Nr.	Clausule	Benaming	Soort	Beschrijving	Toepasselijk	Geïmplementeerd?	Reden in/uitsluiting
	A.5	Informatiebeveiligingsb	Sectie				
	A.5.1	Aansturing door de directie van de informatiebeveiliging	Doel	Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.			
1	A.5.1.1	Beleidsregels voor informatiebeveiliging	Control	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja	Ja	Risico Analyse
2	A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	Control	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Ja	Ja	Risico Analyse
	A.6	Organiseren van informatiebeveiliging	Sectie				
	A.6.1	Interne organisatie	Doel	Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.			
3	A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Control	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	Ja	Risico Analyse
4	A.6.1.2	Scheiding van taken	Control	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.	Ja	Ja	Risico Analyse
5	A.6.1.3	Contact met overheidsinstanties	Control	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Ja	Ja	Risico Analyse
6	A.6.1.4	Contact met speciale belangengroepen	Control	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	Ja	Ja	Risico Analyse
7	A.6.1.5	Informatiebeveiliging in projectbeheer	Control	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Ja	Ja	Risico Analyse
	A.6.2	Mobiele apparatuur en telewerken	Doel	Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.			
8	A.6.2.1	Beleid voor mobiele apparatuur	Control	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Ja	Ja	Risico Analyse
9	A.6.2.2	Telewerken	Control	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	Ja	Ja	Risico Analyse
	A.7	Veilig personeel	Sectie				
	A.7.1	Voorafgaand aan dienstverband	Doel	Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.			
10	A.7.1.1	Screening	Control	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.	Ja	Ja	Risico Analyse
11	A.7.1.2	Arbeidsvoorwaarden	Control	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Ja	Risico Analyse
	A.7.2	Tijdens het dienstverband	Doel	Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.			
12	A.7.2.1	Directieverantwoordelijkheden	Control	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Ja	Ja	Best Practices / Bedrijfseisen
13	A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Control	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.	Ja	Ja	Risico Analyse
14	A.7.2.3	Disciplinaire procedure	Control	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Ja	Ja	Risico Analyse
	A.7.3	Beëindiging en wijziging van dienstverband	Doel	Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.			
15	A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Control	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging 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.	Ja	Ja	Risico Analyse
	A.8	Beheer van bedrijfsmiddelen	Sectie				

	A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen	Doel	Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.			
16	A.8.1.1	Inventariseren van bedrijfsmiddelen	Control	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Ja	Ja	Risico Analyse
17	A.8.1.2	Eigendom van bedrijfsmiddelen	Control	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Ja	Ja	Risico Analyse
18	A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Control	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja	Risico Analyse
19	A.8.1.4	Teruggeven van bedrijfsmiddelen	Control	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.	Ja	Ja	Risico Analyse
	A.8.2	Informatieclassificatie	Doel	Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.			
20	A.8.2.1	Classificatie van informatie	Control	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Ja	Ja	Risico Analyse
21	A.8.2.2	Informatie labelen	Control	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja	Risico Analyse
22	A.8.2.3	Behandelen van bedrijfsmiddelen	Control	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja	Risico Analyse
	A.8.3	Behandelen van media	Doel	Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.			
23	A.8.3.1	Beheer van verwijderbare media	Control	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	Ja	Risico Analyse
24	A.8.3.2	Verwijderen van media	Control	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures	Ja	Ja	Risico Analyse
25	A.8.3.3	Media fysiek overdragen	Control	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	Ja	Risico Analyse
	A.9	Toegangsbeveiliging	Sectie				
	A.9.1	Bedrijfseisen voor toegangsbeveiliging	Doel	Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.			
26	A.9.1.1	Beleid voor toegangsbeveiliging	Control	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	Ja	Risico Analyse
27	A.9.1.2	Toegang tot netwerken en netwerkdiensten	Control	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Ja	Ja	Risico Analyse
	A.9.2	Beheer van toegangsrechten van gebruikers	Doel	Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.			
28	A.9.2.1	Registratie en uitschrijving van gebruikers	Control	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Ja	Risico Analyse
29	A.9.2.2	Gebruikers toegang verlenen	Control	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.	Ja	Ja	Risico Analyse
30	A.9.2.3	Beheren van speciale toegangsrechten	Control	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Ja	Ja	Risico Analyse
31	A.9.2.4	Beheer van geheime authenticatieinformatie van gebruikers	Control	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Ja	Ja	Risico Analyse
32	A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Control	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Ja	Ja	Risico Analyse
33	A.9.2.6	Toegangsrechten intrekken of aanpassen	Control	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.	Ja	Ja	Risico Analyse
	A.9.3	Gebruikersverantwoordelijkheden	Doel	Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.			
34	A.9.3.1	Geheime authenticatie-informatie gebruiken	Control	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Ja	Ja	Risico Analyse
	A.9.4	Toegangsbeveiliging van systeem en toepassing	Doel	Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.			
35	A.9.4.1	Beperking toegang tot informatie	Control	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Ja	Ja	Risico Analyse
36	A.9.4.2	Beveiligde inlogprocedures	Control	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Ja	Ja	Risico Analyse
37	A.9.4.3	Systeem voor wachtwoordbeheer	Control	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Ja	Ja	Risico Analyse
38	A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Control	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Ja	Risico Analyse
39	A.9.4.5	Toegangsbeveiliging op programmabroncode	Control	Toegang tot de programmabroncode moet worden beperkt.	Ja	Ja	Risico Analyse
	A.10	Cryptografie	Sectie				

