Classification: Public

Versie: 2.3
Datum: Sept. 2020

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	**Sectie**	**Beheersmaatregel**	**Maatregel omschrijving**			
A.5 Informatiebeveiliging- en privacybeleid						
	A.5.1 Management direction for information security	A.5.1.1 Beleidsregels voor informatiebeveiliging en privacy	Ten behoeve van informatiebeveiliging en privacy moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	1	1	Verplicht voor uitvoering ISMS
		A.5.1.2 Beoordelen van het informatiebeveiligings- en privacybeleid	Het beleid voor informatiebeveiliging en privacy moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is	1	1	Verplicht voor uitvoering ISMS
		Totals:		2	2	
A.6 Organisatie van informatiebeveiliging en privacy						
	A.6.1 Internal organization	A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging en privacy	Alle verantwoordelijkheden bij informatiebeveiliging en privacy moeten worden gedefinieerd en toegewezen.	1	1	Risico Analyse
		A.6.1.2 Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	1	1	Risico Analyse
		A.6.1.3 Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	1	1	Wettelijke verplichtingen
		A.6.1.4 Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	1	1	Risico Analyse
		A.6.1.5 Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	1	1	Risico Analyse
	A.6.2 Mobile devices and teleworking	A.6.2.1 Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligings- en privacy maatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	1	1	Risico Analyse
		A.6.2.2 Telewerken	Beleid en ondersteunende beveiligings- en privacy maatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	1	1	Risico Analyse
		Totals:		7	7	
A.7 Veilig personeel						
	A.7.1 Prior to employment	A.7.1.1 Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	1	1	Risico Analyse
		A.7.1.2 Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging, privacy en die van de organisatie vermelden.	1	1	Risico Analyse
	A.7.2 During employment	A.7.2.1 Directieverantwoordelijkheden	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging en privacy toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	1	1	Risico Analyse

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	**Sectie**	**Beheersmaatregel**	**Maatregel omschrijving**			
		A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging en privacy	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	1	1	Risico Analyse
		A.7.2.3 Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging en/of privacy.	1	1	Risico Analyse
	A.7.3 Termination and change of employment	A.7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging en privacy die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	1	1	Risico Analyse
		Totals:		6	6	
A.8 Beheer van bedrijfsmiddelen						
	A.8.1 Responsibility for assets	A.8.1.1 Inventariseren van bedrijfsmiddelen	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	1	1	Risico Analyse
		A.8.1.2 Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	1	1	Risico Analyse
		A.8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	1	1	Risico Analyse
		A.8.1.4 Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	1	1	Risico Analyse
	A.8.2 Information classification	A.8.2.1 Classificatie van informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	1	1	Risico Analyse
		A.8.2.2 Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	1	1	Risico Analyse
		A.8.2.3 Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	1	1	Risico Analyse
	A.8.3 Media Handling	A.8.3.1 Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	1	1	Risico Analyse
		A.8.3.2 Verwijderen van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	1	1	Risico Analyse

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	Sectie	Beheersmaatregel	Maatregel omschrijving			
		A.8.3.3 Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	1	1	Risico Analyse
		Totals:		10	10	
A.9 Toegangsbeveiliging						
	A.9.1 Business requirements of access control	A.9.1.1 Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs-, informatie- en privacybeveiligingseisen.	1	1	Risico Analyse
		A.9.1.2 Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	1	1	Risico Analyse
	A.9.2 User access management	A.9.2.1 Registratie en uitschrijving van gebruikers	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	1	1	Risico Analyse
		A.9.2.2 Gebruikers toegang verlenen	Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	1	1	Risico Analyse
		A.9.2.3 Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd	1	1	Risico Analyse
		A.9.2.4 Beheer van geheime authenticatieinformatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	1	1	Risico Analyse
		A.9.2.5 Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	1	1	Risico Analyse
		A.9.2.6 Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	1	1	Risico Analyse
	A.9.3 User responsibilities	A.9.3.1 Geheime authenticatie-informatie gebruiken.	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	1	1	Risico Analyse
	A.9.4 System and application access control	A.9.4.1 Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	1	1	Risico Analyse
		A.9.4.2 Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	1	1	Risico Analyse
		A.9.4.3 Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	1	1	Risico Analyse
		A.9.4.4 Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	1	1	Risico Analyse
		A.9.4.5 Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	1	1	Risico Analyse
		Totals:		14	14	
A.10 Cryptografie						

