Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Fysiek	0 / Entry	7.1	Fysieke beveiligingszone	Worden er beveiligingszones gehanteerd?	Fysieke beveiligingsmaatregelen zijn niet tot nauwelijks in stelling gebracht en er zijn geen formele beleidsregels. De organisatie is niet in staat diefstal of aanvallen op gebouwen en bedrijfsmiddelen snel te detecteren. De organisatie is hierin afhankelijk van de scherpte en vaardigheden van individuele personen.	Er zijn zones gecreëerd o.b.v. beveiligingseisen van de daarin aanwezige bedrijfsmiddelen. Barrières en begrenzingen zijn gebaseerd op een risicobeoordeling en fysiek in orde. Hoewel mogelijk niet allesomvattend en wordt de naleving niet altijd gedetecteerd, zijn er beheersmaatregelen aanwezig, zoals bijvoorbeeld controle van fysieke toegang tot locaties/gebouwen, van alarmen voorziene branddeuren en detectiesystemen op buitendeuren en ramen.	Beveiligingszones zijn gedefinieerd en worden gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.
Organisatorisch	0 / Entry	5.1	Beleidsregels voor informatiebeveiliging en privacy	Heeft de organisatie actuele beleidsregels omtrent informatiebeveiling en privacy?	Hoewel er enkele beleidslijnen zijn, is er vooral sprake van een gangbare praktijk van handelen die niet op beleid gebaseerd is.	Het beleid is niet formeel goedgekeurd. Er is beleid op hoofdlijnen gepubliceerd met doelstellingen en uitgangspunten. Verantwoordelijkheden zijn toegekend en processen voor het behandelen van afwijkingen en uitzonderingen zijn bepaald. Het beleid op hoofdlijnen is nader uitgewerkt in onderwerpspecifieke beleidsregels die de implementatie van beheersmaatregelen voor informatiebeveiliging en privacy verplicht stellen.	Het gepubliceerde beleid op hoofdlijnen (zie L2) is goedgekeurd door de directie en tevens gecommuniceerd aan medewerkers en relevante externe partijen. Het beleid wordt periodiek beoordeeld op actualiteit én wanneer er zich een ernstig incident voordoet.
Organisatorisch	0 / Entry	5.15	Toegangsbeveiliging	Wordt toegang beheerd?	Toegang wordt verleend tot bedrijfsmiddelen, netwerken en netwerkdiensten maar deze is niet gebaseerd op beleid op basis van bedrijfs- en informatiebeveiligings-/privacyeisen.	Hoewel er een autorisatiematrix wordt gebruikt, is er sprake van een informeel toegangsbeleid.	Een beleid voor toegangsbeveiliging is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligings-/privacyeisen. Gebruikers krijgen alleen toegang tot bedrijfsmiddelen, netwerk en netwerkdiensten waarvoor zij specifiek bevoegd zijn.
Organisatorisch	0 / Entry	5.16	Registratie en uitschrijving van gebruikers	Wordt er gewerkt met gebruikersaccounts?	Gebruikersaccounts zijn aan personen gekoppeld, gedeelde accounts worden op een manier beheerd zodat onbevoegden hier geen toegang tot hebben.	Er bestaan procedures welke omschrijven hoe met accounts omgegaan wordt. Alleen bevoegden hebben aantoonbaar toegang tot accounts, of deze nu persoonlijk of gedeeld zijn. Rechten tot deze accounts worden periodiek aantoonbaar beoordeeld.	Persoonlijke gebruikersaccounts zijn alleen actief voor personen welke toegang tot de betreffende systemen of informatie moeten hebben. Gedeelde accounts worden zo beheerd dat alleen bevoegden hier toegang tot hebben. Periodiek worden alle rechten beoordeeld. Bij gebruik van accounts van derden wordt er binnen een risico analyse rekening gehouden met de risico's daarvan. Alle hierboven genoemde zaken zijn vastgelegd in procedures en aantoonbaar toegepast.
Organisatorisch	0 / Entry	5.18	Toegangsrechten	Worden toegangsrechten verleend en beheerst?	Er is geen beleid voor gebruikersaccounts en gerelateerde privileges en geen administratieprocedure voor gebruikers en toegangsgroepen (rollen). Toegangsrechten worden op ad-hoc basis verleend en ingetrokken, afhankelijk van de individuele personen. Gebruikers kunnen toegang krijgen tot meer informatie dan op basis van het 'need-to-know / have'-principe.	Er is een informeel beleid voor alle accounts en toegangsrechten (intern, extern, beheerders) en alle omstandigheden (normaal, noodgeval). Er is een beheerprocedure voor accounts en gerelateerde privileges gedefinieerd maar niet geformaliseerd. Accounts en gerelateerde toegangsrechten worden geblokkeerd / ingetrokken als een gebruiker ontslag neemt of wordt ontslagen.	Een formele gebruikerstoegangsverleningsprocedure is geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. Eigenaren van bedrijfsmiddelen beoordelen toegangsrechten van gebruikers regelmatig. De toegangsrechten van alle medewerkers en externe gebruikers worden bij beëindiging van hun dienstverband, contract of overeenkomst verwijderd, en bij wijzigingen aangepast.
Organisatorisch	0 / Entry	5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging en privacy	Heeft de organisatie verantwoordelijkheden m.b.t. informatiebeveiliging en privacy vastgesteld?	Enkele specifieke rollen zijn bekend in de organisatie ook al zijn deze niet formeel vastgesteld.	Cruciale rollen en verantwoordelijkheden voor informatiebeveiliging en privacy zijn gedefinieerd en toegewezen waaronder m.b.t. risicobeheer (incl. acceptatie van restrisico's) bescherming van faciliteiten en bedrijfsmiddelen.	Alle verantwoordelijkheden voor informatiebeveiliging en privacy zijn gedefinieerd en toegewezen. Vastgelegd is welke personen voor welke gebieden aangesteld zijn. Verantwoordelijkheden en bevoegdheden zijn voor elk organisatorisch niveau duidelijk.
Organisatorisch	0 / Entry	5.22	Monitoring van, beoordeling van en beheer van veranderingen in de dienstverlening van leveranciers	Wordt de dienstverlening van leveranciers gemanaged?	Monitoring en beoordeling van de dienstverlening vindt ad hoc plaats of reactief wanneer er zich incidenten/conflicten voordoen.	Monitoring en beoordeling van de dienstverlening vindt structureel en periodiek plaats. Er is een focus op verbetering en herbeoordeling van risico's.	De dienstverlening van leveranciers wordt regelmatig gemonitord, beoordeeld en geaudit. Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, worden beheerd, rekening houdend met het belang van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.
Organisatorisch	0 / Entry	5.29	Informatiebeveiliging in ongunstige situaties	Is de organisatie voorbereid op het beheer van beschikbaarheid, integriteit en vertrouwelijkheid van informatie tijdens calamiteiten?	Enkele ongunstige situaties (crisis/rampen) zijn in beeld maar niet geformaliseerd in processen, procedures of beheersmaatregelen. De organisatie acteert in die gevallen reactief en leunt op specifieke personen.	Eisen voor informatiebeveiliging zijn vastgesteld en vertaald naar processen, procedures en beheersmaatregelen waarvan tenminste de scenario's met de hoogste impact periodiek getest worden of anderszins aantoonbaar werken.	Eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties zijn vastgesteld. Processen, procedures en beheersmaatregelen zijn vastgesteld, gedocumenteerd, geïmplementeerd en worden gehandhaafd om het vereiste continuïteitsniveau te waarborgen. Vastgestelde en geïmplementeerde beheersmaatregelen worden regelmatig geverifieerd om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Personeel	0 / Entry	6.1	Screening	Wordt de achtergrond van personeel geverifieerd voor aanstelling?	Deze vindt op ad hoc basis plaats.	Er is een recruitementproces voor (IT)personeel vastgesteld en geïmplementeerd waarin bedrijfseisen zijn opgenomen. Verificatie van de achtergrond kan plaatsvinden, maar is niet geformaliseerd.	Toegang te hebben tot experts.
Personeel	0 / Entry	6.3	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Wordt kennis van het personeel op peil gebracht/gehouden?	Training en opleiding vindt op ad hoc basis plaats. Er is (vrijwel) geen sprake van persoonlijke certificering.	Er zijn processen m.b.t. certificering, training en opleiding voor medewerkers en persoonlijke ontwikkelingsplannen worden gehanteerd.	In geval van incidenten toegang te hebben tot personen welke ondersteuning kunnen bieden.
Personeel	0 / Entry	6.7	Telewerken	Wordt informatie beveiligd die middels telewerken wordt benaderd?	De organisatie heeft een omgeving beschikbaar gesteld waarmee remote werken wordt ondersteund. Er zijn afspraken gemaakt voor het gebruik van middelen welke hiervoor ingezet mogen worden en onder welke voorwaarden er gebruik gemaakt mag worden van deze mogelijkheid.	De organisatie ondersteunt remote werken en heeft hiervoor een omgeving beschikbaar gesteld. Los van deze omgeving zijn er geen andere methoden waarmee remote gewerkt wordt. Er bestaat een procedure rond remote werken waarin de volgende punten (voor zover wetgeving dit toelaat) minimaal zijn vastgelegd: - Waar dient de gebruiker rekening mee te houden wanneer deze remote aan het werken is. - Welke digitale omgeving er gebruikt wordt. - Risico's van werken in openbare ruimtes. - Beveiligingen tegen malware en gebruik van firewalls e.d. - Verantwoordelijkheid van veilige opslag van middelen van de organisatie.	De organisatie ondersteunt remote werken en heeft hiervoor een omgeving beschikbaar gesteld. Los van deze omgeving zijn er geen andere methoden waarmee remote werken mogelijk is. Er bestaat een procedure rond remote werken waarin de volgende punten (voor zover wetgeving dit toelaat) minimaal zijn vastgelegd: - Waar dient de fysieke omgeving waarvanuit remote gewerkt wordt aan te voldoen. - Waar dient de gebruiker rekening mee te houden wanneer deze remote aan het werken is. - Eisen gesteld aan de te gebruiken verbinding. - Welke digitale omgeving er gebruikt wordt. - De risico's welke gepaard gaan met b.v. gezinsleden welke bij zakelijke informatie kunnen komen. - Risico's van werken in openbare ruimtes. - Beveiligingen tegen malware en gebruik van firewalls e.d. - De kwetsbaarheid van single-factor toegang waar dit gebruikt wordt. - Verantwoordelijkheid van veilige opslag van middelen van de organisatie. - Welke classificatie van documenten er gebruikt mag worden. - Beschikbaar stellen van training voor het veilig remote werken.
Personeel	0 / Entry	6.8	Rapportage van informatiebeveiligingsgebeurtenissen	Worden informatiebeveiligingsgebeurtenissen gerapporteerd?	Er is een pragmatische afhandeling van incidenten. Binnen de organisatie is alom bekend bij wie medewerkers zich kunnen melden als er sprake is van een Informatiebeveiligingsgebeurtenis.	Er is sprake van een formeel incident management proces waarin prioritering en escalatiepaden zijn opgenomen en rollen en verantwoordelijkheden zijn benoemd. Alle medewerkers zijn bewust gemaakt dat zij incidenten z.s.m. melden en kennen de procedure en het contactpunt waar zij dit moeten rapporteren.	Informatiebeveiligingsgebeurtenissen worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd. Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie wordt geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
Privacy	0 / Entry	B.8.2.2	Doeleinden van de organisatie	Beperkt de verwerking zich tot zijn verwerkingsdoeleinden?	We richten ons erop om de opdracht uit te voeren. Doelbinding leunt op de scherpte en competentie van individuen.	Het principe van doelbinding is staand beleid maar in de schriftelijke opdracht zijn niet of niet altijd specifieke doeleinden aangegeven.	Er wordt voor gezorgd dat de in opdracht verwerkte persoonsgegevens uitsluitend verwerkt wordt voor de doeleinden die worden aangegeven in de schriftelijke opdracht van de opdrachtgever.
Privacy	0 / Entry	B.8.2.6	Registraties met betrekking tot het verwerken van persoonsgegevens	Worden er registraties bijgehouden die kunnen helpen om naleving van privacywet- en regelgeving aan te tonen?	De mate waarin registraties onderhouden worden ter ondersteuning van het aantonen van het voldoen aan verplichtingen hangt van individuen af.	Hoewel niet specifiek met de klant afgestemd, worden er standaard registraties onderhouden ter ondersteuning van het aantonen van het voldoen aan verplichtingen.	De benodigde registraties worden vastgesteld en onderhouden ter ondersteuning van het aantonen van het voldoen aan verplichtingen.
