secured.	Applicable
CC-AVAIL-07	Proper documentation	All components and procedures are documented and this documentation is kept up to date	Applicable

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