TRAIN THE TRAINER

Hulpgids voor personen en organisaties die MKB begeleiden

in hun groei van cyberweerbaarheid

Hulpgids gebaseerd op ervaringen van anderen
Versie 28 mei 2026

Evelien Bras

The Cyber Partners

contact@thecyberpartners.com

Voorwoord

Dit *Train the Trainer*-document is ontwikkeld vanuit één centrale overtuiging: duurzame impact ontstaat niet door kennisoverdracht alleen, maar door het trainen van mensen om anderen te leren denken, handelen en reflecteren.

Dit document is bedoeld voor trainers die bedrijven (willen) begeleiden in het behalen van een cybersecurity certificaat. Het bevat veel 'best practices' van trainers die al enkele jaren in dit veld actief zijn. Het is opgeschreven als werktekst, niet als eindpunt. Het vraagt om actieve lezing en om toepassing in de praktijk. Alles wat opgeschreven is, is "Experience based". Trainers die dit programma doorlopen, worden niet geacht het klakkeloos te volgen, maar het kritisch te gebruiken, aan te scherpen om het toepasbaar te maken voor hun publiek en daar waar nodig tegen te spreken of uit te breiden. Alleen zo blijft trainen een levend vak.

Wie dit document leest, staat aan het begin – of midden – van een leerproces dat verder reikt dan vaardigheden. Het gaat over houding, over verantwoordelijkheid nemen voor het leerproces van anderen, en over de bereidheid om zelf steeds opnieuw leerling te blijven.

> ***Een trainer is geen consultant.***
> ***Als consultant los je de problemen van een bedrijf op.***
> ***Als trainer leer je het bedrijf om zélf de oplossing te bedenken.***

Inhoudsopgave

1 Voorbereiding

1.1 Introductie op cyber

Digitalisering heeft bedrijven veel voordelen gebracht. We werken sneller, slimmer en flexibeler. Maar het heeft ook een nieuwe kwetsbaarheid gemaakt: cyberrisico's. Cyber is geen apart IT-onderwerp meer dat je kunt overlaten aan specialisten. Het raakt het hele bedrijf: hoe mensen werken, beslissingen nemen en verantwoordelijkheid dragen. Trainers spelen hierin een belangrijke rol.

Cyberdreigingen groeien snel. Sneller dan regels, techniek en bewustzijn kunnen bijhouden. Aanvallen zijn geen uitzondering meer, maar dagelijkse realiteit. Denk aan phishing, ransomware, datalekken en misleiding. Het probleem zit daarbij niet alleen in "onwetende medewerkers". Vaak gaat het mis door werkdruk, onduidelijke afspraken, tijdgebrek, tegenstrijdige belangen of slechte organisatie.

Daarom is cyber geen puur technisch probleem. Het is een samenspel van mens, organisatie en techniek. Systemen falen meestal niet alleen door techniek, maar doordat mensen ermee moeten werken in een lastige praktijk. Cyberweerbaarheid vraagt om goed nadenken, alert zijn op situaties en keuzes maken met – soms onvolledige – informatie. Precies dat zijn vaardigheden die trainers kunnen helpen ontwikkelen.

Voor trainers verandert hierdoor de rol. Het gaat niet om het afvinken van lijstjes of het onthouden van regels. Het gaat om het begeleiden van mensen die:

- Willen of moeten gaan begrijpen waarom cybermaatregelen nodig zijn,
- Herkennen wanneer vaste routines niet meer werken, en
- Durven handelen, ook als ze niet alle antwoorden hebben.

Deze training is het startpunt voor trainers. Niet alleen regels volgen, maar werken aan weerbaarheid, verantwoordelijkheid en volwassen oordeelsvorming.