Technologisch	0 / Entry	8.15	Genereren, bewaren en beoordelen van logbestanden	Wordt er gebruik gemaakt van logbestanden?	Er vindt geen actief gebruik van logbestanden plaats. Wanneer logs worden gegenereerd, gebeurd dit meestal onbewust ('standaard instellingen') en er wordt zelden of nooit actief naar gekeken.	Er is beleid met betrekking tot welke activiteiten gelogd moeten worden. Toegang tot logbestanden is voorbehouden aan (systeem)beheerders. Toegang tot persoonsgegevens wordt (indien mogelijk) geregistreerd.	Logbestanden worden gericht gegenereerd en beschermd. Beoordeling vindt regelmatig plaats met als doel afwijkingen ten opzichte van normaal gebruik/functioneren te kunnen vaststellen en rapporteren. Logbestanden worden beschouwd als mogelijk bewijsmateriaal, waarbij toegang door beheerders en de integriteit van de bestanden wordt beheerst. Mogelijkheden tot manipulatie worden technisch voorkomen of gecompenseerd door organisatorische maatregelen. Geregistreerd wordt wie wanneer toegang had tot welke persoonsgegevens en welke aanpassingen er evt. zijn doorgevoerd. Er is een procedure om te bewerkstelligen dat persoonsgegevens in logbestanden wordt gewist of niet-identificeerbaar gemaakt, zoals gespecificeerd is in het bewaarschema.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0 / Entry	8.20	Beschermen van informatie in netwerken en ondersteunende systemen	Wordt informatie op het netwerk beheerd?	De organisatie gebruikt netwerkcomponenten (routers, firewalls, switches, wifirouters) zonder dat er beleid is geformuleerd over hoe deze toegang tot het netwerk zouden moeten verlenen. Er wordt niet, of slechts beperkt, gebruikgemaakt van instellingen om het netwerk actief te beschermen tegen misbruik (standaard instellingen). Protocollen (DHCP) zijn wellicht zodanig ingesteld dat gemakkelijk toegang kan worden verkregen met een willekeurig systeem.	Er is schematische documentatie aanwezig over de structuur van het netwerk. Op basis hiervan en op basis van beleid wordt vastgesteld op welke wijze verschillende systemen en netwerkcomponenten met elkaar mogen communiceren. Er wordt bijvoorbeeld gebruik gemaakt van VPN en/of IP whitelisting.	Er is beleid/documentatie aanwezig over hoe netwerkcomponenten en infrastructuur dienen te worden geconfigureerd. Firewall settings en VPN verbindingen worden actief geadministreerd, geüpdate, gelogd en gemonitord. Systemen worden zodanig ingericht dat ze zo onkwetsbaar mogelijk zijn (hardening). Er vindt mogelijk active controle op ongeoorloofde toegang plaats (Intrusion Detection).
Technologisch	0 / Entry	8.21	Veiligheid in het gebruik van netwerkdiensten garanderen	Wordt de veiligheid van netwerkdiensten vastgesteld?	De organisatie gebruikt netwerkdiensten (bijvoorbeeld internetverbindingen, VoIP) zonder van de inhoud van de geleverde dienst of beveiligingseisen een duidelijk beeld te hebben. Netwerkgebruik van (externe) gebruikers wordt niet gemonitord.	Er is beleid m.b.t. toegang tot het netwerk door leveranciers en het gebruik van VPN verbindingen. Bij de keuze van leverancier van netwerkdiensten is rekening gehouden met veiligheidsaspecten, die echter niet aantoonbaar vastgelegd of nageleefd worden.	De organisatie heeft servicecontracten met leveranciers van netwerkdiensten waarin is vastgelegd welke veiligheidsaspecten voor een specifieke dienst van toepassingen zijn. Te denken valt bijvoorbeeld aan rapportages, meldingen van incidenten, recht van audit, toegangslogs. Op VPN verbindingen (intern en extern) vindt monitoring plaats. Voor kritische netwerkdiensten is mogelijk redundantie aanwezig.
Technologisch	0 / Entry	8.24	Garanderen van goed en effectief gebruik van versleuteling om vertrouwelijkheid, integriteit en beschikbaarheid te garanderen in lijn met van toepassing zijnde wet- en regelgeving.	Wordt versleuteling (cryptografie) toegepast?	De organisatie gebruikt ad hoc versleuteling (bijvoorbeeld van harde schijven van PC's en laptops en HTTPS) op basis van standaard instellingen of door leveranciers ingerichte opties. Er is geen gericht beleid.	Er is beleid voor het gebruik van cryptografische toepassingen. Voor informatiesystemen is vastgelegd welk niveau van bescherming volstaat. Het beleid dekt echter mogelijk alleen de meest voor de hand liggende toepassingen.	De organisatie heeft een volledig beeld van toepassing van encryptie en er is actief beheer van encryptiesleutels. Encryptie wordt toegepast op statische informatie (at rest) en op informatietransport (in motion). In een internationale setting heeft de organisatie ook een inventarisatie gemaakt van van toepassing zijnde wet- en regelgeving anders dan de nationale.
Technologisch	0 / Entry	8.25	Beleid voor beveiligd ontwikkelen	Wordt er security by design toegepast bij softwareontwikkeling?	Er is geen aantoonbaar beleid m.b.t de aanpak van informatiebeveiliging in de ontwikkelingslevenscyslus van informatiesystemen. De organisatie leunt op de professionaliteit van de ontwikkelaars, architecten, etc. voor wie dit vanzelfsprekend is.	De organisatie heeft maatregelen aantoonbaar in stelling gebracht i.h.k.v: – Beveiliging v/d ontwikkelomgeving – Beveiliging in de ontwikkelmethode – Coderingsrichtlijnen en conventies – Versiecontrole – Kennis en het vermogen om kwetsbaarheden te vermijden, te vinden en te repareren	De organisatie heeft aantoonbaar regels vastgesteld voor het veilig ontwikkelen van software en systemen binnen de organisatie, waarin o.a. de onderdelen uit level 2 zijn opgenomen, en legt deze ook op bij uitbesteding.
Technologisch	0 / Entry	8.26	Informatiebeveiligingseisen in ontwerp en aanschaf van applicaties	Speelt informatiebeveiliging een rol in de aanschaf/ontwikkeling van (nieuwe) applicaties?	Bij de ontwikkeling en/of aanschaf van nieuwe applicaties wordt met name gekeken naar functionele eisen, gebruiksgemak en kosten. Informatiebeveiliging is van ondergeschikt belang.	Bij de ontwikkeling en/of aanschaf van nieuwe applicaties wordt wel gekeken naar de eisen voor informatiebeveiliging. Deze maken ook een deel uit van de vereisten, maar er wordt met name gekeken naar de meest voor de hand liggende zaken als login, rollen en rechten en beschikbaarheid. Bij de keuze van leverancier wordt wel gekeken naar de mogelijke leverancier (bijvoorbeeld naar een mogelijke certificatie), maar niet direct naar eventuele (al dan niet bekende) kwetsbaarheden van de gebruikte technologie. Voldoen aan informatiebeveiligingseisen mag economische gevolgen hebben maar (deels) niet voldoen is geen knock-out criterium.	Voordat over gegaan wordt tot aanschaf of ontwikkeling van applicaties, vindt vaststelling van vereisten plaats, waarbij normaal gesproken op basis van een (volledige) risico-analyse beveiligingseisen worden vastgesteld. Eisen bevatten o.a. - van toepassing zijnde wetteleijke en/of contractuele eisen, bijvoorbeeld met betrekking tot logging - verwerking van persoonsgegevens - verwerking van betalingsgegevens - mate van authenticatie en vertrouwen - classificatie van de informatie in de (nieuwe) applicatie - behoefte om rollen en rechten te kunnen scheiden - bescherming van vertrouwelijkheid van statische informatie (at rest) en op informatietransport (in motion) - gebruik van versleuteling - beveiligde verbindingen - weerstand tegen kwaadwilligen van buiten (SQL injectie etc), met name wanneer applicaties over het internet bereikbaar zijn Niet kunnen voldoen aan informatiebeveiligingseisen leidt tot een negatief implementatie-advies

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0 / Entry	8.32	Wijzigingsbeheer	Worden veranderingen in informatieverwerkende faciliteiten en systemen beheerst uitgevoerd?	Wijzigingen worden doorgevoerd op het moment dat dit praktisch is. Er wordt rekening gehouden met het kunnen ontstaan van mogelijke problemen, maar deze worden in principe ad hoc (bij voorkomen van) opgelost.	Er vindt een vorm van planning en inventarisatie plaats voordat een ingrijpende wijziging wordt uitgevoerd. Vaak is er wel autorisatie, maar geen volledige inventarisatie van alle mogelijke consequenties en/of communiecatie met alle betrokkenen, waardoor mogelijk geen goede borging van problemen bestaat. Niet alle ingrijpende wijzigingen worden per definitie getest/geaccepteerd vóór implementatie.	Voor installatie van software zijn procedures vastgelegd (8.19), maar ook voor andere ingrijpende wijzigingen zijn procedures aanwezig (bijvoorbeeld voor technische toegangsbeveiliging of netwerkinfrastructuur). Deze procedures houden o.a. in: (a) plan van aanpak, (b) afhankelijkheden en impact, (c) toestemming, (d) communicatie, (e) fall-back, (f) documentatie en (g) bewijs van testen en acceptatie vóór uitvoering.
Technologisch	0 / Entry	8.5	Beveiligde inlogprocedures	Wordt gecontroleerd of gebruikers die toegang hebben tot informatiesystemen zijn wie ze claimen te zijn?	Voor verschillende systemen wordt door gebruikers ingelogd met een wachtwoord. Er ontbreekt echter een formeel beleid waarin de relatie tussen de waarde van de informatie en de manier waarop wordt ingelogd is vastgelegd. Er kan ook gebruik gemaakt worden van gedeelde accounts.	Er is beleid aanwezig op basis waarvan gebruikers worden geïdentificeerd, bijvoorbeeld in het inzetten van 2-factor/multi-factor authenticatie (via authenticator-apps, of biometrische gegevens of tokens). Bij uitgifte van middelen van authenticatie (logins, sleutels, tokens) vindt controle van identiteit plaats, eventueel met verificatie bij management.	Er is beleid waardoor acties en toegang door gebruikers altijd terug te voeren zijn naar individuen. Er is een mate van beheersing die garandeert dat er nooit gevoelige informatie zichtbaar wordt voor gebruikers totdat de identiteit is vastgesteld. Op basis waarvan wordt autorisatie verleend. Er is monitoring aanwezig om (on)succesvolle loginpogingen te signaleren (monitoring) en/of te blokkeren (o.a. brute force pogingen). Het kunnen onderscheppen van logons (sniffers, camera's, keyloggers) wordt vermeden. Inactieve sessies worden afgesloten.
Technologisch	0 / Entry	8.7	Technische en organisatorische bescherming tegen malware	Wordt de organisatie beschermd tegen malware?	Er zijn mogelijk ad hoc virusscanners ingericht, maar er is geen beleid op basis waarvan installatie, onderhoud en controle plaatsvindt. Eindgebruikers zijn niet bekend met handelwijze indien malware wordt aangetroffen of hoe installatie van malware actief te voorkomen. Beheer van patches is ad hoc (vaak op basis van standaard instellingen). Kwetsbare/oudere versies van besturingssytemen hebben mogelijk direct contact met het internet. Datadragers mogen vrij door (eind)gebruikers worden gebruikt/aangesloten.	Er is beleid m.b.t. keuze voor, installatie en onderhoud van virusscanners, patchmanagement en voorkoming van installatie van malware. Beleid en bewustwording bij medewerkers zijn niet altijd aantoonbaar. Vaststelling van de effectiviteit van de genomen maatregelen ontbreekt, met name door vertrouwen op de gekozen leveranciers en/of producten. Patchmanagement is mogelijk niet 'waterdicht'. Alle extern aangeleverde datadragers worden gescanned en goedgekeurd alvorens te mogen worden gebruikt.	Er is sprake van beheersing van bescherming tegen malware. Installatie en updates van virusscanners en patches worden (centraal) beheerd. Gebruikers zijn bekend in handelwijze m.b.t. voorkomen van installatie van malware en het tijdig melden van incidenten. Er vindt monitoring/scanning plaats van internettoegang en externe netwerktoegang (webpagina's, e-mailbijlages, downloads/FTP uploads). Geïnfecteerde systemen kunnen tijdig worden geïsoleerd. Effectiviteit van maatregelen wordt regelmatig geëvalueerd.
Technologisch	0 / Entry	8.8	Voorkomen van exploitatie van technische kwetsbaarheden	Worden technische kwetsbaarheden voorkomen?	Kwetsbaarheden worden ad hoc - 'op gevoel' - vastgesteld en er zijn geen gedefinieerde procedures om dit op een gestructureerde wijze vast te stellen. Getroffen maatregelen zijn niet aantoonbaar effectief. Bij de ontwikkeling van software wordt niet structureel gekeken naar bestaan/ontstaan van nieuwe kwetsbaarheden.	Er is een procedure om op basis van de volledige inventarisatie van informatiesystemen en geïnventariseerde dreigingen een zo compleet mogelijk overzicht van kwetsbaarheden vast te stellen. Er is beleid geformuleerd m.b.t. het behandelen en voorkomen van nieuwe kwetsbaarheden.	Er zijn rollen en verantwoordelijkheden gedefinieerd voor de vaststelling, het updaten en de behandeling van kwetsbaarheden. Er wordt actief gemonitord op kwetsbaarheden, bijvoorbeeld door scanning of penetratietesten en bij veranderingen in software of infrastructuur. Er wordt op kwetsbaarheden gerapporteerd en de effectiviteit van getroffen maatregelen wordt vastgesteld.
