SURF	***ISO 27001 Verklaring van Toepasselijkheid / Statement of Applicability***
Reikwijdte	*"Leveren van computing, data opslag en -analyse, visualisatie, authenticatie, autorisatie, cloud en grid diensten zoals vastgesteld door het management en in overeenstemming met de Verklaring van Toepasselijkheid versie 6.0., dd. 10 oktober 2022."*
Datum	*24 oktober 2016*
Herzien op	*10 oktober 2022*
Versie	*6.0*

Risiconiveau	
Kritiek	Beheersen
Hoog	Beheersen
Medium	Geaccepteerd
Laag	Geaccepteerd

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
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	*Control* Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja		Geïmplementeerd	Best practice maatregel
A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid	*Control* Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Ja		Geïmplementeerd	Best practice maatregel
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	*Control* Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Ja	R5, R6, R66, R7	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.6.1.2	Scheiding van taken	*Control* Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Ja		Geïmplementeerd	Best practice maatregel
A.6.1.3	Contact met overheidsinstanties	*Control* Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	Ja	R64	Geïmplementeerd	Best practice maatregel
A.6.1.4	Contact met speciale belangengroepen	*Control* Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.	Ja	R66	Geïmplementeerd	Best practice maatregel
A.6.1.5	Informatiebeveiliging in projectbeheer	*Control* Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Ja	R8, R54, R58	Geïmplementeerd	Best practice maatregel
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	*Control* Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Ja	R72, R46	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.6.2.2	Telewerken	*Control* Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Ja	R46, R47	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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 rollen waarvoor zij in aanmerking komen.						
A.7.1.1	Screening	*Control* Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	Ja	R67	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.7.1.2	Arbeidsvoorwaarden	*Control* De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Ja	R64	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Ja	R64	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	*Control* All employees of the organization and, where relevant, contrac- tors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Ja	R12, R10	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.7.2.3	Disciplinaire procedure	*Control* Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Ja	R72, R62, R64	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.7.3 Beëindiging en wijziging van dienstverband						

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
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	*Control* Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	Ja	R68	Geïmplementeerd	Best practice maatregel
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	*Control* Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	Ja		Geïmplementeerd	Verplicht document
A.8.1.2	Eigendom van bedrijfsmiddelen	*Control* Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	Ja	R68	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmi	*Control* Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja		Geïmplementeerd	Verplicht document
A.8.1.4	Teruggeven van bedrijfsmiddelen	*Control* Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	Ja	R68	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Ja	R62, R66	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.8.2.2	Informatie labelen	*Control* Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	R66	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.8.2.3	Behandelen van bedrijfsmiddelen	*Control* Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja		Geïmplementeerd	Best practice maatregel
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	*Control* Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	R72, R62, R60	Geïmplementeerd	Best practice maatregel
A.8.3.2	Verwijderen van media	*Control* Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Ja		Geïmplementeerd	Verplicht document
A.8.3.3	Media fysiek overdragen	*Control* Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Ja	R72, R62	Geïmplementeerd	Best practice maatregel
A.9 Toegangsbeveiliging						
A.9.1 Bedrijfseisen voor toegangsbeveiliging						
Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.						
A.9.1.1	Beleid voor toegangsbeveiliging	*Control* Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	R68	Geïmplementeerd	Verplicht document
A.9.1.2	Toegang tot netwerken en netwerkdiensten	*Control* Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Ja	R10, R68	Geïmplementeerd	Best practice maatregel
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 afmelden van gebruikers	*Control* Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	R68	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.9.2.2	Gebruikers toegang verlenen	*Control* Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Ja	R68	Geïmplementeerd	Best practice maatregel
A.9.2.3	Beheren van speciale toegangsrechten	*Control* Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Ja	R65, R68	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	*Control* Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst	Ja	R10, R68	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	*Control* Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers	Ja	R68	Geïmplementeerd	Best practice maatregel
A.9.2.6	Toegangsrechten intrekken of aanpassen	*Control* De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Ja	R68	Geïmplementeerd	Best practice maatregel
A.9.3 Verantwoordelijkheden van gebruikers						
Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatieinformatie.						