1.1.1 Het verschil tussen cybersecurity en digitale weerbaarheid

Cybersecurity gaat over beveiligen en voorkomen. Het zijn vaak een som van technische maatregelen, gezien als onderdeel van 'informatiebeveiliging'. Voorbeelden zijn firewalls, wachtwoorden, updates en procedures. De centrale vraag bij cybersecurity is: *"Hoe houden we aanvallen buiten de deur?"*

Digitale weerbaarheid gaat over omgaan met risico's en verstoringen. Het kijkt naar wat mensen en organisaties doen als het tóch misgaat. Denk aan alertheid, besluitvorming, samenwerking, herstel en leren van fouten. De centrale vraag bij digitale weerbaarheid is: *"Wat doen we als het fout gaat, en hoe blijven we functioneren?"*

- Cybersecurity = voorkomen
- Digitale weerbaarheid = herkennen, handelen, herstellen en leren

Een organisatie kan technisch goed beveiligd zijn. Maar als medewerkers phishing niet melden, fouten verbergen of niet weten wie beslist bij een incident, dan is de digitale weerbaarheid laag. In dit document stellen we de risicoanalyse van een bedrijf (organisatie) als startpunt centraal en werken – middels een framework – aan digitale weerbaarheid.

1.1.2 Wetten en regels: focus van techniek, naar mens naar bestuur

Het cyberwerkveld is de afgelopen jaren sterk veranderd. Waar cyber vroeger vooral een technisch onderwerp was, is het nu een organisatie- en bestuursvraagstuk geworden.

In het begin lag de focus op techniek. IT-afdelingen moesten systemen beveiligen, firewalls instellen en virussen tegenhouden. Cyber was "iets van de IT". Daarna werd duidelijk dat techniek alleen niet genoeg is.

De meeste incidenten ontstonden niet door falende systemen, maar door menselijk handelen: phishingmails, verkeerde keuzes onder tijdsdruk, onduidelijke verantwoordelijkheden. De aandacht verschoof naar gedrag, bewustzijn en training.

Vandaag is de volgende stap gezet: cyber ligt bij het bestuur.

Cyberincidenten kunnen bedrijfscontinuïteit, reputatie en zelfs veiligheid van mensen raken. Daarmee is cyber een onderwerp geworden voor directie, management en toezichthouders. Overheden eisen middels wetgeving steeds vaker dat organisaties:

- risico's structureel in kaart brengen
- maatregelen vastleggen en naleven
- incidenten melden
- en kunnen aantonen dat ze "in control" zijn

Belangrijke wetten en regels die nu gelden of eraan komen zijn onder andere:

- AVG (GDPR) – bescherming van persoonsgegevens
- CWB: Cyberweerbaarheidswet, een Nederlandse wet volgend op de Europese NIS2-richtlijn die in een 18-tal sectoren eisen stelt aan digitale en operationele weerbaarheid
- De Cyber Resilience Act (CRA), is een EU-wet die strenge cybersecurity-eisen stelt aan alle digitale producten (hardware en software) die in de EU worden verkocht. Fabrikanten, importeurs en distributeurs krijgen daarmee verantwoordelijkheden, inclusief een verplichting tot 'security-by-design', het leveren van updates en een meldplicht voor kwetsbaarheden.
- Sectorale normen en richtlijnen (zoals ISO-normen, BIO, zorg- en onderwijsregels)

Deze regels gelden niet alleen voor grote organisaties. Ook MKB-bedrijven krijgen ermee te maken, direct of via klanten en ketenpartners. Door deze wetten is compliance een vast onderdeel geworden van het werkveld.

Compliance betekent: kunnen aantonen dat je regels kent, toepast en naleeft. Dat heeft gevolgen voor de praktijk:

- meer beleid en documentatie
- duidelijke rollen en verantwoordelijkheden
- vastgelegde processen en controles
- training en bewustwording van medewerkers

Compliance gaat niet alleen over regels volgen, maar over aantoonbaar verantwoord handelen.

1.1.3 Frameworks

Maar hoe toon je aan dat je verantwoord handelt? In het huidige werkveld is "we doen ons best" niet meer genoeg. Organisaties moeten kunnen aantonen dat zij risico's kennen, afwegen en beheersen. Dat geldt bij incidenten, audits, klanten, toezichthouders en bestuur.