Fysiek	0 +1 / Basic	7.12	Beveiliging van bekabeling	Worden kabels beschermd?	Voedings- en telecommunicatiekabels zijn professioneel aangelegd maar bescherming ervan vindt ad hoc plaats. Maatregelen worden (vooral) getroffen nadat er iets mis is gegaan.	Formeel beleid ontbreekt maar kabels lopen ondergronds of zijn anderszins beschermd en voedingskabels zijn van communicatiekabels gescheiden. Overige maatregelen zijn pragmatisch ingestoken.	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, worden beschermd tegen interceptie, verstoring of schade. Maatregelen uit level 2 zijn voor gevoelige/essentiële systemen aangevuld met bijvoorbeeld afgesloten kabelgoten/kamers, beveiligde schakelpanelen/kabelruimtes en technische schoonmaakbeurten en controles op aangesloten niet-goedgekeurde apparaten
Fysiek	0 +1 / Basic	7.14	Veilig verwijderen of hergebruiken van apparatuur	Worden opslagmedia verwijderd of hergebruikt?	Er zijn geen formele procedures voor het verwijderen van gegevens. Gegevens worden ad hoc verwijderd.	Er zijn informele procedures geïmplementeerd die ervoor zorgen dat voorafgaand aan verwijdering of hergebruik wordt gecontroleerd of apparatuur opslagmedia bevat. De verantwoordelijkheden voor het verwijderen van gegevens zijn gedeeltelijk gedefinieerd.	Alle onderdelen van de apparatuur die opslagmedia bevatten, worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven. In aanvuling op level 2 worden opslagmedia die vertrouwelijke of auteursrechtelijk beschermde informatie bevatten, fysiek vernietigd of de informatie wordt technologisch dusdanig vernietigd dat de oorspronkelijke informatie niet terug te halen is.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Fysiek	0 +1 / Basic	7.2	Fysieke toegangsbeveiliging	Wordt de fysieke toegang tot beveiligde gebieden beperkt tot bevoegd personeel?	Er zijn geen procedures vastgesteld voor de registratie van fysieke toegang. Eventuele overige procedures ter bescherming van fysieke IT-middelen is niet of beknopt gedefinieerd.	Informele procedures zijn geïmplementeerd om toegang tot specifieke locaties in gebouwen te verlenen, te beperken en in te trekken. Enkele elementen zijn waarneembaar zoals bijvoorbeeld bezoekersregistratie/-begeleiding, zichtbare identificatie en extra restrictie tot gebieden waar vertrouwelijke informatie wordt verwerkt.	Beveiligde gebieden zijn beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, worden beheerst, en zijn zo mogelijk afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.
Fysiek	0 +1 / Basic	7.3	Kantoren, ruimten en faciliteiten beveiligen	Worden (kantoor)ruimtes en overige faciliteiten binnen de locatie beveiligd?	Niet iedere ruimte is voor iedereen toegankelijk. Afscherming vind plaats middels sloten en/of beperkingen die opgelegd worden door (begeleidend) personeel. Er wordt vooral geleund op gezond verstand.	Er zijn beleidsregels en er zijn aantoonbare fysieke beveiligingsmaatregelen getroffen die niet afhankelijk zijn van (begeleidend) personeel. Vertrouwelijke informatie en activiteiten is/zijn van buitenaf niet zicht- en hoorbaar. Adres-/telefoonboeken waarin locaties zijn aangeduid die vertrouwelijke informatie verwerken, zijn niet voor onbevoegden inzichtelijk.	Er is een formeel beleid m.b.t. de beveiliging van (kantoor)ruimtes en faciliteiten waarin de maatregelen op level 2 zijn opgenomen. Vanuit buiten zijn er zo min mogelijk aanwijzingen van informatieverwerkende activiteiten (indien van toepassing).
Fysiek	0 +1 / Basic	7.4	Monitoren van de fysieke beveiliging	Wordt er toezicht gehouden op fysiek ongeautoriseerde toegang tot de organisatie?	Er zijn enkele beveiligingsmaatregelen getroffen om de fysieke locatie(s) van de organisatie te beschermen tegen ongeautoriseerde toegang. Structureel toezicht of monitoring op fysieke toegang vindt niet plaats.	Er is een beveiligingssysteem aanwezig om de fysieke locatie(s) te beschermen tegen ongeautoriseerde toegang. Hierin is (enige mate van) toezicht of monitoring op fysieke toegang geïmplementeerd.	Er is een beveiligingssysteem aanwezig om de fysieke locatie(s) te beschermen tegen ongeautoriseerde toegang. Locaties die voor de organisatie kritieke systemen onderbrengen zijn voorzien van continue videobewaking en detectiemiddelen. Getroffen maatregelen worden periodiek gecontroleerd.
Fysiek	0 +1 / Basic	7.5	Beschermen tegen bedreigingen van buitenaf	Wordt fysieke bescherming geboden tegen externe bedreigingen?	Er is enige pragmatische bescherming tegen natuurrampen, kwaadwillige aanvallen en/of ongelukken op eigen inzicht, waaronder brandbestrijding.	Ten behoeve van beschermingsmaatregelen is specialistisch advies ingewonnen over het vermijden van schade door brand, overstroming, aardbeving, explosie, oproer en andere vormen van natuurrampen of door personen veroorzaakte rampen.	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken is fysieke bescherming ontworpen en toegepast op basis van specialistisch advies.
Fysiek	0 +1 / Basic	7.6	Werken in beveiligde gebieden	Wordt het werken in beveiligde gebieden beheerst?	Voor het werken in beveiligde gebieden wordt geleund op gezond verstand en de professionaliteit van personen in kwestie.	Voor het werken in beveiligde gebieden zijn enkele niet-geformaliseerde regels van kracht.	Voor het werken in beveiligde gebieden zijn procedures ontwikkeld en toegepast. Zo is personeel er alleen op grond van need-to-know mee bekend, zijn leegstaande ruimten afgesloten, is opnameapparatuur niet toegestaan en wordt zonder toezicht werken in beveiligde gebieden vermeden.
Fysiek	0 +1 / Basic	7.7	'Clear desk'- en 'clear screen'-beleid	Wordt een Clear Desk en Clear Screen beleid gehanteerd?	Van personeel wordt verwacht dat ze hun systeem locken als ze hun werkplek verlaten.	Er is een clear desk beleid voor papieren documenten en verwijderbare opslagmedia en een clear screen beleid voor informatieverwerkende faciliteiten ingesteld. De praktijken van level 2 zijn hierin onder andere in meegenomen.	Er is een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten ingesteld. De praktijken van level 2 zijn hierin onder andere in meegenomen.
Fysiek	0 +1 / Basic	7.8	Plaatsing en bescherming van apparatuur	Wordt apparatuur fysiek beschermd en afgeschermd?	Apparatuur is naar eer en geweten zo goed mogelijk geplaatst, zonder expliciet te kijken naar gevaren van buitenaf of de kans op onbevoegde toegang/inzage.	Er is een cultuur waarin enkele van deze praktijken worden toegepast: het beveiligen van opslagfaciliteiten tegen onbevoegde toegang, de positionering van informatieverwerkende faciliteiten (zoals monitors) waarmee onbevoegde inzage wordt voorkomen, getroffen beheersmaatregelen die risico's reduceren van fysieke bedreigingen en bedreigingen van buitenaf (diefstal, brand, rook, stof, water, etc.) en/of de vastgestelde richtlijnen voor eten, drinken en roken in nabijheid van faciliteiten.	Apparatuur is zo geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang wordt verkleind. De praktijken van level 2 maken hier onderdeel vanuit.
Fysiek	0 +1 / Basic	7.9	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Worden bedrijfsmiddelen buiten het terrein beveiligd?	Medewerkers worden geacht zorgvuldig om te gaan met bedrijfsmiddelen als zij deze buiten het terrein gebruiken en de organisatie leunt hierop.	Er is een cultuur waarin enkele van deze praktijken worden toegepast: het niet onbeheerd achterlaten van apparatuur, het opvolgen van voorschriften van de fabrikant en/of de vastgestelde beheersmaatregelen voor thuiswerken en tijdelijke locaties.	Bedrijfsmiddelen die zich buiten het terrein bevinden, worden beveiligd, rekeninghoudend met de verschillende risico's van werken buiten het terrein van de organisatie. De praktijken van level 2 maken hier onderdeel vanuit.
Organisatorisch	0 +1 / Basic	5.12	Classificatie van informatie	Hanteert de organisatie een classificatiemechanisme?	Informatie en de bedrijfsmiddelen waarin die is opgeslagen of anderszins wordt verwerkt, wordt/worden (deels) geclassificeerd. Ten behoeve hiervan wordt een classificatieschema gehanteerd met verschillende uniek benoemde niveaus.	Informatie en de bedrijfsmiddelen waarin die is opgeslagen of anderszins wordt verwerkt, wordt/worden geclassificeerd en zijn voorzien van bijbehorende beheersmaatregelen per niveau. Eigenaren van bedrijfsmiddelen zijn verantwoordelijk voor de classificatie ervan. Het classificatieschema omvat regels voor classificatie en criteria voor herbeoordeling. Classificatie is opgenomen in procedures van de organisatie en is in overeenstemming met toegangsbeveiliging.	Informatie is geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
Organisatorisch	0 +1 / Basic	5.19	Informatiebeveiligingsbeleid voor leveranciersrelaties	Worden informatiebeveiligingseisen gehanteerd m.b.t. leveranciers die toegang hebben tot de bedrijfsmiddelen van de organisatie?	Informatiebeveiligingseisen komen niet preventief voort uit het voorkomen of reduceren van risico's, maar komen op ad hoc basis of reactief bij incidenten aan de orde.	Beheersmaatregelen zijn verplicht gesteld specifiek voor leveranciers met toegang tot informatie van de organisatie, zoals vastlegging van soorten leveranciers, een gestandaardiseerd proces voor het relatiebeheer van leveranciers, standaardeisen en/of de monitoring van naleving.	Met leveranciers zijn de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leveranciers tot de bedrijfsmiddelen van de organisatie, overeengekomen en gedocumenteerd.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Organisatorisch	0 +1 / Basic	5.20	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Worden informatiebeveiligingseisen opgenomen in de overeenkomsten met leveranciers die toegang hebben tot de IT-infrastructuur of anderszins informatie verwerken?	Informatiebeveiligingseisen kunnen in leveranciersovereenkomsten voorkomen maar dit is niet structureel de aanpak en/of bevat doorgaans enkel algemene bepalingen over geheimhouding en/of datalekken.	Er zijn overeenkomsten opgesteld met leveranciers voorzien van verplichtingen om te voldoen aan informatiebeveiligingseisen, waarin aspecten als bijvoorbeeld classificatie, wettelijke eisen, toegang en/of procedures worden geregeld.	Alle relevante informatiebeveiligingseisen zijn vastgesteld en overeengekomen met elke leverancier die (a) toegang heeft tot IT-infrastructuur t.b.v. de informatie van de organisatie of (b) informatie van de organisatie verwerkt, opslaat, communiceert of biedt.
Organisatorisch	0 +1 / Basic	5.21	Toeleveringsketen van informatie- en communicatietechnologie	Neemt de organisatie beveiligingseisen in leveranciersovereenkomsten op m.b.t. de toeleveringsketen?	Er is geen standaard of formeel beleid dat rekening houdt met de risico's in verband met de ICT-toeleveringsketen ook al kunnen deze wel in overeenkomsten voorkomen.	In leveranciersovereenkomsten komen onderwerpen aan de orde zoals bijvoorbeeld eisen voor acquisitie van producten of diensten en de doorgifte van informatiebeveiligingseisen bij verdere uitbesteding.	Overeenkomsten met leveranciers bevatten eisen die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
Organisatorisch	0 +1 / Basic	5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Wordt er gebruik gemaakt van clouddiensten?	Bij het gebruik van clouddiensten wordt stilgestaan bij informatiebeveiliging.	Het is duidelijk hoe voor het gebruik van clouddiensten omgegaan wordt met informatiebeveiliging. Selectiecriteria worden gehanteerd en exit strategieën zijn bekend. De scope van de dienst, het beheer van de omgeving, de betrokken rollen/verantwoordelijkheden en procedures voor het omgaan met incidenten zijn overeengekomen met leveranciers.	Er zijn processen opgesteld voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten overeenkomstig de informatiebeveiligingseisen van de organisatie.
Organisatorisch	0 +1 / Basic	5.27	Lering uit informatiebeveiligingsincidenten	Wordt lering getrokken uit informatiebeveiligingsincidenten?	Dergelijke incidenten worden vastgelegd en er wordt op individueel niveau van geleerd.	Dergelijke incidenten worden vastgelegd, er wordt gekeken naar de oorzaak en waar nodig worden passende maatregelen getroffen om dit in de toekomst te voorkomen of de mogelijke impact te verkleinen. Periodiek wordt gekeken naar trends in (type) incidenten.	Er is een procedure voor het vastleggen van informatiebeveiligingsincidenten en het afhandelen hiervan. De lering die uit incidenten getrokken wordt, wordt gebruikt worden om: - Het calamiteitenplan van passende scenarios te voorzien. - Het risico van een dergelijk incident in te schatten. - Bewustzijn bij gebruikers te verruimen.
Organisatorisch	0 +1 / Basic	5.34	Privacy en bescherming van persoonsgegevens	Hanteert de organisatie privacywet- en regelgeving?	Er is een privacybeleid opgesteld en personeel heeft één of meerdere privacytrainingen gehad. De organisatie leunt sterk op de professionele houding van personeel.	Beleid is ontwikkeld en geïmplementeerd voor privacy en bescherming van persoonsgegevens. Er is aantoonbare kennis omtrent privacy in de organisatie aanwezig. Passende technische en organisatorische maatregelen zijn getroffen om persoonsgegevens te beschermen.	Beleid is ontwikkeld en geïmplementeerd voor privacy en bescherming van persoonsgegevens. Deze is gecommuniceerd met betrokkenen bij de verwerking. Er wordt een beheerstructuur gehanteerd en een privacy functionaris/officer aangesteld. Passende technische en organisatorische maatregelen zijn getroffen om persoonsgegevens te beschermen.
