	Norm	Maatregel	Van toepassing	Geïmplementeerd	Verantwoording toepasselijkheid: IRA	Verantwoording toepasselijkheid: wet/contract en regelgeving	Reden van uitsluiting
A.5 Informatiebeveiligingsbeleid							
A.5.1 Aansturing door de directie van de informatiebeveiliging							
Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.							
A.5.1.1	Beleidsregels voor informatiebeveiliging	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.6 Organiseren van informatiebeveiliging							
A.6.1 Interne organisatie							
Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.							
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	*Beheersmaatregel Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.6.1.2	Scheiding van taken	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.6.1.3	Contact met overheidsinstanties	*Beheersmaatregel Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.6.1.4	Contact met speciale belangengroepen	*Beheersmaatregel Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.6.1.5	Informatiebeveiliging in projectbeheer	*Beheersmaatregel Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.6.2 Mobiele apparatuur en telewerken							
Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.							
A.6.2.1	Beleid voor mobiele apparatuur	*Beheersmaatregel Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.6.2.2	Telewerken	*Beheersmaatregel Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.7 Veilig personeel							
A.7.1 Voorafgaand aan het dienstverband							
Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.							
A.7.1.1	Screening	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.7.1.2	Arbeidsvoorwaarden	*Beheersmaatregel De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.7.2 Tijdens het dienstverband							
Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.							
A.7.2.1	Directieverantwoordelijkheden	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.

A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.7.2.3	Disciplinaire procedure	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.7.3 Beëindiging en wijziging van dienstverband							
Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.							
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.8 Beheer van bedrijfsmiddelen							
A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen							
Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.							
A.8.1.1	Inventariseren van bedrijfsmiddelen	*Beheersmaatregel Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.8.1.2	Eigendom van bedrijfsmiddelen	*Beheersmaatregel Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.

A.8.1.4	Teruggeven van bedrijfsmiddelen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.8.2 Informatieclassificatie							
Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.							
A.8.2.1	Classificatie van informatie	*Beheersmaatregel Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.8.2.2	Informatie labelen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.8.2.3	Behandelen van bedrijfsmiddelen	*Beheersmaatregel Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.8.3 Behandelen van media							
Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.							
A.8.3.1	Beheer van verwijderbare media	*Beheersmaatregel Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.8.3.2	Verwijderen van media	*Beheersmaatregel Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.8.3.3	Media fysiek overdragen	*Beheersmaatregel Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9 Toegangsbeveiliging							
A.9.1 Bedrijfseisen voor toegangsbeveiliging							
Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.							

A.9.1.1	Beleid voor toegangsbeveiliging	*Beheersmaatregel Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.1.2	Toegang tot netwerken en netwerkdiensten	*Beheersmaatregel Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.2 Beheer van toegangsrechten van gebruikers							
Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.							
A.9.2.1	Registratie en uitschrijving van gebruikers	*Beheersmaatregel Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.2.2	Gebruikers toegang verlenen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.9.2.3	Beheren van speciale toegangsrechten	*Beheersmaatregel Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	*Beheersmaatregel Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	*Beheersmaatregel Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.2.6	Toegangsrechten intrekken of aanpassen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.9.3 Gebruikersverantwoordelijkheden							
Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.							

A.9.3.1	Geheime authenticatie-informatie gebruiken	*Beheersmaatregel Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.4 Toegangsbeveiliging van systeem en toepassing							
Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.							
A.9.4.1	Beperking toegang tot informatie	*Beheersmaatregel Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.4.2	Beveiligde inlogprocedures	*Beheersmaatregel Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.4.3	Systeem voor wachtwoordbeheer	*Beheersmaatregel Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.9.4.5	Toegangsbeveiliging op programmabroncode	*Beheersmaatregel Toegang tot de programmabroncode moet worden beperkt.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.10 Cryptografie							
A.10.1 Cryptografische beheersmaatregelen							
Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.			Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	*Beheersmaatregel Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.10.1.2	Sleutelbeheer	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.11 Fysieke beveiliging en beveiliging van de omgeving							
A.11.1 Beveiligde gebieden							