De centrale vraag is niet meer:

"Hebben we maatregelen genomen?"

maar:

"Kunnen we laten zien waarom we deze keuzes maken en hoe we ze borgen?"

Verantwoord handelen betekent dat je risico's bewust in kaart brengt, bewuste keuzes maakt over wat je wel en niet afdekt, deze keuzes vastlegt en regelmatig controleert en bijstuurt.

Niet alles hoeft perfect veilig te zijn. Maar alles moet uitlegbaar en verdedigbaar zijn. Een framework is een gestructureerd denk- en werkkader dat hierbij helpt. Een framework schrijft meestal niet exact voor wat je moet doen, maar hoe je moet nadenken en organiseren.

Voor meer informatie over frameworks en welke we tegenkomen inclusief hun werkveld, zie Bijlage A.

1.2 Het verschil tussen principle-based en rule-based

In wetgeving, frameworks en compliance zie je twee fundamenteel verschillende manieren van sturen: rule-based en principle-based. Het verschil bepaalt sterk hoe professionals moeten denken en handelen.

Rule-based betekent dat gedrag wordt gestuurd door concrete, vastgelegde regels. De vraag is steeds:

"Volg ik de regel, ja of nee?"

Principle-based werken betekent handelen op basis van kernprincipes en professionele afwegingen. De vraag is hier: "Handel ik in de geest van het doel?"

De Nederlandse wetgever heeft gekozen voor een 'principle-based' implementatie van de cyberweerbaarheidswet. Dat betekent dat een organisatie altijd begint met een eigen risicoanalyse: waar loop ik risico voor mezelf – voor anderen – en hoe maak ik mijn doelen inzichtelijk?

Voor veel MKB is dit een lastige manier van werken – het afvinken van een lijstje is eenvoudiger – maar een mooie rol waar trainers hen bij kunnen helpen.

1.2.1 Startpunt voor dit document: CYRA, niveau: entry, level 3 (defined)

CYRA is een framework dat door de Nederlandse overheid wordt erkend en gebruikt en dat een duidelijk instapniveau voor MKB-organisaties biedt.

De scope van dit document is vastgesteld op entry level 3.

Er is bewust gekozen voor het niveau "entry" met het kleinste aantal controls. Dit betekent dat slechts een beperkt aantal principes van toepassing is, waaraan voldaan moet worden. Deze principes vormen de basis voor verantwoord handelen op het gebied van cyber en digitale weerbaarheid.

Hoewel het aantal controls beperkt is, moeten zij op een gedefinieerde ('defined') manier worden ingericht. Dat houdt in dat keuzes, verantwoordelijkheden en werkwijzen duidelijk zijn vastgelegd. Juist deze structuur zorgt ervoor dat organisaties hun handelen aantoonbaar kunnen maken, wat essentieel is voor compliance en verantwoording.

1.3 Welke kennis moet ik in huis hebben? Startkwalificatie trainer

Als trainer werk je in het overlapgebied van meerdere disciplines. Je bent niet per se een specialist in één hoek, maar verbindt verschillende perspectieven met elkaar.

- Cybersecurity als werkveld
- De CYRA tooling en controls, een subset van de ISO27001 controls
- Kennis van beschikbare termen, best practices en handvatten[1]
- Mogelijkheid om kennis over te dragen en deelnemers te activeren
- Kennis en begrip van de aard en werkwijze – beleidsvoering – van de organisaties waarmee je werkt

Dit document helpt je vooral met de CYRA controls en de tooling en begrip van het werkveld. Het behandelt de meestgestelde vragen en veelvoorkomende situaties. Het is zinnig om als start wel al kennis van de denkwereld van de bedrijven waarmee je werkt te hebben: weten hoe hun primaire processen lopen en welke risico's ze hebben.

1.4 Het kiezen van een werkvorm om bedrijven te begeleiden

Er wordt vaak gevraagd **om 1-op-1 begeleiding** door de bedrijven zelf.