	A.10.1	Cryptografische beheersmaatregelen	Doel	Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.			
40	A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Control	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja	Risico Analyse
41	A.10.1.2	Sleutelbeheer	Control	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Ja	Ja	Risico Analyse
	A.11	Fysieke beveiliging en beveiliging van de omgeving	Sectie				
	A.11.1	Beveiligde gebieden	Doel	Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.			
42	A.11.1.1	Fysieke beveiligingszone	Control	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Ja	Ja	Risico Analyse
43	A.11.1.2	Fysieke toegangsbeveiliging	Control	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	Risico Analyse
44	A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Control	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Ja	Ja	Risico Analyse
45	A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Control	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Ja	Ja	Risico Analyse
46	A.11.1.5	Werken in beveiligde gebieden	Control	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Ja	Ja	Risico Analyse
47	A.11.1.6	Laad- en loslocatie	Control	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.	Nee	Nee	Overig
	A.11.2	Apparatuur	Doel	Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.			
48	A.11.2.1	Plaatsing en bescherming van apparatuur	Control	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Ja	Ja	Risico Analyse
49	A.11.2.2	Nutsvoorzieningen	Control	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja	Ja	Risico Analyse
50	A.11.2.3	Beveiliging van bekabeling	Control	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja	Risico Analyse
51	A.11.2.4	Onderhoud van apparatuur	Control	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	Ja	Ja	Risico Analyse
52	A.11.2.5	Verwijdering van bedrijfsmiddelen	Control	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Ja	Risico Analyse
53	A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Control	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.	Ja	Ja	Risico Analyse
54	A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Control	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.	Ja	Ja	Risico Analyse
55	A.11.2.8	Onbeheerde gebruikersapparatuur	Control	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja	Ja	Risico Analyse
56	A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Control	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Ja	Ja	Risico Analyse
	A.12	Beveiliging bedrijfsvoering	Sectie				
	A.12.1	Bedieningsprocedures en verantwoordelijkheden	Doel	Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.			
57	A.12.1.1	Gedocumenteerde bedieningsprocedures	Control	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Ja	Ja	Risico Analyse
58	A.12.1.2	Wijzigingsbeheer	Control	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	Ja	Ja	Risico Analyse
59	A.12.1.3	Capaciteitsbeheer	Control	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Ja	Ja	Risico Analyse
60	A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Control	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	Ja	Risico Analyse
	A.12.2	Bescherming tegen malware	Doel	Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.			
61	A.12.2.1	Beheersmaatregelen tegen malware	Control	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	Ja	Risico Analyse
	A.12.3	Back-up	Doel	Doelstelling: Beschermen tegen het verlies van gegevens.			

62	A.12.3.1	Back-up van informatie	Control	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Ja	Ja	Risico Analyse
	A.12.4	Verslaglegging en monitoring	Doel	Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.			
63	A.12.4.1	Gebeurtenissen registreren	Control	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Ja	Ja	Risico Analyse
64	A.12.4.2	Beschermen van informatie in logbestanden	Control	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Ja	Risico Analyse
65	A.12.4.3	Logbestanden van beheerders en operators	Control	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	Ja	Ja	Risico Analyse
66	A.12.4.4	Kloksynchronisatie	Control	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	Ja	Ja	Risico Analyse
	A.12.5	Beheersing van operationele software	Doel	Doelstelling: De integriteit van operationele systemen waarborgen.			
67	A.12.5.1	Software installeren op operationele systemen	Control	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Ja	Ja	Risico Analyse
	A.12.6	Beheer van technische kwetsbaarheden	Doel	Doelstelling: Benutting van technische kwetsbaarheden voorkomen.			
68	A.12.6.1	Beheer van technische kwetsbaarheden	Control	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	Ja	Ja	Risico Analyse
69	A.12.6.2	Beperkingen voor het installeren van software	Control	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Ja	Ja	Risico Analyse
	A.12.7	Overwegingen betreffende audits van informatiesystemen	Doel	Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.			
70	A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Control	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Ja	Ja	Risico Analyse
	A.13	Communicatiebeveiliging	Sectie				
	A.13.1	Beheer van netwerkbeveiliging	Doel	Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.			
71	A.13.1.1	Beheersmaatregelen voor netwerken	Control	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	Risico Analyse
72	A.13.1.2	Beveiliging van netwerkdiensten	Control	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Ja	Ja	Risico Analyse
73	A.13.1.3	Scheiding in netwerken	Control	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Ja	Ja	Risico Analyse
	A.13.2	Informatietransport	Doel	Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.			
74	A.13.2.1	Beleid en procedures voor informatietransport	Control	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Ja	Ja	Risico Analyse
75	A.13.2.2	Overeenkomsten over informatietransport	Control	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	Ja	Risico Analyse
76	A.13.2.3	Elektronische berichten	Control	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	Ja	Ja	Risico Analyse
77	A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Control	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Ja	Ja	Risico Analyse
	A.14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Sectie				
	A.14.1	Beveiligingseisen voor informatiesystemen	Doel	Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.			
78	A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	Control	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	Ja	Risico Analyse
79	A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Control	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Ja	Ja	Risico Analyse
80	A.14.1.3	Transacties van toepassingsdiensten beschermen	Control	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Ja	Ja	Risico Analyse
	A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	Doel	Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.			