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.							
A.11.1.1	Fysieke beveiligingszone	*Beheersmaatregel Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.1.2	Fysieke toegangsbeveiliging	*Beheersmaatregel Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	*Beheersmaatregel Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	*Beheersmaatregel Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.1.5	Werken in beveiligde gebieden	*Beheersmaatregel Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.1.6	Laad- en loslocatie	*Beheersmaatregel 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.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2 Apparatuur							
Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.							
A.11.2.1	Plaatsing en bescherming van apparatuur	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.2	Nutsvoorzieningen	*Beheersmaatregel Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.11.2.3	Beveiliging van bekabeling	*Beheersmaatregel Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.4	Onderhoud van apparatuur	*Beheersmaatregel Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.5	Verwijdering van bedrijfsmiddelen	*Beheersmaatregel Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.8	Onbeheerde gebruikersapparatuur	*Beheersmaatregel Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	*Beheersmaatregel Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12 Beveiliging bedrijfsvoering							
A.12.1 Bedieningsprocedures en verantwoordelijkheden							
Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.							
A.12.1.1	Gedocumenteerde bedieningsprocedures	*Beheersmaatregel Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.12.1.2	Wijzigingsbeheer	*Beheersmaatregel Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.1.3	Capaciteitsbeheer	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	*Beheersmaatregel Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.2 Bescherming tegen malware							
Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.							
A.12.2.1	Beheersmaatregelen tegen malware	*Beheersmaatregel Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.3 Back-up							
Doelstelling: Beschermen tegen het verlies van gegevens.							
A.12.3.1	Back-up van informatie	*Beheersmaatregel Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.4 Verslaglegging en monitoren							
Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.							
A.12.4.1	Gebeurtenissen registreren	*Beheersmaatregel Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.4.2	Beschermen van informatie in logbestanden	*Beheersmaatregel Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.12.4.3	Logbestanden van beheerders en operators	*Beheersmaatregel Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.4.4	Kloksynchronisatie	*Beheersmaatregel De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.5 Beheersing van operationele software							
Doelstelling: De integriteit van operationele systemen waarborgen.							
A.12.5.1	Software installeren op operationele systemen	*Beheersmaatregel Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.6 Beheer van technische kwetsbaarheden							
Doelstelling: Benutting van technische kwetsbaarheden voorkomen.							
A.12.6.1	Beheer van technische kwetsbaarheden	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.12.6.2	Beperkingen voor het installeren van software	*Beheersmaatregel Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.12.7 Overwegingen betreffende audits van informatiesystemen							
Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.							
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.13 Communicatiebeveiliging							
A.13.1 Beheer van netwerkbeveiliging							
Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.							
A.13.1.1	Beheersmaatregelen voor netwerken	*Beheersmaatregel Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.13.1.2	Beveiliging van netwerkdiensten	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.13.1.3	Scheiding in netwerken	*Beheersmaatregel Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.13.2 Informatietransport							
Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.							
A.13.2.1	Beleid en procedures voor informatietransport	*Beheersmaatregel Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.13.2.2	Overeenkomsten over informatietransport	*Beheersmaatregel Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.13.2.3	Elektronische berichten	*Beheersmaatregel Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen							
A.14.1 Beveiligingseisen voor informatiesystemen							
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.							
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	*Beheersmaatregel De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.14.1.3	Transacties van toepassingsdiensten beschermen	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen							
Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.							
A.14.2.1	Beleid voor beveiligd ontwikkelen	*Beheersmaatregel Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	*Beheersmaatregel Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	*Beheersmaatregel Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.5	Principes voor engineering van beveiligde systemen	*Beheersmaatregel Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

A.14.2.6	Beveiligde ontwikkelomgeving	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.7	Uitbestede softwareontwikkeling [1]	*Beheersmaatregel Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.8	Testen van systeembeveiliging	*Beheersmaatregel Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.14.2.9	Systeemacceptatietests	*Beheersmaatregel Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.14.3 Testgegevens							
Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.							
A.14.3.1	Bescherming van testgegevens	*Beheersmaatregel Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.15 Leveranciersrelaties							
A.15.1 Informatiebeveiliging in leveranciersrelaties							
Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.							
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.

A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.15.2 Beheer van dienstverlening van leveranciers			Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.			Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	*Beheersmaatregel Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.16 Beheer van informatiebeveiligingsincidenten							
A.16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen							
Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.							
A.16.1.1	Verantwoordelijkheden en procedures	*Beheersmaatregel Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	*Beheersmaatregel Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.

A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	*Beheersmaatregel* *Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.16.1.5	Respons op informatiebeveiligingsincidenten	*Beheersmaatregel* *Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.16.1.6	Lering uit informatiebeveiligingsincidenten	*Beheersmaatregel* *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	Integrale risico analyse	N.V.T.	N.V.T.
A.16.1.7	Verzamelen van bewijsmateriaal	*Beheersmaatregel* *De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer							
A.17.1 Informatiebeveiligingscontinuïteit							
Doelstelling: Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.							
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	*Beheersmaatregel* *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	Integrale risico analyse	N.V.T.	N.V.T.
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	*Beheersmaatregel* *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	Integrale risico analyse	N.V.T.	N.V.T.
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	*Beheersmaatregel* *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	Integrale risico analyse	N.V.T.	N.V.T.
A.17.2 Redundantecomponenten			Ja	Ja	Integrale risico analyse		

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.			Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	*Beheersmaatregel Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
A.18 Naleving							
A.18.1 Naleving van wettelijke en contractuele eisen							
Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.							
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	*Beheersmaatregel 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	Integrale risico analyse	Wet en regelgeving	N.V.T.
A.18.1.2	Intellectuele eigendomsrechten	*Beheersmaatregel Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele- eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.*	Ja	Ja	Integrale risico analyse	Wet en regelgeving	N.V.T.
A.18.1.3	Beschermen van registraties	*Beheersmaatregel Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.*	Ja	Ja	Integrale risico analyse	Wet en regelgeving	N.V.T.
A.18.1.4	Privacy en bescherming van persoonsgegevens	*Beheersmaatregel Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.*	Ja	Ja	Integrale risico analyse	Wet en regelgeving	N.V.T.
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	*Beheersmaatregel Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.*	Ja	Ja	Integrale risico analyse	Wet en regelgeving	N.V.T.
A.18.2 Informatiebeveiligingsbeoordelingen							
Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.							

A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	*Beheersmaatregel 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	Integrale risico analyse	N.V.T.	N.V.T.
A.18.2.2	Naleving van beveiligingsbeleid en -normen	*Beheersmaatregel leidinggevenden moeten 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	Integrale risico analyse	N.V.T.	N.V.T.
A.18.2.3	Beoordeling van technische naleving	*Beheersmaatregel Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.*	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

[1] Voor krachtplan app worden externe developpers gebruikt