Dat is begrijpelijk: vanuit het perspectief van bedrijven is dit een logische start wanneer er weinig andere bedrijven zijn die men vertrouwt om mee samen te werken. In een 1-op-1 setting kunnen direct vragen worden gesteld en onzekerheden worden weggenomen. Dit houdt het veilig voor een organisatie.

Tegelijkertijd is 1-op-1 begeleiding slecht schaalbaar en creëert het het risico op consultancy-afhankelijkheid ("zeg maar wat ik moet doen"). Door dit als standaard startpunt te nemen, leer je gedrag aan dat je later weer af wilt leren: externe sturing in plaats van eigen verantwoordelijkheid.

Samenwerken in leerkringen kan minstens zo effectief zijn, mits goed ontworpen.

Groepsdruk vergroot vaak de succeskansen ("als zij dit kunnen, moeten wij het ook kunnen"). Diezelfde groepsdruk kan echter ook averechts werken. Bedrijven kunnen afhaken wanneer:

- het niveau sterk uiteenloopt (te ver voor of juist te ver achter),
- de problematiek onvoldoende overeenkomt,
- of wanneer men zich niet veilig voelt om informatie te delen.

Wanneer er een groep bedrijven is die bereid is om informatie te delen en voldoende overlap heeft – bijvoorbeeld in scope, risicoprofiel, volwassenheid en/of sector – is een werkgroep van 10 tot 15 bedrijven een geschikte werkvorm. In deze setting ontstaat herkenning, sociale vergelijking en onderlinge versnelling, zonder dat het leerproces verzandt in individuele problematiek.

Een werkvorm is voordoen–meedoen–zelf doen, eventueel ondersteund door een voorbeeldbedrijf. Bij alle werkvormen is het belangrijk om de verhouding presenteren versus zelf aan de slag te bewaken. Een richtlijn is 20% theorie en 80% actief werken.

Ervaring leert dat het voor veel bedrijven lastig is om tussen sessies door zelfstandig door te werken als de sessies alleen uit het delen van de theorie bestaat. Dit komt niet alleen door tijdsdruk, maar ook door verlies van momentum en onduidelijk eigenaarschap.

Daarom is het binnen leerkringen aan te bevelen om sessies in te plannen waarin ruimte is voor 'samen doen', 'samen werken'. Als trainer breng je dan niet alleen kennis over maar ben je ook coach voor het voorbereiden van de juiste beslissing.

[1] Zie hiervoor ook het template informatiebeveiligingsbeleidsdocument van “Brasholt Hekwerk BV”

Ook is een werkvorm waarin deelnemende bedrijven twee dagen aaneengesloten werken een interessante variant. In zo'n opzet worden juist besluiten genomen en keuzes vastgelegd, wat de kans op daadwerkelijke opvolging vergroot.

> ***Let als trainer op dat je de werkvorm kiest die het juiste gedrag en de juiste resultaten stimuleert, let vooral op eigenaarschap, besluitvorming en uitvoering. Zeg ook gerust 'nee' als de werkvorm niet past bij de doelstelling.***

1.5 Beslisboom / overwegingen bij het opzetten van een leerkring

Onderstaand staan overwegingen bij het opzetten van een leerkring als beslisboom weergegeven:

Overweging 1: Is er een externe noodzaak?

Bijvoorbeeld wetgeving, klanteis, audit, incident, directie-opdracht.

- Nee → Start kort, afgebakend met een risicoanalyse, dit kan bijvoorbeeld door een voorbereidende 1 op 1 sessie. Doel: probleem scherp krijgen, nog geen oplossingen uitwerken.
- Ja → Ga door naar overweging 2.

Overweging 2: Is er mandaat aanwezig?

Neemt de deelnemer beslissingen over beleid, budget of prioriteiten of heeft deze bevoegdheid van de directie om dit onderwerp op te pakken?

- Nee → Wellicht is een 'introductiecursus' cyber beter geschikt. Deelname alleen zinvol met expliciete opdracht van directie, of aanwezigheid van beslisser bij beslismomenten.
- Ja → Ga door naar overweging 3.