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
A.9.3.1	Geheime authenticatie-informatie gebruiken	*Control* Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatieinformatie houden aan de praktijk van de organisatie.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.9.4 Toegangsbeveiliging van systeem en toepassing						
Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.						
A.9.4.1	Beperking toegang tot informatie	*Control* Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Ja		Geïmplementeerd	Best practice maatregel
A.9.4.2	Beveiligde inlogprocedures	*Control* Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.9.4.3	Systeem voor wachtwoordbeheer	*Control* Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	*Control* Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	Ja	R68	Geïmplementeerd	Best practice maatregel
A.9.4.5	Toegangsbeveiliging op programmabroncode	*Control* Toegang tot de programmabroncode behoort te worden beperkt.	Ja		Geïmplementeerd	Best practice maatregel
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.						
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	*Control* Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Ja	R72, R62, R59	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.10.1.2	Sleutelbeheer	*Control* Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.11.1.2	Fysieke toegangsbeveiliging	*Control* Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	*Control* Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Ja	R67	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	*Control* Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Ja		Geïmplementeerd	Best practice maatregel
A.11.1.5	Werken in beveiligde gebieden	*Control* Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Ja		Geïmplementeerd	Best practice maatregel
A.11.1.6	Laad- en loslocatie	*Control* Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Ja		Geïmplementeerd	Best practice maatregel
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	*Control* Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Ja		Geïmplementeerd	Best practice maatregel
A.11.2.2	Nutsvoorzieningen	*Control* Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Ja		Geïmplementeerd	Best practice maatregel
A.11.2.3	Beveiliging van bekabeling	*Control* Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Ja	R62	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.11.2.4	Onderhoud van apparatuur	*Control* Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Ja		Geïmplementeerd	Best practice maatregel
A.11.2.5	Verwijdering van bedrijfsmiddelen	*Control* Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Ja		Geïmplementeerd	Best practice maatregel
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	*Control* Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Ja	R72	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	*Control* Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Ja		Geïmplementeerd	Best practice maatregel

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
A.11.2.8	Onbeheerde gebruikersapparatuur	*Control* Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	*Control* Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	Ja	R12	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Ja	R55, R65, R8,	Geïmplementeerd	Verplicht document
A.12.1.2	Wijzigingsbeheer	*Control* Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Ja	R8, R52	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.1.3	Capaciteitsbeheer	*Control* Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Ja	R49, R8	Geïmplementeerd	Best practice maatregel
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	*Control* Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	R52, R68	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.2 Bescherming tegen malware						
Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.						
A.12.2.1	Beheersmaatregelen tegen malware	*Control* Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	R22, R46, R10, R47	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.3 Back-up						
Doelstelling: Beschermen tegen het verlies van gegevens.						
A.12.3.1	Back-up van informatie	*Control* Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Ja	R65, R10, R52, R60	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.4 Verslaglegging en monitoren						
Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.						
A.12.4.1	Gebeurtenissen registreren	*Control* Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Ja		Geïmplementeerd	Verplicht document
A.12.4.2	Beschermen van informatie in logbestanden	*Control* Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	R22	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.4.3	Logbestanden van beheerders en operators	*Control* Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Ja		Geïmplementeerd	Verplicht document
A.12.4.4	Kloksynchronisatie	*Control* De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.5 Beheersing van operationele software						
Doelstelling: De integriteit van operationele systemen waarborgen						
A.12.5.1	Software installeren op operationele systemen	*Control* Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Ja	R54	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.6 Beheer van technische kwetsbaarheden						
Doelstelling: Benutting van technische kwetsbaarheden voorkomen.						
A.12.6.1	Beheer van technische kwetsbaarheden	*Control* Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	Ja	R22	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.12.6.2	Beperkingen voor het installeren van software	*Control* Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Ja	R52	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	R46, R47	Geïmplementeerd	Geselecteerd als onderdeel van de RA