Organisatorisch	0 +1 / Basic	5.37	Gedocumenteerde bedieningsprocedures	Borgt de organisatie bedieningsprocedures m.b.t. informatieverwerkende en communicatiefaciliteiten?	Er zijn één of meerdere locaties waar relevante bedieningsprocedures gevonden kunnen worden. Deze worden (ongecontroleerd) naar eigen inzicht geplaatst.	Bedieningsprocedures worden beheerd en gepubliceerd zoals installatie-/configuratie-instructies, opstart-/herstelprocedures, voorschriften, etc.	Bedieningsprocedures zijn gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.
Organisatorisch	0 +1 / Basic	5.7	Informatie en analyse over dreigingen	Wordt er gekeken naar bedreigingen op het gebied van informatiebeveiliging?	Er wordt rekening gehouden met mogelijke bedreigingen rond informatiebeveiliging.	Mogelijke bedreigingen van de informatiebeveiliging van de organisatie worden in de gaten gehouden en hier wordt lering uit getrokken.	Op de hoogte te blijven van kennis van best practices en andere relevante informatie op het gebied van informatiebeveiliging.
Organisatorisch	0 +1 / Basic	5.9	Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen	Worden de met informatie samenhangende bedrijfsmiddelen vastgelegd?	Enkele bedrijfsmiddelen zijn in een overzicht opgenomen dat (ad hoc) actueel wordt gehouden.	Geïdentificeerde bedrijfsmiddelen zijn voorzien van eigenaren en de inventaris wordt actueel gehouden.	In een vroeg stadium op de hoogte te blijven van mogelijk bedreigingen op het gebied van informatiebeveiliging, denk aan beschikbare updates e.d.
Personeel	0 +1 / Basic	6.2	Arbeidsvoorwaarden	Zijn verantwoordelijkheden voor informatiebeveiliging/privacy opgenomen in arbeidsovereenkomsten?	Er zijn arbeidsvoorwaarden overeengekomen. Verantwoordelijkheden voor informatiebeveiliging/privacy kunnen hierin voorkomen, maar dit is niet altijd het geval.	Er zijn arbeidsvoorwaarden overeengekomen met medewerkers waarin verantwoordelijkheden voor informatiebeveiliging/privacy zijn opgenomen. Voor contractanten vindt dit niet of niet structureel plaats.	Informatie kunnen uitwisselen op het gebied van informatiebeveiliging.
Personeel	0 +1 / Basic	6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Worden vertrouwelijkheid-/geheimhoudingsovereenkomsten gebruikt?	Vertrouwelijkheids- of geheimhoudingsovereenkomsten worden op ad hoc basis toegepast en omvatten het beschermen van vertrouwelijke informatie en persoongegevens in algemene zin.	Vertrouwelijkheids- of geheimhoudingsovereenkomsten zijn afgestemd op de informatiebeveiligings-/privacy-eisen van de organisatie en omvatten ook elementen als vereiste acties als de overeenkomst wordt beëindigd, eigendom van informatie en/of afspraken over notificaties en teruggave.	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie en persoonsgegevens weerspiegelen zijn vastgesteld en worden regelmatig beoordeeld en gedocumenteerd.
Privacy	0 +1 / Basic	B.8.2.1	Overeenkomst met de klant	Wordt de klant ondersteund in zijn privacyverplichtingen?	Als de klant ondersteuning nodig heeft dan wordt dat ad hoc geleverd.	Het desgewenst ondersteunen van de klant behoort tot onze praktijk, maar dit is in de verwerkersovereenkomst niet nader uitgewerkt.	In de verwerkersovereenkomst met de klant is de rol van de organisatie opgenomen in het ondersteunen van de klant in zijn verplichtingen.
Privacy	0 +1 / Basic	B.8.2.5	Verplichtingen van klanten	Wordt de opdrachtgever passend geïnformeerd, zodat hij aan zijn eigen privacyverplichtingen kan voldoen?	Heeft de klant informatie nodig dan wordt deze ad hoc aangeleverd.	Er zijn procedures t.b.v. het aanleveren van passende informatie voor de klant.	Op basis van een vastgestelde behoefte wordt de klant voorzien van de passende informatie zodat deze kan aantonen dat hij aan zijn privacyverplichtingen voldoet.
Privacy	0 +1 / Basic	B.8.5.6	Bekendmaking van onderaannemers die worden ingezet voor het verwerken van persoonsgegevens	Wordt de opdrachtgever op de hoogte gesteld als de organisatie een onderaannemer in de arm neemt?	De opdrachtgever wordt soms op de hoogte gesteld over de inzet van subverwerkers voordat deze worden ingezet.	De opdrachtgever wordt informeel op de hoogte gesteld over de inzet van subverwerkers voordat deze worden ingezet.	De opdrachtgever wordt formeel op de hoogte gesteld over de inzet van subverwerkers voordat deze worden ingezet.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0 +1 / Basic	8.1	Beheersing van informatie die wordt opgeslagen of verwerkt op werkplekken en/of mobiele apparaten.	Wordt gebruikersapparatuur (laptop, PC, tablet, smartphone) dat als onderdeel van de werkplek fungeert beschermd?	Er is geen formeel beleid wat gebruikers wel en niet mogen in het gebruik van (mobiele) informatiesystemen. Er vindt ad hoc registratie van systemen plaats en mogelijk maken medewerkers gebruik van privémiddelen voor zakelijke doeleinden zonder dat daar beleid voor is.	Verantwoordelijkheden m.b.t. systemen gebruikt door eindgebruikers zijn vastgelegd en in principe bekend bij eindgebruikers. Hier hoeft niet actief op te worden gecontroleerd. Er is bij de organisatie beleid en een methodiek die bepaalt welke systemen er welke toegang hebben tot informatie van de organisatie. Er is echter geen sprake van structureel (remote) beheer van deze systemen.	Gebruikers zijn zich bewust van procedures en vereisten in het gebruik van informatiesystemen, onder meer m.b.t. afsluiten wanneer niet in gebruik en handelen in openbare ruimtes. Er is (waar van topepassing) gecontroleerd beleid voor BYOD (Bring Your Own Device). De status van systemen (bijvoorbeeld m.b.t. patches en encryptie) wordt geregistreerd en installatie van software op werkplekken wordt door de organisatie beheerd. Er is sprake van een technische en organisatorische beheersing van alle door eindgebruikers gebruikte apparatuur.
Technologisch	0 +1 / Basic	8.10	Wissen van informatie	Wordt informatie verwijderd als de noodzaak om deze te behouden is weggevallen?	Op ad hoc basis wordt informatie die niet langer nodig is, verwijderd. Er is geen structurele aanpak in lijn met vastgesteld beleid en er zijn geen tools ter ondersteuning.	Periodiek wordt informatie die niet langer nodig is, opgeschoond. Er zijn geen tools ter ondersteuning. Er zijn bewaartermijnen in kaart gebracht van de belangrijkste informatie(sets).	Informatie die niet langer nodig is, wordt structureel verwijderd in lijn met vastgesteld beleid van de organisatie. Bewaartermijnen zijn in kaart gebracht en worden (indien mogelijk automatisch) gehanteerd. Bij het verwijderen wordt rekening gehouden met (a) de afspraken met opdrachtgevers, (b) logging als bewijslast en (c) oude versies en tijdelijke bestanden. Indien bij het verwijderen gebruik gemaakt wordt van diensten van een leverancier wordt bewijslast vastgelegd rond het verwijderen en wordt vastgelegd dat de leverancier hiertoe bevoegd is.
Technologisch	0 +1 / Basic	8.12	Voorkomen van gegevenslekken	Zijn er binnen de organisatie maatregelen getroffen om inbreuken op de informatiebeveiliging te voorkomen?	Er zijn binnen de organisatie enkele maatregelen getroffen om de kans op inbreuken te beperken. Hierbij wordt sterk geleund op het bewustzijn en de alertheid van medewerkers.	Er zijn binnen de organisatie maatregelen getroffen om de kans op inbreuken te beperken. Dit is gedaan door systemen te beveiligen en gebruikers bewust te maken van een eigen verantwoordelijk om veilig te werken.	Er zijn binnen de organisatie maatregelen getroffen om de kans op inbreuken te beperken. Dit is gedaan door systemen te beveiligen en gebruikers bewust te maken van hun eigen verantwoordelijkheid om veilig te werken. Hierover zijn afspraken gemaakt in de vorm van een beleid. Informatie binnen de organisatie is voorzien van een classificatie. Veel gebruikte communicatiekanalen worden gemonitord op mogelijke inbreuken. Veel gebruikte methoden waarbij inbreuken kunnen ontstaan zijn geblokkeerd zoals b.v. het kopiëren van database gegevens in Excel.
Technologisch	0 +1 / Basic	8.13	Back-up van informatie	Wordt er binnen de organisatie informatie gebackupt?	Binnen de organisatie is een backup beleid aanwezig. Het periodiek testen is hier onderdeel van.	De organisatie beschikt over een backup beleid welke de volgende zaken behandelt: - Wat wordt meegenomen in de backup - Hoe kan een backup teruggeplaatst worden - Hoe wordt gegarandeerd dat de opslaglocatie van de backup veilig en betrouwbaar is en de eisen minimaal hetzelfde zijn als gesteld aan de eigenlijke opslaglocatie - Test schema welk aantoonbaar uitgevoerd wordt en de lading dekt van een herstelactie in een noodsituatie	De organisatie beschikt over een backup beleid welke de volgende zaken behandelt: - Wat wordt meegenomen in de backup - Hoe kan een backup teruggeplaatst worden - Hoe wordt gegarandeerd dat de opslaglocatie van de backup veilig en betrouwbaar is en de eisen minimaal hetzelfde zijn als gesteld aan de eigenlijke opslaglocatie - Test schema welk aantoonbaar uitgevoerd wordt en de lading dekt van een herstelactie in een noodsituatie - Toepassen van encryptie op de backup overeenkomend met de informatie classificatie van de betreffende informatiesoorten - Een backup niet gestart wordt wanneer onbedoeld dataverlies plaatsvindt. Bij het gebruik van clouddiensten dient bepaald te worden tot in hoeverre de fasciliteiten van de leverancier passend zijn bij de eisen van de organisatie overeenkomend met de informatieclassificatie welke van toepassing is.
Technologisch	0 +1 / Basic	8.19	Beschermen van operationele systemen door procedures en maatregelen voor de installatie van software	Wordt software beheerst geïnstalleerd op systemen die een essentieel onderdeel uitmaken van operationele processen?	Software wordt geïnstalleerd - al dan niet door een leverancier - op een wijze die en moment dat passend is. Er wordt geen uitgebreide analyse gemaakt van mogelijke consequenties voor de van het desbetreffende systeem afhankelijke processen	Er is een gedocumenteerd proces op basis waarvan installatie van software op operationele systemen zou moeten plaatsvinden en verstoring van operationele processen zoveel mogelijk moet voorkomen. Afhankelijk van de situatie wordt dit proces in meer of mindere mate gevolgd.	Er zijn vastomlijnde processen en procedures met betrekking tot de installatie van software op operationele systemen. Dit gebeurt alleen - conform eisen en beleid van de organisatie - na autorisatie van de eigenaar van een informatiesysteem of het management - door kundig personeel - na succesvol testen - met een strategie voor 'terug naar normaal' bij een alsnog falende installatie - middels het bijhouden van een log van updates en wijzigingen - met behoud van het kunnen verwerken van nog relevante historische data Daar waar mogelijk vindt hardening plaats van (operationele) systemen.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0 +1 / Basic	8.2	Beheren van speciale toegangsrechten	Wordt toewijzing en gebruik van speciale toegangsrechten (systeembeheerders, super users, etc.) beperkt?	Hoewel niet exact geinventariseerd, zijn er enkele rollen met speciale rechten. Betrokken medewerkers zijn zich bewust van hun verantwoordelijkheid en worden vertrouwd.	De organisatie weet exact welke speciale toegangsrechten gebruikt worden. Deze zijn tot noodzaak beperkt, in lijn met het toegangsbeleid. Speciale toegangsrechten worden pas verleend nadat de autorisatieprocedure is doorlopen. Waar mogelijk zijn dit persoonlijke accounts welke over niet meer rechten beschikken als wat nodig is om de werkzaamheden uit te voeren.	Aanvullend op level 2: Gebruikers hebben de minimale hoeveelheid rechten om werkzaamheden uit te kunnen voeren. Gebruikers zijn zich bewust met welke rechten ze op dat moment aan het werk zijn. Er bestaat een proces voor het uitdelen en intrekken van de rechten. Van het verloop van dit proces wordt een registratie bijgehouden. Hoofd accounts zoals b.v. root zijn extra beveiligd en er zijn maatregelen getroffen om het gebruik hiervan zoveel mogelijk te beperken. Er wordt gewerkt met persoonlijke accounts. Wanneer dit niet mogelijk is, zal een gedeeld account naar een gebruiker herleid kunnen worden. Competenties van gebruikers met speciale toegangsrechten worden regelmatig beoordeeld.