Overweging 3: Is er voldoende overlap tussen bedrijven?

Zoek de overeenkomsten, bijvoorbeeld in: risicoprofiel, volwassenheid, doelstelling (bijv. CYRA entry), gemeenschappelijke deadline, sector/type bedrijfsvoering, omvang organisatie.

- Nee → Geen vaste werkgroep voor uitwerking mogelijk. Alternatief: thematische sessies of gefaseerde groepen (start/gevorderd).
- Ja → Ga door naar overweging 4.

Overweging 4: Is er bereidheid tot delen?

Openheid over aanpak, knelpunten, keuzes – geen details, wel richting.

- Nee → Geen leerkring, wel gezamenlijke sessies waarna ieder individueel aan de slag gaat. De trainer zal meer centraal blijven staan in het aanbod van kennis.
- Ja → Ga door naar overweging 5.

Overweging 5: Kunnen deelnemers tijd vrijmaken?

Minimaal 2 aaneengesloten dagen of vaste blokken.

- Nee → Dit is een waarschuwingssignaal. Verwacht lage opvolging. Overweeg kortere maar verplichte beslissessies, minder inhoud, meer keuzes.
- Ja → Geschikt voor leerkring 10-15 bedrijven: voordoen–meedoen–zelf doen, gezamenlijke reflectie.

2 Starten met de analyse en de tool

2.1 Wat betekent cyber voor organisaties van jouw klanten?

Jouw klanten moeten begrijpen waar hun bedrijf afhankelijk is van digitale middelen en van anderen. De volgende vragen helpen dat in kaart te brengen en/of om het gesprek te starten:

- **Welke risico's zijn er voor de organisatie?**
  Denk aan uitval van systemen, verlies van gegevens, fouten door menselijk handelen of misbruik van accounts. Wat gebeurt er als dit misgaat, en wat is daarvan de impact op het bedrijf?

- **Hoe wordt er nu met die risico's omgegaan?**
  Zijn er nu al afspraken, maatregelen of procedures? Of wordt er vooral gereageerd als er iets misgaat?

- **Hoe afhankelijk is de organisatie van digitale systemen?**
  Welke processen kunnen niet doorgaan zonder IT, internet of software? Wat ligt direct stil als systemen uitvallen?

- **Hoe afhankelijk is de organisatie van anderen?**
  Van leveranciers (bijv. IT-dienstverleners, cloudleveranciers) en van klanten (digitale koppelingen, portals, data-uitwisseling)?

  Wat gebeurt er als een leverancier uitvalt of een klant niet kan aansluiten?

Deze vragen helpen om cyberrisico's concreet en herkenbaar te maken. Ze vormen het startpunt voor keuzes over maatregelen, prioriteiten en verantwoordelijkheden.

2.2 Het doen van een risicoanalyse

Een start van een goede cyberaanpak is altijd een risicoanalyse. Een bedrijf begint met het in kaart brengen van wat belangrijk is voor de organisatie: systemen (bijv. boekhouding, planning), informatie (klantgegevens, offertes) en processen (productie, levering). Daarna stel je per onderdeel drie simpele vragen: wat kan er misgaan, hoe groot is de kans, en wat is de impact als het gebeurt.

Dit hoeft niet exact; "laag / middel / hoog" is voor MKB vaak voldoende. Vervolgens kijk je welke maatregelen al bestaan en bepaal je welk rest-risico overblijft. Alleen die risico's die zowel waarschijnlijk als pijnlijk zijn, verdienen prioriteit. Een veelgemaakte fout is om alle risico's gelijk te behandelen of te starten vanuit een norm in plaats van vanuit de bedrijfsrealiteit.

> ***!! Begin altijd bij het werkproces en de risico's, begin nooit direct bij het framework.***

Concreet MKB-voorbeeld: Brasholt Hekwerk BV

Een hekwerkbedrijf gebruikt voor op kantoor één cloudpakket voor planning en facturatie, maakt gebruik van een gedeelde cloud-drive en heeft in de fabriek een machine.