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	Sectie	Beheersmaatregel	Maatregel omschrijving			
	A.10.1 Cryptographic controls	A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	1	1	Risico Analyse
		A.10.1.2 Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	1	1	Risico Analyse
		Totals:		2	2	
A.11 Fysieke beveiliging en beveiliging van de omgeving						
	A.11.1 Secure areas	A.11.1.1 Fysieke beveiligingszone	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	1	1	Risico Analyse
		A.11.1.2 Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	1	1	Risico Analyse
		A.11.1.3 Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	1	1	Risico Analyse
		A.11.1.4 Beschermen tegen bedreigingen van buitenaf.	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	1	1	Risico Analyse
		A.11.1.5 Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	1	1	Risico Analyse
		A.11.1.6 Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	1	1	Risico Analyse
	A.11.2 Equipment	A.11.2.1 Plaatsing en bescherming van apparatuur	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	1	1	Risico Analyse
		A.11.2.2 Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	1	1	Risico Analyse
		A.11.2.3 Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	1	1	Risico Analyse
		A.11.2.4 Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	1	1	Risico Analyse
		A.11.2.5 Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	1	1	Risico Analyse
		A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein.	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	1	1	Risico Analyse
		A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	1	1	Risico Analyse
		A.11.2.8 Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is	1	1	Risico Analyse
		A.11.2.9 'Clear desk'- en 'clear screen'-beleid	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	1	1	Risico Analyse
		Totals:		15	15	
A.12 Operations security						
	A.12.1 Operational procedures and responsibilities	A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them. (o.a. DR voor klanten)	1	1	Risico Analyse

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	Sectie	Beheersmaatregel	Maatregel omschrijving			
		A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
	A.12.2 Protection from 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.	1	1	Risico Analyse
	A.12.3 Backup	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.	1	1	Risico Analyse
	A.12.4 Logging and monitoring	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	1	1	Risico Analyse
		A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	1	1	Risico Analyse
		A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
	A.12.5 Control of operational software	A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	1	1	Risico Analyse
	A.12.6 Technical vulnerability management	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.	1	1	Risico Analyse
		A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	1	1	Risico Analyse
	A.12.7 Information systems audit considerations	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.	1	1	Risico Analyse
		Totals:		14	14	
A.13 Communications security						
	A.13.1 Network security management	A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	1	1	Risico Analyse
	A.13.2 Information transfer	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.	1	1	Risico Analyse

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	Sectie	Beheersmaatregel	Maatregel omschrijving			
		A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	1	1	Risico Analyse
		A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	1	1	Risico Analyse
		A.13.2.4 Confidentiality or nondisclosure 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.	1	1	Risico Analyse
		Totals:		7	7	
A.14 System acquisition, development and maintenance			*All the controls that are applicable in this section are based on automation and scripting of Saas and Hosting environments. These controls are NOT applicable to regular software development of Exact like, UBW, Exact Online, P2P, Payroll software or other software that is hosted on the Exact Cloud Services environments.*			
	A.14.1 Security requirements of information systems	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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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, unauthorized message duplication or replay.	1	1	Risico Analyse
	A.14.2 Security in development and support processes	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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	0	0	
		A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	1	1	Risico Analyse
		A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	1	1	Risico Analyse
	A.14.3 Test data	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.	1	1	Risico Analyse
		Totals:		12	12	
A.15 Supplier relationships						
	A.15.1 Information security in supplier relationships	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.	1	1	Risico Analyse

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	Sectie	Beheersmaatregel	Maatregel omschrijving			
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		Totals:		5	5	
A.16 Information security incident management						
	A.16.1 Management of information security incidents and improvements	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.	1	1	Risico Analyse, Wettelijke verplichtingen
		A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	1	1	Risico Analyse, Wettelijke verplichtingen
		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.	1	1	Risico Analyse, Wettelijke verplichtingen
		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.	1	1	Risico Analyse, Wettelijke verplichtingen
		A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	1	1	Risico Analyse, Wettelijke verplichtingen
		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.	1	1	Risico Analyse, Wettelijke verplichtingen
		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.	1	1	Risico Analyse, Wettelijke verplichtingen
		Totals:		7	7	

ISO/IEC 27001:2013 Statement of Applicability				Maatregel van toepassing?	Maatregel geïmplementeerd?	Reden selectie
Area	Sectie	Beheersmaatregel	Maatregel omschrijving			
A.17 Information security aspects of business continuity management						
	A.17.1 Information security continuity	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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
		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.	1	1	Risico Analyse
	A.17.2 Redundancies	A.17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	1	1	Risico Analyse
		Totals:		4	4	
A.18 Compliance						
	A.18.1 Compliance with legal and contractual 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.	1	1	Risico Analyse
		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.	1	1	Wettelijke verplichtingen
		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.	1	1	Wettelijke verplichtingen
		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.	1	1	Wettelijke verplichtingen
		A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	1	1	Wettelijke verplichtingen
	A.18.2 Information security reviews	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.	1	1	Wettelijke verplichtingen
		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.	1	1	Wettelijke verplichtingen
		A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	1	1	Wettelijke verplichtingen
		Totals:		8	8	