Technologisch	0 +1 / Basic	8.3	Beperking toegang tot informatie	Wordt de toegang tot informatie en systeemfuncties van applicaties beperkt?	Toegang wordt pragmatisch beperkt in afwezigheid van een formeel beleid voor toegangsbeveiliging. Toegang wordt ad hoc/op individuele basis verleend, mogelijk zelfs aan derden (leveranciers).	Toegang wordt beperkt in overeenstemming met een informeel en/of onvolledig beleid voor toegangsbeveiliging. Beleidsonderdelen, zoals een autorisatiematrix, worden gehanteerd maar niet formeel gebruikt. Er bestaat geen garantie dat er meer toegang wordt verleend dan nodig voor het vervullen van rol of functie.	Er is sprake van toegangsmanagement, waarbij toegang wordt beperkt/beheerst in overeenstemming met formeel en actueel beleid voor toegang, gerelateerd aan functies/rollen en de waarde van informatie. Toegang is gebaseerd op 'geen toegang, tenzij...' Er wordt, waar noodzakelijk, onderscheid gemaakt in lees- schrijf- en uitvoeringsrechten.
Fysiek	0+1+2/Intermediate	7.10	Opslag media	Wordt onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen?	Er zijn maatregelen getroffen binnen de organisatie die zorgdragen voor beveiliging van de bedrijfsinformatie of toegang tot informatieverwerkendeprocessen op fysieke opslagmedia.	Er zijn procedures aanwezig binnen de organisatie welke zorgdragen voor het beveiligen van bedrijfsinformatie of informatieverwerkende processen op fysieke opslagmedia. Er is een procedure aanwezig waarin is vastgelegd hoe om te gaan met verwijderbare media; daarbij moet aan de volgende eisen worden voldaan: - Betrokkenen weten dat deze procedure gebruikt moet worden. - De informatie op het medium of de media zelf dient op een manier versleuteld te zijn passend bij de classificatie van de informatie. - Indien de bewaartermijn een rol speelt, dient hiermee rekening gehouden te worden. - Indien verloren gaan van de informatie op het medium een risico vormt, dienen er meerdere kopieën te bestaan.	Er zijn procedures aanwezig binnen de organisatie welke zorgdragen voor het beveiligen van bedrijfsinformatie of informatieverwerkende processen op fysieke opslagmedia. Er is een procedure aanwezig waarin vastgelegd staat hoe om te gaan met verwijderbare media; daarbij moet aan de volgende eisen worden voldaan: - Betrokkenen weten dat deze procedure gebruikt moet worden. - Alle media dient opgeslagen te worden op een manier overeenkomstig met de classificatie van de betreffende informatie op het medium zelf. - De informatie op het medium of de media zelf dient op een manier versleuteld te zijn passend bij de classificatie van de informatie. - Indien de bewaartermijn een rol speelt dient hiermee rekening gehouden te worden. - Indien verloren gaan van de informatie op het medium een risico vormt dienen er meerdere kopieen te bestaan. - Poorten op hardware (USB en cardreaders etc.) dienen alleen beschikbaar gesteld te worden wanneer er een organisatorische reden voor is. - Wanneer er reden voor bestaat om informatie op verwijderbare media op te slaan dient opslag in een audittrail opgenomen te worden.
Fysiek	0+1+2/Intermediate	7.11	Nutsvoorzieningen	Worden nutsvoorzieningen beschermd te verstoringen?	Nutsvoorzieningen (elektriciteit, telecommunicatie, watervoorziening, gas, riolering, ventilatie en airconditioning) is professioneel aangesloten. Eventuele ontregeling wordt ad hoc opgepakt.	Ter bescherming van apparatuur tegen ontregeling van nutsvoorzieningen komt de installatie (voor zover nodig en van toepassing) overeen met de technische beschrijving van de fabrikant en wettelijke eisen, wordt deze periodiek beoordeeld op capaciteit, geïnspecteerd en getest, is voorzien van detectie en/of meervoudige stroomvoorziening.	Apparatuur is beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. Onder meer met de maatregelen uit level 2 tenminste aangevuld met de aanwezigheid van noodverlichting en communicatie middelen en noodschakelaars/knoppen om voorzieningen als stroom, water en gas uit te kunnen schakelen.
Fysiek	0+1+2/Intermediate	7.13	Onderhoud van apparatuur	Wordt apparatuur onderhouden?	Er is geen proces gedefinieerd voor het onderhoud. Wijzigingen worden doorgevoerd zonder een formele strategie of algemeen plan. Onderhoud wordt gedaan op basis van incidenten en/of kortetermijnbehoeften.	Er is een informeel onderhoudsproces geïmplementeerd dat niet is afgestemd op bedrijfseisen/-strategie. Onderhoud vindt door bevoegd onderhoudspersoneel plaats in overeenstemming met door leverancier aanbevolen voorschriften en intervallen voor servicebeurten en eventuele onderhoudseisen in verzekeringspolissen.	Apparatuur wordt correct onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. Ten behoeve hiervan is een duidelijk, gedefinieerd en algemeen begrepen onderhoudsproces waarin aspecten van level 2 zijn aangevuld met de registraties van vermeende en daadwerkelijke fouten, de in bedrijfstelling na inspectie en de passende maatregelen voor vertrouwelijkheid van gegevens.
Organisatorisch	0+1+2/Intermediate	5.10	Aanvaardbaar gebruik van informatie en overige bedrijfsmiddelen	Stuurt de organisatie op aanvaardbaar gebruik van informatie en van bedrijfsmiddelen?	Er zijn algemene instructies gegeven aan het personeel over het fatsoenlijk gebruiken van informatie(middelen). Deze zijn tevens opgenomen in een awareness programma.	Er zijn concrete regels voor aanvaardbaar gebruik. Procedures voor het behandelen van bedrijfsmiddelen zijn ontwikkeld en geïmplementeerd.	Regels voor aanvaardbaar gebruik zijn geïdentificeerd, gedocumenteerd en geïmplementeerd. Procedures voor het behandelen van bedrijfsmiddelen zijn ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Organisatorisch	0+1+2/Intermediate	5.11	Teruggeven van bedrijfsmiddelen	Wordt er binnen de organisatie bij wijzging van de functie van een medewerker of uitdiensttreding gewerkt met een vast proces?	Er wordt gewerkt middels een proces dat ervoor zorgt dat uitgegeven middelen aan medewerkers, die er door wijziging of beëindiging van functie geen recht meer op hebben, ingenomen worden.	Er wordt gewerkt middels een proces dat ervoor zorgt dat uitgegeven middelen aan medewerkers, die er door wijziging of beeindiging van functie geen recht meer op hebben, ingenomen worden. Van de inname wordt een registratie bijgehouden.	Er wordt gewerkt middels een proces binnen de organisatie dat ervoor zorgt dat de volgende zaken aantoonbaar retour komen bij wijziging van functie of einde dienstverband van een medewerker: - End-point devices (laptop, smartphone etc.) - Opslagmedia (USB sticks, hardeschijven etc.) - Specialistische apparatuur - Authenticatie hardware (smartcards etc.) - Fysieke documenten Zowel van originele uitgifte als inname bestaat een registratie waaruit opgemaakt kan worden dat zowel uitgever als ontvanger akkoord gaan met de uitwisseling.
Organisatorisch	0+1+2/Intermediate	5.13	Informatie labelen	Wordt informatie binnen de organisatie voorzien van een label?	Informatie binnen de organisatie wordt soms van een label.	Er bestaat een procedure die omschrijft welke classificaties er gebruikt worden binnen de organisatie en informatie is voorzien van labels.	Binnen de organisatie wordt informatie voorzien van een label en er is duidelijk omschreven: - Wanneer hier een uitzondering op wordt gemaakt. - Hoe dit label aanwezig is en wat de lading van het label is. - Hoe er om gegaan wordt met situaties waar een label gebruiken niet mogelijk is door b.v. technische beperkingen. De procedures omschrijven hoe omgegaan moet worden met de classificatie van de informatie, denk aan geheim, vertrouwelijk, openbaar etc. Betrokkenen dienen op de hoogte te zijn van deze procedures.
Organisatorisch	0+1+2/Intermediate	5.17	Authenticatieinformatie	Hanteert de organisatie een wachtwoorbeleid?	Binnen de organisatie bestaat er een wachtwoordbeleid waarin aangegeven wordt: - Hoe complex een wachtwoord minimaal moet zijn. - Wat de verantwoordelijkheid van een gebruiker rond wachtwoorden is.	Binnen de organisatie bestaat er een wachtwoordbeleid waarin aangegeven wordt: - Hoe complex een wachtwoord minimaal moet zijn. - Wat de verantwoordelijkheid van een gebruiker rond wachtwoorden is. - Wachtwoorden zijn uniek.	De organisatie heeft een wachtwoordbeleid waarin de volgende punten zijn vastgelegd: - Minimale complexiteit wachtwoorden. - Gebruik en omschrijving van sterke wachtwoorden (het voorkomen van toepassen van makkelijk te raden wachtwoorden). - Verantwoordelijkheden gebruiker binnen het proces. - Werken met unieke wachtwoorden. - Wachtwoorden worden op een veilige afgesproken plek bewaard. - Indien het tradiotenele systemen betreft (zonder hardware key of MFA) dienen wachtwoorden met een vaste interval vervangen te worden.
Organisatorisch	0+1+2/Intermediate	5.24	Verantwoordelijkheden en procedures	Zijn directieverantwoordelijkheden en -procedures vastgesteld om adequaat op informatiebeveiligingsincidenten te reageren?	Er zijn geen formele procedures vastgesteld, maar iedereen weet bij wie hij/zij moet zijn als er zich een incident voordoet.	Er zijn diverse procedures aanwezig voor onder andere respons op en monitoren/rapporteren van incidenten. Er is een contactpunt in de organisatie en competent personeel bij betrokken. Definities zijn vastgesteld en standaard formulieren worden gebruikt.	Aanvullend op level 2: Er worden passende contacten onderhouden met instanties, belangengroepen en fora. Procedures omtrent forensisch bewijsvoering zijn aanwezig. Er vindt een verwijzing plaats naar disciplinaire procedures en er wordt feedback teruggegeven naar de melder van het incident.
Organisatorisch	0+1+2/Intermediate	5.25	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Worden incidenten binnen de organisatie geregistreerd?	Incidenten worden binnen de organisatie geregistreerd, informatiebeveiligingsincidenten worden als dusdanig aangegeven.	Incidenten worden binnen de organisatie geregistreerd, informatiebeveiligingsincidenten worden als dusdanig aangegeven. Ieder incident wordt voorzien van een prioriteit en er is vastgelegd welke oplossingstijden verbonden zijn aan deze prioriteiten. Registratie van deze incidenten is van een dermate niveau dat oorzaak en gevolg duidelijk is en wat er gedaan is om het probleem te verhelpen.	Incidenten worden binnen de organisatie geregistreerd, informatiebeveiligingsincidenten worden als dusdanig aangegeven. Ieder incident wordt voorzien van een prioriteit en er is vastgelegd welke oplossingstijden verbonden zijn aan deze prioriteiten. Binnen de organisatie is iemand verantwoordelijk voor informatiebeveiligingsincidenten. Deze persoon beoordeelt en classificeert deze incidenten en monitort het verloop. Deze incidenten worden inclusief oorzaakanalyse, verloop en oplossing tot in detail vastgelegd om in de toekomst van te leren.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Organisatorisch	0+1+2/Intermediate	5.26	Respons op informatiebeveiligingsincidenten	Worden incidenten binnen de organisatie behandeld?	Informatiebeveiligingsincidenten worden binnen de organisatie behandeld en opgelost.	Informatiebeveiligingsincidenten worden binnen de organisatie zo behandeld en opgelost dat er altijd: - Een oorzaakanalyse aanwezig is. - Duidelijk omschreven staat wat de impact van het incident is. - Wat gedaan is om het incident te verhelpen. - Wat de structurele oplossing is.	Informatiebeveiligingsincidenten worden binnen de organisatie afgehandeld waarbij de volgende punten opgenomen zijn: - Wat is de impact op de organisatie van het incident. - Welke systemen zijn er geraakt en wat is hier de impact op. - Welk bewijs is er aanwezig en waar is dit veilig gesteld. - Is het eventueel nodig om crisismanagement toe te passen en wordt er volgens gemaakte afspraken geëscaleerd. - Voorziet de verslaglegging in een eenduidig beeld van de uitgevoerde handelingen. - Belanghebbenden worden voorzien van de benodigde informatie middels het need-to-know principe. - Bij afronding van het incident wordt deze formeel gesloten en opgeslagen. - Afhankelijk van het soort incident wordt er forensisch onderzoek uitgevoerd. - Een incident beschikt uiteindelijk o.a. over een oorzaakanalyse en een oplossing. Indien er mogelijk een trend aanwezig is of overkoepelend risico bestaat, wordt deze in kaart gebracht en behandeld volgens de afspraken binnen de organisatie.
Organisatorisch	0+1+2/Intermediate	5.3	Scheiding van taken	Worden taken binnen de organisatie gescheiden?	De organisatie maakt gebruik van rollen voor gebruikers en streeft least privilage na.	Rollen zijn zo samengesteld en toegekend dat deze onderling geen conflicten veroorzaken.	Er wordt met rollen gewerkt en een geautomatiseerd proces houdt toezicht op wijzigingen en mogelijke conflicten.