De meest belangrijke processen zijn als eerste het produceren van hekwerk door de machine in de fabriek en als tweede de planning voor plaatsing en de facturatie. Alle andere processen zijn secundair, waarvan de directie de verantwoordelijkheid voor de uitval van de processen acceptabel vindt.

Risico: uitval of gijzeling (ransomware) van machine.
Kans: middel tot hoog (het is een ouder systeem)
Impact: hoog (geen productie)
Bestaande maatregel: geen

Risico: uitval of gijzeling (ransomware) van cloudpakket & cloud-drive.
Kans: middel (veel aanvallen in de sector).
Impact: hoog (geen facturen, geen planning).
Bestaande maatregel: wachtwoord + back-up.

Deze bovenstaande risico’s worden gebruikt voor het treffen van de juiste maatregelen. Pas na deze risicoinventarisatie wordt het meest passende framework gekozen.

Gratis en toegankelijke tooling voor risicoanalyse:

NCSC Stappenplan Risicoanalyse (NL)

https://www.ncsc.nl/risicomanagement/stappenplan-risicoanalyse
Goede start voor bewustwording en eerste prioriteiten. Voor MKB is deze analyse volledig.

ENISA Risk Assessment Method

https://www.enisa.europa.eu/topics/risk-management
Iets formeler, nuttig voor trainers die verdieping zoeken.

CYRA tooling (NL, overheidserkend)

https://www.hetccv.nl
Geeft een paar opties voor risicoanalyse in de keten. Sluit aan op MKB-niveau en ISO-doorgroei.

> ***Kanttekening voor trainers: een 'ruwe maar gedeelde' risicoanalyse die elk half jaar wordt herhaald is inhoudelijk sterker dan een perfecte analyse die in een la verdwijnt. Train dus besluitvorming, niet documentproductie.***

2.3 Van risico naar raamwerk

Afhankelijk van je risico én de vraag uit je omgeving kies je een specifiek raamwerk waarmee je aan de slag gaat. Zie voor een overzicht van raamwerken Bijlage A. Wie vraagt bewijs van jouw cybersecurity maatregelen?

Voor organisaties zonder ervaring met cybersecurity-certificering biedt CYRA[2] een belangrijk voordeel: het is stapsgewijs opgezet. Je kunt groeien van 'ad-hoc' maatregelen naar 'defined' en je kunt groeien in het aantal controls.

De praktijk laat zien dat MKB-bedrijven die direct van nul naar ISO 27001 willen, vaak vastlopen in detail, documentatie en abstractie; de stap is te groot.

Binnen deze train-de-trainer-opleiding wordt daarom gewerkt met CYRA Entry – niveau 3 (well-defined). Dit niveau is gekozen vanwege:

- de expliciete focus op MKB,
- de ondersteuning en herkenning door de Nederlandse overheid,
- en de eenvoud en toepasbaarheid van de methodiek.

[2] In dit document wordt – als er over “CYRA” wordt gesproken, “CYRA-IT” bedoeld. Zie het hoofdstuk over CYRA voor verdere uitleg hierover.

2.4 Over ISO27001

ISO/IEC 27001 is een internationale norm voor het opzetten, invoeren en verbeteren van een Information Security Management System (ISMS). In eenvoudige taal: ISO 27001 helpt organisaties om gestructureerd en aantoonbaar om te gaan met informatiebeveiliging.

Voor veel MKB-organisaties is ISO 27001 te zwaar als startpunt. De administratieve last, documentatie-eisen en auditstructuur kunnen leiden tot focus op "voldoen aan de norm" in plaats van daadwerkelijk risico's beheersen. In de praktijk wordt ISO 27001 daarom vaak alleen gebruikt:

- wanneer klanten of ketenpartners dit eisen,
- bij organisaties met hogere risico's of complexere IT-omgevingen,
- of als vervolgstap, nadat de basis al op orde is.