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
A.13.1.2	Beveiliging van netwerkdiensten	*Control* Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Ja	R46, R47	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.13.1.3	Scheiding in netwerken	*Control* Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Ja	R22, R46, R10,	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Ja	R59	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.13.2.2	Overeenkomsten over informatietransport	*Control* Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Ja	R59	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.13.2.3	Elektronische berichten	*Control* Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	Ja		Geïmplementeerd	Best practice maatregel
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, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	Ja	R72, R67	Geïmplementeerd	Verplicht document
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						
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	*Control* De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	R54	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.1.2	Toepassingen op openbare netwerken beveiligen	*Control* Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Ja	R59	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.1.3	Transacties van toepassingen beschermen	*Control* Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*Control* Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	*Control* Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Ja	R22, R8, R54, R52	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	*Control* Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Ja	R54, R52	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	*Control* Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.2.5	Principes voor engineering van beveiligde systemen	*Control* Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Ja	R8	Geïmplementeerd	Verplicht document
A.14.2.6	Beveiligde ontwikkelomgeving	*Control* Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.2.7	Uitbestede softwareontwikkeling	*Control* Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Nee		SURF besteedt geen software ontwikkeling uit	
A.14.2.8	Testen van systeembeveiliging	*Control* Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.2.9	Systeemacceptatietests	*Control* Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Ja	R54	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.14.3 Testgegevens						
Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.						
A.14.3.1	Bescherming van testgegevens	*Control* Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.15 Leveranciersrelaties						
A.15.1 Informatiebeveiliging in leveranciersrelaties						
Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.						

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	*Control* Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	Ja	R59, R8, R47	Geïmplementeerd	Verplicht document
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	*Control* Alle relevante informatiebeveiligingseisen behoren te 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	R49, R8, R67, R47	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	*Control* Overeenkomsten met leveranciers behoren eisen te 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	R54	Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.15.2 Beheer van dienstverlening van leveranciers						
Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.						
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	*Control* Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Ja	R22, R8	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Ja	R55, R8, R58	Geïmplementeerd	Geselecteerd als onderdeel van de RA
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						
A.16.1.1	Verantwoordelijkheden en procedures	*Control* Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	*Control* Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Ja		Geïmplementeerd	Best practice maatregel
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 behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Ja		Geïmplementeerd	Best practice maatregel
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	*Control* Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.16.1.5	Respons op informatiebeveiligingsincidenten	*Control* Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.16.1.6	Lering uit informatiebeveiligingsincidenten	*Control* Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Ja		Geïmplementeerd	Best practice maatregel
A.16.1.7	Verzamelen van bewijsmateriaal	*Control* De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer						
A.17.1 Informatiebeveiligingscontinuïteit						
Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.						
A.17.1.1	Informatiebeveiligingscontinuïteit plannen	*Control* De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	*Control* De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Ja		Geïmplementeerd	Verplicht document
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	*Control* De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Ja		Geïmplementeerd	Best practice maatregel
A.17.2 Redundante componenten						
Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.						
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	*Control* Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	R49	Geïmplementeerd	Best practice maatregel
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	*Control* Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja		Geïmplementeerd	Verplicht document

ISO 27001: 2013			Van toepassing	RA RID	Implementatie	Toelichting
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 behoren passende procedures te worden geïmplementeerd.	Ja		Geïmplementeerd	Wet- en regelgeving, Auteursrecht
A.18.1.3	Beschermen van registraties	*Control* Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Ja	R60	Geïmplementeerd	Wet- en regelgeving, Wet op rijksbelastingen
A.18.1.4	Privacy en bescherming van persoonsgegevens	*Control* Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Ja		Geïmplementeerd	Wet- en Regelgeving, AVG
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	*Control* Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Ja		Geïmplementeerd	Geselecteerd als onderdeel van de RA
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	*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), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	Ja		Geïmplementeerd	Onlosmakelijk verbonden met de norm
A.18.2.2	Naleving van beveiligingsbeleid en -normen	*Control* De directie behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja		Geïmplementeerd	Onlosmakelijk verbonden met de norm
A.18.2.3	Beoordeling van technische naleving	*Control* Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Ja	R60	Geïmplementeerd	Geselecteerd als onderdeel van de RA