Organisatorisch	0+1+2/Intermediate	5.31	Vaststellen van toepasselijke wetgeving en contractuele eisen	Wordt rekening gehouden met contractuele informatiebeveiligingseisen en eisen vanuit relevante wet-/regelgeving?	Er is bekend door welke partijen (wetgeving, klanten, verzekeraars etc.) informatiebeveiligingseisen worden opgelegd aan de organisatie.	Het is inzichtelijk door welke partijen (wetgeving, klanten, verzekeraars etc.) informatiebeveiligingseisen worden opgelegd aan de organisatie en er is een aanpak vastgesteld om hier invulling aan te geven.	De organisatie houdt zich aan informatiebeveiligingseisen welke opgelegd zijn vanuit wetgeving en contractuele eisen. De volgende zaken zijn vastgelegd binnen de betreffende procedure(s): - Bij het opstellen en wijzigen van beheersmaatregelen rond informatiebeveiliging wordt rekening gehouden met de hierboven genoemde eisen. - Bij het classificeren van informatie en middelen, het houden van risico analyses en het toekennen van rollen en rechten wordt hier ook rekening mee gehouden. - Voor het toepassen van cryptografische beheersmaatregelen en middelen wordt rekening gehouden met de wetgeving en contractuele eisen.
Organisatorisch	0+1+2/Intermediate	5.32	Intellectuele eigendomsrechten	Wordt intellectueel eigendom door de organisatie gerespecteerd?	De organisatie werkt alleen met legale software en informatie. Eigen gemaakte producten (denk aan b.v. softwareontwikkelaar) zijn voorzien van een licentieovereenkomst.	De organisatie werkt alleen met legale software en informatie. Er wordt toezicht gehouden op het hiermee juist omgaan (niet vaker installeren dan toegestaan, geen illegale software) en er kan worden aangetoond dat de organisatie ook daadwerkelijk eigenaar is. Eigen gemaakte producten (denk aan b.v. softwareontwikkelaar) zijn voorzien van een licentieovereenkomst.	De organisatie heeft geborgd dat licentieovereenkomsten en zaken rond intelectueel eigendom zo geborgd zijn dat deze aansluiten op de bijbehorende eisen. Zaken welke door de organisatie zelf zijn gebouwd en worden aangeboden zijn ook voorzien van dergelijke overeenkomsten. De volgende zaken zijn daarbij aanwezig: - Er bestaan procedures voor het omgaan met rechten rond het gebruik van software en informatie producten. - Software mag alleen verkregen worden van door de organisatie vertrouwde bronnen. - Er is een policy binnen de organisatie voor wat betreft intelectueel eigendom. - Het eigenaarschap kan aangetoond worden. - Bij licentieovereenkomsten i.c.m. maximaal gebruik (denk aan CPU, gebruikers etc.) wordt toezicht gehouden. - Er wordt toezicht gehouden op geïnstalleerde software op systemen. - Er is grip op licentie gebruik. - Er zijn procedures voor het afschrijven van licenties of het overdragen hiervan. - Een kopie maken is niet toegestaan, tenzij de overeenkomst anders zegt.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Organisatorisch	0+1+2/Intermediate	5.33	Beschermen van registraties	Heeft de organisatie registraties als bewijs van naleving voor compliance doeleinden?	De organisatie heeft inzichtelijk welke datastromen er zijn en heeft de logging veilig gesteld waarbij voldaan wordt aan wetgeving, contractuele afspraken en eigen policy.	Er bestaat een verwerkingsregister binnen de organisatie welke voorziet in het identificeren van de verschillende soorten informatie. Er zijn afspraken gemaakt rond het gebruik en de bewaartermijn van deze informatie.	Er is een verwerkingsregister aanwezig binnen de organisatie welke voorziet in het identificeren van verschillende voorkomende soorten informatie. Voor deze soorten informatie zijn er afspraken vastgelegd welke aantoonbaar nageleefd worden rond opslag en beheer hiervan. Opslag en omgang vinden op een manier plaats welke overeenkomen met de aanbevelingen van de betreffende leveranciers. Bij langdurige opslag is rekening gehouden met op termijn kunnen uitlezen van informatie. Denk daarbij aan media waarvoor op termijn geen hardware meer verkregen kan worden om deze uit te lezen. Voor alle gebruikte soorten media bestaan richtlijnen voor hoe om te gaan met de volgende zaken: - Wat voor soort opslag betreft het. - Hoe dient hiermee omgegaan te worden. - Hoe moet e.e.a. vernietigd worden. - Hoe lang moet informatie bewaard worden.
Organisatorisch	0+1+2/Intermediate	5.36	Naleving van beveiligingsbeleid/-normen	Beoordeelt de directie de naleving van informatieverwerking en -procedures a.d.h.v. de eigen beleidsregels, normen en eisen m.b.t. beveiliging?	Naleving van eigen beleidsregels, normen en eisen vindt ad hoc plaats en/of als daartoe aanleiding is.	Naleving van eigen beleidsregels, normen en eisen vindt periodiek plaats ten behoeve waarvan een meet- en rapportage-instrument wordt gehanteerd.	Binnen de organisatie wordt getoetst of daadwerkelijk het beleid rond informatiebeveiliging wordt nageleefd. Er zijn maatregelen genomen om te toetsen of binnen de organisatie aan alle eisen gesteld door de eigen organisatie, wetgeving en andere belanghebbenden voldaan wordt. Bij afwijkingen wordt de volgende informatie vastgelegd: - Welke afwijking het betreft. - De oorzaak van de afwijking. - De noodzaak van een correctieve actie. - Implementatie van een correctieve actie. - Toetsing van de effectiviteit van de correctieve actie en identificatie van mogelijk rest risico. - Tijdspanne waarin bovenstaande allemaal afgehandeld zal zijn.
Organisatorisch	0+1+2/Intermediate	5.4	Directieverantwoordelijkheden	Is er een informatiebeveiliging beleid aanwezig binnen de organisatie?	Dit beleid is voor alle medewerkers toegankelijk en wordt ook aantoonbaar nageleefd.	Dit beleid omschrijft de richtlijnen van de organisatie op het gebied van informatiebeveiliging, bevat een procedure rond klokkenluiders. Dit beleid wordt aantoonbaar nageleefd.	Management heeft aantoonbaar geborgd dat personeel: - Beschikking heeft over richtlijnen op het gebied van informatiebeveiliging, weet wat hun verantwoordelijkheden zijn op dit gebied en ook over de benodigde rechten, resources en tijd beschikken deze uit te kunnen voeren. - Beschikking heeft over een klokkenluidersprocedure waarmee anoniem (of op een manier waarop veiligheid van de melder geborgd is) melding gemaakt kan worden van schendingen van het informatiebeleid die de organisatie (kunnen) schaden.
Organisatorisch	0+1+2/Intermediate	5.8	Informatiebeveiliging in projectbeheer	Komt informatiebeveiliging aan bod in projecten en worden beveiligingseisen meegenomen in het aanschaffen/aanpassen van systemen?	In sommige projecten komt informatiebeveiliging aan de orde. Informatiebeveiligingseisen worden ad hoc bekeken. In sommige gevallen worden risicobeoordelingen uitgevoerd als onderdeel van het projectplan. Veel hangt af van individuele competenties.	In alle projecten worden implicaties van informatiebeveiliging behandeld en beoordeeld. Risicobeoordelingen vinden in een vroeg stadium v/h project plaats als onderdeel van het risicobeheerproces waarin risico's worden geïdentificeerd. Concrete eisen (logging etc.) en risico's worden bepaald o.b.v. van algemene criteria en zijn niet altijd volledig afgestemd op de bedrijfsdoelstellingen.	Zekerheid te krijgen dat getroffen maatregelen op het gebied van informatiebeveiliging nog steeds aansluiten op de situatie in de wereld.
Personeel	0+1+2/Intermediate	6.5	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Wordt door de organisatie rekening gehouden met impact op de informatiebeveiliging na wijziging van functie of uitdiensttreding van een medewerker?	De organisatie houdt rekening met functies en rollen op het gebied van informatiebeveiliging bij wijzigingen in het personeelsbestand.	De organisatie houdt rekening met functies en rollen op het gebied van informatiebeveiliging bij wijzigingen in het personeelsbestand. Medewerkers weten dat zij bij uitdiensttreding zich moeten houden aan de geldende afspraken rond het informatiebeveiligingsbeleid, denk daarbij aan geheimhoudingsplicht.	Onderdeel van de procedures rond wijzigen functies en uitdiensttreding is medewerkers erop wijzen dat na het verlaten van het bedrijf gehouden moet worden aan de geldende afspraken uit het informatiebeveiligingsbeleid. Functies die betrekking hebben op de informatiebeveiliging van de organisatie zijn geborgd, raken niet onbemand en blijven ook bij dergelijke wijzigingen functioneren.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Privacy	0+1+2/Intermediate	B.8.2.4	Opdracht die inbreuk oplevert	Wordt de klant op de hoogte gesteld als zijn opdracht wet- en/of regelgeving schendt?	Of de klant in kennis gesteld wordt indien een verwerkingsopdracht inbreuk oplevert op toepasselijke wet- en/of regelgeving, hangt sterk af van individuen.	Indien een verwerkingsopdracht inbreuk oplevert op toepasselijke wet- en/of regelgeving dan wordt de klant daar informeel van in kennis gesteld.	De klant wordt schriftelijk in kennis gesteld indien een verwerkingsopdracht inbreuk oplevert op toepasselijke wet- en/of regelgeving.
Privacy	0+1+2/Intermediate	B.8.4.2	Retournering, doorgifte of verwijdering van persoonsgegevens	Kunnen persoonsgegevens desgewenst geretourneerd, overgedragen of verwijderd worden?	Als de klant op beveiligde wijze persoonsgegevens geretourneerd wenst, over te laten dragen en/of te laten verwijderen, dan zullen we dit desgevraagd ad hoc doen.	Er zijn voorzieningen om persoonsgegevens op beveiligde wijze te retourneren, over te dragen en/of te verwijderen. Beleid hieromtrent ontbreekt of wordt de klant niet kenbaar gemaakt.	De mogelijkheid wordt geboden om persoonsgegevens op beveiligde wijze te retourneren, over te dragen en/of te verwijderen. Beleid hieromtrent wordt aan de klant ter beschikking gesteld.
Privacy	0+1+2/Intermediate	B.8.5.3	Registraties van de verstrekking van persoonsgegevens aan derden	Wordt een verstrekking van persoonsgegevens aan derden geregistreerd?	Of de verstrekking van persoonsgegevens aan derden wordt vastgelegd, als ook wel informatie daarvan wordt geregistreerd, hangt van individuen af.	Verstrekking van persoonsgegevens aan derden wordt pragmatisch en inconsistent vastgelegd.	Verstrekking van persoonsgegevens aan derden wordt geregistreerd, met inbegrip van welke persoonsgegevens zijn verstrekt, aan wie en wanneer.
Technologisch	0+1+2/Intermediate	8.14	Beschikbaarheid van informatieverwerkende faciliteiten	Zijn er binnen de organisatie maatregelen getroffen om de beschikbaarheid van de betreffende dienstverlening op het gewenste niveau te houden?	Er is binnen de organisatie stilgestaan bij de eisen vanuit wetgeving en contractuele afspraken met klanten rond beschikbaarheid van de dienstverlening van de organisatie. Er zijn maatregelen getroffen om aan deze eisen te voldoen.	Binnen de organisatie is in beeld aan welke wettelijke eisen en contractuele afspraken voldaan moet worden met oog op beschikbaarheid. Getroffen maatregelen zijn passend bij deze eisen. Er bestaat een procedure waarin dit is vastgelegd. Voor kritieke processen zijn contracten met 2 of meer leveranciers, denk aan internet providers. Processen en systemen zijn zo ingeregeld dat deze gebruik maken van redudante oplossingen, passend bij de geeiste beschikbaarheid.	Binnen de organisatie is in beeld aan welke wettelijke eisen en contractuele afspraken voldaan moet worden met oog op beschikbaarheid. Getroffen maatregelen zijn passend bij deze eisen. Er bestaat een procedure waarin dit is vastgelegd en omvat de volgende punten: - Voor kritieke processen zijn contracten met 2 of meer leveranciers, denk aan internet providers - Gebruik van redudante netwerken - Gebruik van 2 datacenters op verschillende locaties welke gespiegeld zijn - Gebruik van redudante voedingen en groepen - Gebruik van parallelle verwerkingen van software voorzien van een load balancer - Reduntante hardware In geval van het actief worden van een fail over (storing en de redudante oplossing grijpt in) wordt dit automatisch gedaan en wordt er melding van gemaakt.
Technologisch	0+1+2/Intermediate	8.16	Monitoren van activiteiten	Wordt afwijkend gedrag in netwerken, systemen en applicaties gemonitord?	Netwerken, systemen en applicaties worden ad hoc gecontroleerd op afwijkend gedrag.	Netwerken, systemen en applicaties worden gecontroleerd op afwijkend gedrag en passende maatregelen worden genomen om mogelijke informatiebeveiligingsincidenten te evalueren. Monitoring wordt realtime gedaan of met periodieke tussenpozen.	Netwerken, systemen en applicaties worden gecontroleerd op afwijkend gedrag en passende maatregelen worden genomen om mogelijke informatiebeveiligingsincidenten te evalueren.