ISO27001 bevat 93 zogeheten 'controls'. Een control is een maatregel die je neemt om een specifiek risico te beheersen.

2.5 Kent de organisatie ISO 9001 al?

Veel organisaties hebben al een ISO certificaat, zoals 9001 voor kwaliteit. Het helpt de implementatie door de documenten geïntegreerd op te pakken. Dus niet voor CYRA separate beleidsdocumenten van scratch te beginnen, maar om de beleidsdocumenten die al zijn opgesteld voor de ISO 9001 te hergebruiken als basis voor de CYRA implementatie.

ISO 9001 richt zich op het leveren van constante kwaliteit, ISO 27001 op het beschermen van informatie — maar ze organiseren dit met vrijwel hetzelfde managementmodel. Zowel de context van de organisatie, het nemen van leiderschap en verantwoordelijkheid en in basis risicodenken, het implementeren van Plan-Do-Act-Check en het eisen van bestuurlijke verantwoordelijkheid zijn gelijk.

Ook voorkomt deze aanpak een aantal denkfouten en onuitgesproken aannames:

“Informatieveiligheid - implementatie van CYRA -
kunnen we bij IT of kwaliteit neerleggen”
Nee.

Beide normen – zowel ISO27001, als ISO9001, eisen bestuurlijke verantwoordelijkheid, niet delegatie zonder mandaat.

“ISO27001 is veel bureaucratischer dan ISO9001.”

In werkelijkheid: ISO 9001 vraagt hetzelfde, maar organisaties zijn eraan gewend geraakt. De mechanismes zijn identiek. Informatiebeveiligingsbeleid is vaak nieuwer en ‘voelt’ daarom als bureaucratischer, wat het niet is. Een andere onjuiste aanname:

“Als we ISO 9001 hebben,
is ISO 27001 maar een kleine stap.”

In beide moeten medewerkers competent zijn, moeten ze weten wat hun rol is en
moet kennis geborgd zijn. De managementlaag is weliswaar herbruikbaar maar informatieveiligheid is een eigen vakgebied; de risicoanalyse, controls en maatregelen vergen nieuwe keuzes. Als een bestuurder dit vakgebied moet leren als bestuurder, wordt dat lastig gevonden en is daarmee gevoelsmatig geen kleine stap.

Juist omdat ISO27001 ervaren wordt als een grote stap is; het framework bevat 93 controls, is de aanpak middels CYRA, waarbij het aantal controls aanzienlijk kleiner is, meer acceptabel.

2.6 Over CYRA

CYRA staat voor Cyber Rating en is een praktisch raamwerk dat organisaties helpt om hun digitale weerbaarheid stap voor stap te verbeteren. Het is ontwikkeld om vooral MKB-organisaties houvast te geven bij cybersecurity, zonder dat het direct zo zwaar en complex wordt als internationale normen zoals ISO-27001.

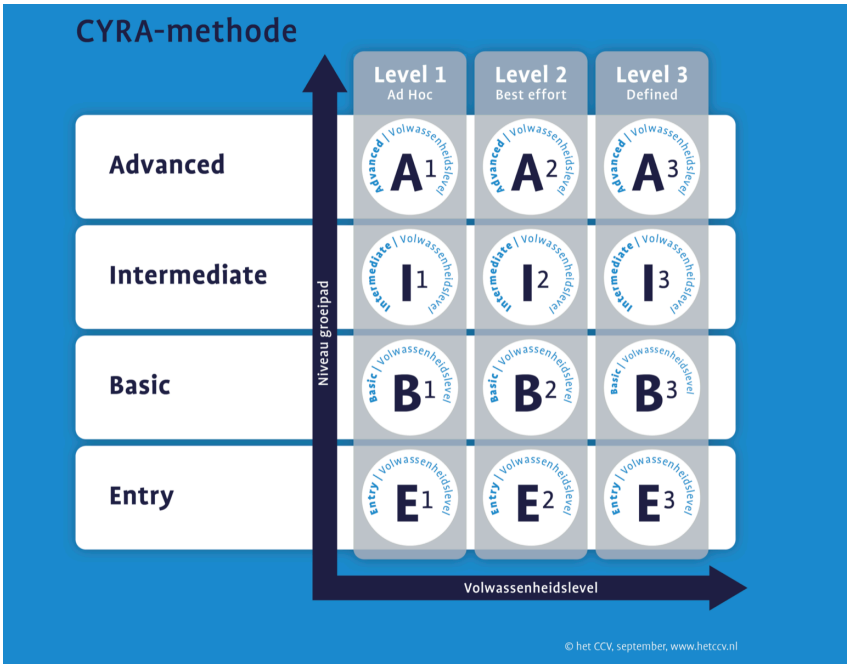
De focus ligt niet op techniek alleen, maar op het geheel: risico's herkennen, verantwoordelijkheden vastleggen, passende maatregelen nemen en kunnen uitleggen waarom je iets doet.