81	A.14.2.1	Beleid voor beveiligd ontwikkelen	Control	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Ja	Ja	Risico Analyse
82	A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Control	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	Ja	Ja	Risico Analyse
83	A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Control	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Ja	Ja	Risico Analyse
84	A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Control	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Ja	Ja	Risico Analyse
85	A.14.2.5	Principes voor engineering van beveiligde systemen	Control	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Ja	Ja	Risico Analyse
86	A.14.2.6	Beveiligde ontwikkelomgeving	Control	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Ja	Ja	Risico Analyse
87	A.14.2.7	Uitbestede softwareontwikkeling	Control	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Nee	Nee	
88	A.14.2.8	Testen van systeembeveiliging	Control	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Ja	Ja	Risico Analyse
89	A.14.2.9	Systeemacceptatietests	Control	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Ja	Ja	Risico Analyse
	A.14.3	Testgegevens	Doel	Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.			
90	A.14.3.1	Bescherming van testgegevens	Control	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Ja	Ja	Risico Analyse
	A.15	Leveranciersrelaties	Sectie				
	A.15.1	Informatiebeveiliging in leveranciersrelaties	Doel	Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.			
91	A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Control	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	Ja	Ja	Risico Analyse
92	A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Control	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Ja	Ja	Risico Analyse
93	A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Control	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Ja	Ja	Risico Analyse
	A.15.2	Beheer van dienstverlening van leveranciers	Doel	Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.			
94	A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Control	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Ja	Ja	Risico Analyse
95	A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Control	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Ja	Ja	Risico Analyse
	A.16	Beheer van informatiebeveiligingsincidenten	Sectie				
	A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	doel	Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.			
96	A.16.1.1	Verantwoordelijkheden en procedures	Control	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Ja	Ja	Risico Analyse
97	A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Control	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	Ja	Risico Analyse
98	A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Control	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Ja	Ja	Risico Analyse
99	A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Control	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja	Ja	Risico Analyse
100	A.16.1.5	Respons op informatiebeveiligingsincidenten	Control	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Risico Analyse
101	A.16.1.6	Lering uit informatiebeveiligingsincidenten	Control	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja	Ja	Risico Analyse

102	A.16.1.7	Verzamelen van bewijsmateriaal	Control	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Ja	Ja	Risico Analyse
	A.17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Sectie				
	A.17.1	Informatiebeveiligingscontinuïteit	Doel	Doelstelling: Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.			
103	A.17.1.1	Informatiebeveiligingscontinuïteit plannen	Control	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Ja	Ja	Risico Analyse
104	A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	Control	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Ja	Ja	Risico Analyse
105	A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Control	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja	Ja	Risico Analyse
	A.17.2	Redundante componenten	Doel	Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.			
106	A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Control	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	Risico Analyse
	A.18	Naleving	Sectie				
	A.18.1	Naleving van wettelijke en contractuele eisen	Doel	Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.			
107	A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Control	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja	Ja	Wet- en regelgeving
108	A.18.1.2	Intellectuele eigendomsrechten	Control	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectueleeigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Ja	Ja	Wet- en regelgeving
109	A.18.1.3	Beschermen van registraties	Control	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	Ja	Wet- en regelgeving
110	A.18.1.4	Privacy en bescherming van persoonsgegevens	Control	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Ja	Ja	Wet- en regelgeving
111	A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Control	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja	Ja	Best Practices / Bedrijfseisen
	A.18.2	Informatiebeveiligingsbeoordelingen	Doel	Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.			
112	A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	Control	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	Ja	Ja	Best Practices / Bedrijfseisen
113	A.18.2.2	Naleving van beveiligingsbeleid en -normen	Control	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja	Ja	Best Practices / Bedrijfseisen
114	A.18.2.3	Beoordeling van technische naleving	Control	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Ja	Ja	Best Practices / Bedrijfseisen