Technologisch	0+1+2/Intermediate	8.17	Kloksynchronisatie	Wordt op systemen waarop informatie wordt verwerkt, rekening gehouden met kloksynchronisatie?	Uitgangspunt is dat systemen naar dezelfde tijd kijken omdat proffesionals deze hebben geïnstalleerd en geconfigureerd. Zeker weten doet de organisatie het niet, maar het heeft (tot op heden) niet tot problemen geleid.	Binnen de organisatie is bekend op welke systemen informatie wordt verwerkt en op deze systemen is kloksynchonisatie actief. Aangetoond kan worden naar welke klok wordt gekeken.	Binnen de organisatie is bekend op welke systemen informatie wordt verwerkt en op deze systemen is kloksynchonisatie actief. Indien er gebruik gemaakt wordt van meerdere verschillende diensten rond kloksynchronisatie (b.v. door het gebruik van clouddiensten) wordt het onderlinge verschil tussen de kloksynchronisatie in de gaten gehouden.
Technologisch	0+1+2/Intermediate	8.22	Scheiding in netwerken	Worden informatieverwerkende systemen van van elkaar gescheiden?	Er zijn maatregelen getroffen om informatieverwerkende systemen zo van elkaar te scheiden dat er geen onnodige koppelingen bestaan. Voorbeelden hiervan zijn netwerk segmentering en scheiding van dergelijke systemen van het internet door het toepassen van b.v. een firewall.	Informatieverwerkende systemen die niet met elkaar verbonden hoeven te zijn, zijn van elkaar en de buitenwereld gescheiden. Waar mogelijk wordt netwerksegmentering toegepast.	Informatieverwerkende systemen die niet met elkaar verbonden hoeven te zijn, zijn van elkaar en de buitenwereld gescheiden. Waar mogelijk wordt netwerksegmentering toegepast. Draadloze netwerken staan niet rechtstreeks in contact met deze systemen. Deze worden gescheiden en dienen middels een extra beveiligingslaag contact hiermee kunnen leggen wanneer nodig.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0+1+2/Intermediate	8.29	Testen van beveiliging tijdens ontwikkeling en acceptatie	Wordt er tijdens of na het ontwikkelproces getest op security?	Onderdeel van het ontwikkelproces en/of de oplevering is testen op security.	Onderdeel van de ontwikkeling en levencyclus is het testen op het gebied van security. Er bestaan richtlijnen binnen de organisatie die voorzien in de volgende punten: - Waar moet de applicatie qua security aan voldoen - Hoe vaak wordt er tijdens het in gebruik zijn van de software opnieuw bij deze eisen stilgestaan - Op welke manier wordt er getest, tijdens het ontwikkelen en erna op code en omgeving - Wanneer wordt er een code review gedaan of 4 ogen principe toegepast - Wanneer gaat code life	Onderdeel van de ontwikkeling en levencyclus is het testen op het gebied van security. Er bestaan richtlijnen binnen de organisatie die voorzien in de volgende punten: - Security functies, b.v. op het gebied van authenticatie en cryptografie - Veilig coderen - Security configuraties inclusief de omgeving en randzaken zoals firewalls e.d. Er bestaat een testplan wat uitgevoerd wordt voordat software life gaat. Hierin zijn de volgende punten opgenomen: - Welke activiteiten onderdeel zijn van het testen - Welke input gebruikt wordt en wat de verwachte output van het systeem zal zijn - Welke criteria van toepassing zijn bij het beoordelen van de resultaten - Welke beslissingen in welke situatie genomen zullen worden Indien software ontwikkeld wordt door de eigen organisatie, moeten de volgende overwegingen gemaakt worden door een onafhankelijk persoon buiten het ontwikkelteam: - Uitvoeren van code review, zijn de gemaakte afspraken daarbij gevolgd en vallen er geen afwijkingen op bij verwerkingen - Scannen op kwetsbaarheden, zijn de systemen wel zo beveiligd als verwacht wordt - Uitvoeren van een pentest op onveilige code en ontwerp
Technologisch	0+1+2/Intermediate	8.30	Uitbestede softwareontwikkeling	Worden er software ontwikkelwerkzaamheden uitbesteed?	Er worden software ontwikkelwerkzaamheden uitbesteed en er zijn afspraken gemaakt met de leverancier rond eigenaarschap en werkzaamheden.	Er worden software ontwikkelwerkzaamheden uitbesteed. Er zijn afspraken met de leverancier gemaakt welke het volgende bevatten: - Licentieovereenkomst / eigenaarschap - Security vereisten van ontwikkelomgeving leverancier - Security en privacy by design - Organisatie blijft verantwoordelijk voor voldoen aan wet en regelgeving	Er worden software ontwikkelwerkzaamheden uitbesteed. Er zijn afspraken met de leverancier gemaakt welke het volgende bevatten: - Licentieovereenkomst / eigenaarschap - Contractuele afspraken rond security en privacy by design, veilig coderen en testen - Risicoanalyse applicatie - Organisatie voert definitieve test zelf uit voor lifegang - Aantoonbaarheid dat geleverde door leverancier voldoet aan gewenste van organisatie - Escrow overeenkomst welke software veilig stelt bij problemenen leverancier - Recht tot uitvoeren audit - Security vereisten van ontwikkelomgeving leverancier - Organisatie blijft verantwoordelijk voor voldoen aan wet en regelgeving
Technologisch	0+1+2/Intermediate	8.6	Capaciteitsbeheer	Wordt capaciteit van middelen binnen de organisatie gemonitord?	Capaciteit van (enkele) informatieverwerkende systemen wordt gemonitord en er zijn mechanismen die (dreigende) overschrijding detecteren. Organisatie is reactief is daartoe (tot op heden) in staat gebleken.	Er zijn beleidsregels omtrent capaciteitsmanagement waarin tevens (toekomstige) capaciteitseisen zijn gedefinieerd. Rekening is gehouden met de mate waarin systemen bedrijfskritisch zijn en met andere type middelen.	Er is een formeel beleid m.b.t. het beheren van de capaciteit van middelen waarbij is opgenomen: - Informatieverwerkende systemen - Menselijke capaciteit - Kantoorruimte - Andere faciliteiten die verstorend kunnen werken Rekening is gehouden met uitbreiding van de capaciteit of het verlagen van de druk d.m.v: - Inhuur van extra personeel - Uitbreiden of aankoop nieuwe ruimte - Aanschaf krachtigere systemen - Vrij maken van opslagruimte - Verwijderen van informatie welke de retentieperiode hebben overschreden - Uit gebruik nemen van overbodige applicaties, databases, systemen en omgevingen - Optimaliseren van geautomatiseerde processen en schema's - Optimalisatie programmatuur en database queries

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Organisatorisch	0+1+2+3/Advanced	5.14	Informatietransport	Wordt er bij uitwisseling van informatie rekening gehouden met de bedrijfsregels hiervoor?	Bij het uitwisselen van informatie bestaan er bedrijfsregels om de bijbehorende vertrouwelijkheid en integriteit hiervan te borgen.	Bij het uitwisselen van informatie bestaan er bedrijfsregels om de bijbehorende vertrouwelijkheid en integriteit hiervan te borgen. Er is een aantoonbaar eigenaarschap van de informatie. Er is bekend wie toegang mag krijgen tot de betreffende informatie.	Er bestaan binnen de organisatie procedures, welke aantoonbaar nageleefd worden, rond het uitwisselen van informatie. Deze procedures omschrijven de volgende punten: - Wat voor soort media het betreft (digitaal, fysiek etc.). - Wie is er verantwoordelijk. - Wie krijgt toegang tot de informatie. - Hoe wordt de informatie overgedragen. - Hoe wordt de informatie beveiligd, inclusief eventuele bijlagen. - Hoe betrouwbaar is de manier van informatie uitwisseling op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid. - Welke labels worden hoe toegepast. - Aantoonbaarheid van het consequent toepassen van deze regels is geregeld.
Organisatorisch	0+1+2+3/Advanced	5.28	Verzamelen van bewijsmateriaal	Wordt bewijsmateriaal verzameld in het geval zich een informatiebeveiligingsincident voordoet?	Wanneer zich een dergelijk incident voordoet, wordt er bewijsmateriaal verzameld. Denk hierbij aan log files van systemen e.d.	Wanneer zich een dergelijk incident voordoet, wordt er bewijsmateriaal verzameld rond het gehele incident.	Wanneer zich een dergelijk incident voordoet, wordt er bewijsmateriaal verzameld rond het gehele incident door gekwalificeerd personeel. Het niveau van het bewijsmateriaal is zo dat het tijdens een mogelijke rechtzaak toegepast kan worden. De kwaliteit van het personeel kan aangetoond worden middels b.v. certificaten en diploma's.
Organisatorisch	0+1+2+3/Advanced	5.30	ICT-gereedheid voor bedrijfscontinuïteit	Zijn bedrijfscontinuïteitseisen en ICT-continuiteitseisen op elkaar afgestemd?	Bij een verstoring van de zakelijke dienstverlening wordt er binnen de organisatie zo gehandeld dat de informatiebeveiliging blijft functioneren.	Bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen zijn bekend en gebaseerd op een bedrijfsimpactanalyse (BIA). Hersteltijddoelstellingen (RTO) worden toegekend als input voor de strategie voor ICT-gereedheid.	De ICT-gereedheid wordt gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.
Organisatorisch	0+1+2+3/Advanced	5.35	Onafhankelijke beoordeling van informatiebeveiliging	Wordt het beheer en de implementatie van informatiebeveiliging onafhankelijk beoordeeld?	De organisatie laat informatiebeveiliging ad hoc toetsen door een onafhankelijk persoon t.o.v. het te beoordelen gebied (interne auditor, onafhankelijk manager of externe organisatie).	De organisatie laat informatiebeveiliging periodiek en bij grote wijzigingen toetsen door een onafhankelijk persoon t.o.v. het te beoordelen gebied (interne auditor, onafhankelijk manager of externe organisatie).	Aanvullend op level 2: Bij deze toetsing worden de volgende zaken meegenomen: - Wet en regelgeving welke betrekking hebben op de organisatie. - Incidenten. - Wijziging van strategie van de organisatie of het starten van nieuwe zaken. - Wijzigingen aan het informatiebeleid welke (mogelijk) risico's met zich meebrengen.
Organisatorisch	0+1+2+3/Advanced	5.5	Contact met overheidsinstanties	Wordt er contact onderhouden met relevante overheidsinstanties?	Waar nodig wordt contact onderhouden met deze instanties.	Er is een overzicht van relevante overheidsinstanties en voor welk doel hiermee contact gezocht wordt.	Er is een overzicht van relevante overheidsinstanties. Bij iedere instantie staat wie hiermee contact opneemt, in welke situatie, op welke manier en welke reactietijden van toepassing zijn.
Organisatorisch	0+1+2+3/Advanced	5.6		Worden relevante informatiekanalen in de gaten gehouden?	Er worden infomatiekanalen in de gaten gehouden welke aansluiten bij de organisatie.	De organisatie wordt op de hoogte gehouden door informatiekanalen en actief te zijn in andere belangengroepen waar gecommuniceerd wordt over zaken welke relevant zijn voor (beveiliging van) de organisatie.	De organisatie is lid van belangengroepen of forums met als doel: - Op de hoogte te blijven van kennis van best practices en andere relevante informatie op het gebied van informatiebeveiliging. - Zekerheid te krijgen dat getroffen maatregelen op het gebied van informatiebeveiliging nog steeds aansluiten op de situatie in de wereld. - In een vroeg stadium op de hoogte te blijven van mogelijk bedreigingen op het gebied van informatiebeveiliging, denk aan beschikbare updates e.d. - Toegang te hebben tot experts. - Informatie kunnen uitwisselen op het gebied van informatiebeveiliging. - In geval van incidenten toegang te hebben tot personen welke ondersteuning kunnen bieden.
Personeel	0+1+2+3/Advanced	0	Disciplinaire procedure	Staan er voor medewerkers sancties op het plegen van inbreuken op de informatiebeveiliging?	Medewerkers die handelen in strijd met het beleid van de organisatie rond informatiebeveiliging kunnen hierop aangesproken worden, ook al zijn ze over deze mogelijkheid niet geïnformeerd en/of is er geen sanctiebeleid vastgesteld.	Wanneer medewerkers handelen in strijd met het beleid rond informatiebeveiliging kunnen zij een sanctie opgelegd krijgen. Over deze mogelijkheid zijn ze geïnformeerd ook al is niet exact duidelijk welke sancties het kunnen zijn en/of t.o.v. welke norm of welk beleid deze van toepassing is.	Er bestaat een sanctiebeleid binnen de organisatie. Wanneer medewerkers handelen in strijd met het beleid rond informatiebeveiliging kunnen zij volgens deze procedure een sanctie opgelegd krijgen. Deze sancties zijn in lijn met geldende wet- en regelgeving. Deze procedure bevat de volgende zaken: - Hoe, wat, wanneer en hoe is de overtreding begaan, wat is de ernst van de situatie en wat is de impact op de organisatie. - Was er opzet in het spel. - Was dit de eerste keer dat de medewerker een dergelijke overtreding beging. - Was de medewerker ervaren genoeg om de fout niet te maken.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0+1+2+3/Advanced	8.11	Maskeren van gegevens	Wordt (persoons)gevoelige informatie binnen de organisatie gemaskeerd, gepseudonimiseerd en/of geanonimiseerd?	Maskeren, pseudonimiseren en/of anonimiseren vindt plaats op initiatief van betrokken medewerkers.	Toegang tot persoonsgevoelige informatie wordt beperkt en er wordt met pseudonimiseren en anonimiseren van deze informatie gewerkt om de groep geautoriseerde medewerkers zoveel mogelijk te beperken.	Toegang tot (persoons)gevoelige informatie wordt in lijn met het beleid hieromtrent beperkt met technieken als maskeren, pseudonimiseren en/of anonimiseren. De gebruikte methoden zijn getest en door de organisatie goedgekeurd. Bij anonimisatie zijn individuen niet terug te herleiden, zowel direct als indirect. Indien gebruik wordt gemaakt van hash functies worden deze gecombineerd met een salt functie. Verwijzingen naar bronnen (zoals internet adressen) wordt voorkomen.
