

Bron	Control	Nummer	Maatregel	BBN1	Verplicht	B	I	V	Dekt risico's af op	Proceseigenaar	Dienstenleverancier
BIO 1.04	Scheiding van taken: Conflicterende taken en verantwoordelijkheden	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	x	ja		x	x	Organisatie	x	x
BIO 1.04	Beheer van verwijderbare media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is (ISO 27002 – implementatierichtlijn 8.3.1.a).	x	ja			x	Gegevens	x	x
BIO 1.04	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	x	ja	x	x	x	Programmatuur	x	x
BIO 1.04	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	x	ja	x	x	x	Programmatuur	x	x
BIO 1.04	Gebruikers toegang verlenen: 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.	9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	x	ja		x	x	Programmatuur	x	x
BIO 1.04	Gebruikers toegang verlenen: 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.	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	x	ja		x	x	Organisatie	x	x

BIO 1.04	Gebruikers toegang verlenen: 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.	9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	x	ja		x	x	Organisatie	x	x
BIO 1.04	Beheren van speciale toegangsrechten: Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	x	ja		x	x	Organisatie	x	x
BIO 1.04	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	x	ja		x	x	Organisatie	x	x
BIO 1.04	Beperking toegang tot informatie: Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	9.4.1.2	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	x	ja		x	x	Organisatie	x	x
BIO 1.04	Beveiligde inlogprocedures: Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	x	ja			x	Programmatuur	x	x
BIO 1.04	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.	x	ja	x	x	x	Omgeving	x	x

BIO 1.04	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	11.1.4.1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	x	ja	x			Omgeving	x	x
BIO 1.04	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	x	ja	x			Omgeving	x	x
BIO 1.04	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	x	ja	x	x		Gegevens	x	x
BIO 1.04	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	12.1.4.2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	x	ja	x	x		Programmatuur	x	x
BIO 1.04	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	x	ja	x			Organisatie	x	x

BIO 1.04	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	x	ja	x			Organisatie	x	x
BIO 1.04	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	x	ja	x	x	x	Programmatuur	x	x
BIO 1.04	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	x	ja	x	x	x	Programmatuur	x	x
BIO 1.04	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	14.2.8.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	x	ja		x		Programmatuur	x	x

BIO 1.04	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	14.2.8.2	Van de resultaten van de testen wordt verslag gemaakt.	x	ja	x	x	x	Programmatuur	x	x
BIO 1.04	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: 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.	15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	x	ja	x	x	x	Diensten	x	x
BIO 1.04	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: 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.	15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	x	ja	x	x	x	Diensten	x	x
BIO 1.04	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: 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.	15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	x	ja	x	x	x	Diensten	x	x

BIO 1.04	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: 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.	15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	x	ja			x	Diensten	x	x
BIO 1.04	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: 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.	15.1.2.5	Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	x	ja	x			Diensten	x	x
BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	x	ja	x	x	x	Mens	x	x

BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.4	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.7	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage (Voorheen werd Coordinated Vulnerability Disclosure (CVD) responsible disclosure genoemd.).	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Rapportage van zwakke plekken in de informatiebeveiliging: 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	16.1.3.1	Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht (voorheen werd Coordinated Vulnerability Disclosure (CVD) responsible disclosure genoemd).	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Verzamelen van bewijsmateriaal: De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	x	ja	x	x	x	Organisatie	x	x

BIO 1.04	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	x	ja			x	Organisatie	x	x
BIO 1.04	Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	18.2.1.1	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	x	ja	x	x	x	Organisatie	x	x
BIO 1.04	Naleving van beveiligingsbeleid en -normen: 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.	18.2.2.1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	x	ja	x	x	x	Organisatie	x	x