Technologisch	0+1+2+3/Advanced	8.18	Speciale systeemhulpmiddelen gebruiken	Wordt het gebruik van programma's/systemen die beheersmaatregelen kunnen omzeilen, beperkt en gecontroleerd?	Gebruik van dergelijke middelen wordt ontraden maar niet uitgesloten. Medewerkers zijn professioneel genoeg en worden hierop niet gemonitord.	Dergelijke oplossingen worden niet gebruikt of er is toezicht in een vorm die traceerbaar maakt wat er gebeurd is.	De organisatie heeft een basislijn vastgesteld van normaal gedrag en controleert deze op afwijkingen. Er wordt gebruikgemaakt van continue monitoring m.b.v. een tool. Monitoring wordt realtime gedaan of met periodieke tussenpozen. Monitoringdata wordt bijgehouden voor de duur van gedefinieerde bewaartermijnen.
Technologisch	0+1+2+3/Advanced	8.23	Toepassen van webfilters	Wordt toegang tot externe websites beheerst?	Medewerkers zijn geïnstrueerd wat voor soort websites zij wel en niet mogen bezoeken. Hierbij wordt sterk geleund op het professionele gedrag van medewerkers.	De organisatie heeft geïdentificeerd en gecommuniceerd tot welke type websites medewerkers wel of geen toegang hebben. Tenminste enkele hiervan zijn technisch ontoegankelijk gemaakt.	De organisatie heeft geïdentificeerd tot welke type websites medewerkers wel of geen toegang hebben. Medewerkers zijn getraind op dergelijke risico's. Websites worden in lijn met het beleid geblokkeerd rekeninghoudend met platformen waar zich (mogelijk) illegale inhoud bevindt of waar data geupload kan worden op een manier die niet strookt met de bedrijfsregels. Het platform dat voor detectie en blokkade zorgt, houdt zichzelf up-to-date.
Technologisch	0+1+2+3/Advanced	8.27	Principes voor engineering van beveiligde systemen	Worden er principes gehanteerd t.b.v. de engineering van beveiligde systemen?	Bij het opzetten van servers, diensten en schrijven van eigen applicaties wordt er stilgestaan bij het veilig opzetten en vervolgens houden van dergelijke omgevingen.	Bij het opzetten van servers, diensten en schrijven van eigen applicaties wordt er stilgestaan bij het veilig opzetten en vervolgens houden van dergelijke omgevingen. Er wordt rekening gehouden met best practices uit de praktijk zoals segmentatie waar mogelijk.	Bij het opzetten van servers, diensten en schrijven van eigen applicaties is security by design een vast onderdeel. Voor het starten aan dergelijke projecten wordt er een risicoanalyse gemaakt welke stilstaat bij de volgende punten: - Welke risico's wordt het project aan bloot gesteld. - Welke vormen van logging en monitoring zijn er nodig om inzicht te krijgen op de bedreigingen. - Welke mogelijkheden zijn er nodig om in te grijpen in geval van dat er zich een calamiteit dreigt voor te doen of voordoet. - Wat moet er gedaan worden om de kans op een incident zo klein mogelijk te maken en de impact zo beperkt mogelijk te houden. Bij al deze maatregelen dient rekening gehouden te worden met: - Integratie in het security landschap. - De organisatie moet in staat zijn dit te kunnen ontwikkelen en uitrollen. - Kosten, tijd en complexiteit dienen inzichtelijk te zijn. - Waar mogelijk gebaseerd te zijn op best practices. - Review op het project vanuit het punt security. - Documentatie dient volledig te zijn en indien er functionaliteit gebruikt wordt welke het rechten systeem van de organisatie overbrugt, dient dit vermeld en door management goedgekeurd te worden. Informatie van de organisatie dient op een manier beschermd te worden waarbij voor het verlenen van toegang rekening gehouden wordt met: - Systemen reeds gehackt zijn. - Vertrouw nooit, maar controleer principe. - Controleer bij iedere aanvraag de afzender. - Hanteer least-privililage.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0+1+2+3/Advanced	8.28	Veilig coderen	Worden er principes gehanteerd t.b.v. het schrijven van veilige code?	Bij programmeerwerkzaamheden wordt op een veilige manier gewerkt. Hiervoor is geen vastomlijnd proces of vastgestelde set aan (codeer)standaarden. Geleund wordt op de professie van de medewerkers.	Er wordt geprogrammeerd door gekwalificeerde medewerkers op een manier die als veilig gezien kan worden. Er wordt gebruik gemaakt van één of meerdere (codeer)standaarden en meerdere praktijken (zoals code reviewing en/of het gebruik van tools)	Er wordt geprogrammeerd door gekwalificeerde medewerkers op een manier die als veilig gezien kan worden. Voor het starten met programmeren wordt rekening gehouden met de volgende punten: - Veiligheidseisen rond gebruikte methoden en verwachtingen gesteld door de organisatie voor interne ontwikkeling en uitbestede ontwikkeling. - Welke situaties vermeden moeten worden gebaseerd op ervaringen om de kans op kwetsbaarheden te beperken. - Gebruik van richtlijnen. - Het gebruik van een up-to-date ontwikkel omgeving. - Gebruik van gekwalificeerde medewerkers. - Veilig ontwerp en architectuur waarbij rekening is gehouden met bedreigingen. - Gebruik van standaarden rond veilig coderen. - Gebruik van afgeschermde ontwikkel omgevingen. Tijdens het programmeren wordt er op een manier gewerkt zoals vastgelegd in een bijbehorende procedure. Hierin staat omschreven hoe er met de OTAP (ontwikkel / test / acceptatie / productie) straat gewerkt wordt en het beheer verloopt. Onderdeel hiervan zijn de volgende punten: - Welke ontwikkel technieken / standaarden worden er gebruikt. - Hoe en waar wordt gedocumenteerd. - Het voorkomen van onveilige code. - Het integreren van een review proces door andere medewerkers. - Verwerken van updates op alle manieren, denk daarbij aan externe bibliotheken. - Logging. - Licenties. - Hoe omgaan met gevonden kwetsbaarheden. - Lange termijn beschikbaarheid. - Indien mogelijk ooit eigenaarschap veranderd (intern naar extern etc.) en hoe hiermee omgegaan wordt. - Compabiliteit.
Technologisch	0+1+2+3/Advanced	8.31	Scheiding van ontwikkel-, test en productieomgevingen	Worden er bij software ontwikkelwerkzaamheden gescheiden omgevingen gebruikt tijdens ontwikkeling en productie?	Er wordt bij het ontwikkelen een andere omgeving gebruikt dan waar productie actief is.	Bij softwareontwikkeling wordt er gewerkt middels een OTAP-straat en-proces. Alle stappen van ontwikkeling tot aan productie vinden plaats op hun eigen omgeving. Er zijn maatregelen getroffen ter voorkoming van verwisseling test en productie informatie met elkaar. Er bestaat een procedure welke het ontwikkelen binnen de OTAP-straat behandeld. Er zijn daarin afspraken gemaakt over controle en test momenten.	Bij softwareontwikkeling wordt er gewerkt middels een OTAP straat en proces. Alle stappen van ontwikkeling tot aan productie vinden plaats op hun eigen omgeving. Deze omgeving is zo gescheiden dat het niet mogelijk is dat informatie tussen onderlinge omgevingen door elkaar gebruikt worden. Er bestaan procedures die borgen dat er een vaste methode gebruikt wordt om het OTAP-proces te doorlopen. Hierbij wordt niet getest in productie omgevingen, tenzij hier gerichte afspraken over zijn gemaakt. Wanneer niet nodig zijn ontwikkeltools en toegang tot betreffende omgevingen niet beschikbaar. Er zijn maatregelen getroffen om het risico van gevoelige informatie in code naar productie te publiceren te voorkomen door te werken met labels in b.v. menu structuren en afspraken rond niet kopiëren van gevoelige informatie De OTAP omgeving wordt up-to-date gehouden middels de policy van de organisatie waarbinnen bibliotheken, besturingssyteem en software op ontwikkelsystemen ook vallen. Alle systemen gebruikt binnen het OTAP proces zijn zo geconfigureerd dat deze als veilig bevonden worden door de organisatie en worden gemonitord op afwijkingen.

Categorie	CYRA 2.0	Norm-element	Onderwerp (NL)	Vraag	Level 1	Level 2	Level 3
Technologisch	0+1+2+3/Advanced	8.33	Bescherming van testgegevens	Wordt zorgvuldig omgegaan met testdata?	Het gebruik van operationele databases met persoonsgegevens of anderszins vertrouwelijke informatie vindt regelmatig plaats. Er is geen beleid omtrent vastgesteld, maar medewerkers zijn wel gewezen op hun verantwoordelijkheid om hier zorgvuldig mee om te gaan.	Het gebruik van operationele databases met persoonsgegevens of anderszins vertrouwelijke informatie wordt vermeden dan wel beperkt. Indien toch noodzakelijk dan worden gevoelige details beschermd en de testdata z.s.m. weer verwijderd.	Er is een procedure m.b.t. test data. Deze procedure heeft als doel het borgen van de vertrouwelijkheid van de informatie binnen de productie data waarbij test resultaten wel een zo juist mogelijk beeld geven. De richtlijnen in de procedure beschrijven: - Welke toegang tot productie systemen nodig is om toegang te krijgen tot de productie data. - Het afdwingen van een autorisatie iedere keer dat er een koppeling gemaakt moet worden van productie naar test. - Het bijhouden van logging rond rond toegang van data uit de productie omgeving. - Het eventuele opschonen van data. - Het verwijderen van data na afronden test.
Technologisch	0+1+2+3/Advanced	8.34	Beheersmaatregelen betreffende audits van informatiesystemen	Wordt rekening gehouden met mogelijke verstoringen t.g.v. verificaties/testen voorkomend uit audits?	Er zijn mogelijkheden om een audit af te nemen op productiesystemen. Afhankelijk van de inschatting van betrokken personeel wordt gecontroleerd of dit geen onacceptabele verstoringen met zich meebrengt.	Er zijn mogelijkheden om een audit af te nemen op productiesystemen. De impact op productie wordt expliciet beoordeeld en wordt daarbij beperkt.	Er zijn mogelijkheden om een audit af te nemen op productiesystemen waarbij impact op productie beperkt wordt. De procedure welke omschrijft hoe hiermee om te gaan bevat de volgende punten: - Het proces rond toestemming verkrijgen voor het uitvoeren van de audit. - Akkoord gaan met de scope. - Toegangsystemen beperken tot alleen lezen. - Bij verlenen toestemming rekening houden met veiligheidseisen systemen auditor, zoals virusscanner e.d. - Bij gebruik speciale software, hier toestemming voor verkrijgen. - Indien er impact kan zijn op productie capaciteit hier afspraken over maken. - Monitoring en logging van alle activiteiten.
Technologisch	0+1+2+3/Advanced	8.4	Toegangsbeveiliging op programmabroncode	Wordt de toegang tot programmabroncodes beheerst?	Toegang tot broncode is beperkt tot een afgeschermde groep medewerkers.	Toegang tot broncode is beperkt tot een afgeschermde groep medewerkers welke over niet meer rechten beschikken dan nodig om werkzaamheden uit te voeren. Wijzigingen aan broncode worden centraal bijgehouden.	Toegang tot broncode binnen de organisatie is zo geregeld dat dit alleen middels de door het bedrijf bepaalde tooling kan gebeuren. Gebruikers waarvoor toegang geregeld is, hebben alleen rechten tot systemen en functionaliteiten voor de benodigde werkzaamheden. Wijzigingen worden centraal geregistreerd in een versiebeheersysteem voorzien van een log waarin toegang en wijzigingen met code wordt bijgehouden. Waar mogelijk zijn voorzorgsmaatregelen getroffen om de integriteit van de broncode te borgen.
Technologisch	0+1+2+3/Advanced	8.9	Configuratiebeheer	Worden configuraties binnen de organisatie gedocumenteerd?	Binnen de organisatie worden van systemen configuraties gedocumenteerd.	Binnen de organisatie worden van systemen die informatiebeveiliging raken de configuraties gedocumenteerd en up-to-date gehouden. Indien er wijzigingen aangebracht moeten worden is bekend door wie dit moet gebeuren.	Binnen de organisatie worden van systemen (software, hardware en diensten) die informatiebeveiliging raken de configuraties zo vastgelegd dat de volgende punten geborgd zijn: - Waar mogelijk verwijzing naar publieke templates en best-practices. - Hoe komt de geboden mate van veiligheid overeen met dat wat wenselijk is. - Op welke manier voor deze configuratie stilgestaan wordt bij ontwikkelingen binnen de wereld en organisatie. - Hoe de groep welke wijzigingen aan kunnen brengen beperkt kunnen worden tot een werkbaar minimum. - Hoe en wanneer rechten beoordeeld en herzien worden. - Synchronisatie van klokken. - Wijzigen van standaard login gegevens van leveranciers. - Automatisch uitloggen na bepaalde tijd. - Wie is de eigenaar van het systeem. - Wat voor log wordt bijgehouden waarin vast staat welke wijzigingen wanneer en door wie zijn aangebracht en goedgekeurd samen met andere mogelijke relevante informatie.