CYRA bestaat uit een gratis framework en een tool, waarvoor een gebruikersfee wordt gevraagd.

CYRA bestaat uit vier niveaus:

- Entry
- Basic
- Intermediate
- Advanced

Elk niveau bestaat uit drie volwassenheidslevels.



Voor meer informatie over CYRA, zie: https://hetccv.nl/keurmerken/cybersecurity/cyra/

Tip: om zelf te begrijpen hoe CYRA werkt, probeer eens zelf de tool in te vullen met aan de ene kant de tool en aan de andere kant een “informatiebeheersproces”, een document waar je voor je eigen of voor een fictief bedrijf de maatregelen opsomt.

Toegang tot de tool kun je verkrijgen via: https://app.cyberrating.nl

Wat kost het gebruik van de tool?

De bijdrage voor kosten van de tooling zijn afhankelijk van het aantal medewerkers:

1-10 medewerkers	€ 90,- per jaar
11-50 medewerkers	€ 150,- per jaar
51-250 medewerkers	€ 300,- per jaar
> 250 medewerkers	€ 600,- per jaar

Zie voor meer informatie:

https://hetccv.nl/app/uploads/2025/10/Tarievenblad-Cybersecurity-2026.pdf

Per bedrijf kun je meerdere gebruikers – maximaal 5 – gebruik laten maken van het account.
Deze kosten bevatten niet de certificering of de kosten voor het certificaat. Zie de FAQ voor de kosten van certificeren.

Is de tool gratis te gebruiken? (Partnercode)

Het framework CYRA is gratis te gebruiken door het framework vanaf de site te gebruiken. Wil je het gemak van de tool, staat daar bovenstaand bedrag voor.

Er zijn grote organisaties of samenwerkingsverbanden die voor hun deelnemers een partnercode beschikbaar stellen. Met een partnercode kan een organisatie ketenpartners uitnodigen om zich te registreren, waardoor je als deelnemer geen bijdrage betaalt; de uitnodigende organisatie faciliteert het eerste abonnementsjaar.

2.6.2 CYRA-IT, CYRA-OT, CYRA-ZORG en NDO

CYRA is een “opstap naar”, geschikt voor MKB. CYRA-IT is de eerste vorm waarin deze beschikbaar is gekomen, ook wel de ‘originele CYRA’ genoemd. CYRA-IT richt zich op IT omgevingen (werkplekken, servers, cloud en gebruikers) en relateert primair aan ISO/IEC 27001 en ISO/IEC 27002; het gaat hier om governance, toegangsbeheer, logging, incidentmanagement en leveranciersbeheersing.

Al snel werd onderkend dat ook voor OT (Operationele Technologie) omgevingen de behoefte bestond aan een instap, stapgewijze aanpak van CYRA.

CYRA-OT focust op industriële omgevingen (PLC’s, SCADA, productielijnen) en sluit inhoudelijk aan bij IEC 62443; beschikbaarheid, veiligheid en fysieke impact staan centraal, met afwijkende keuzes t.o.v. IT (bijv. patchen en segmentatie).

CYRA-ZORG is afgestemd op de zorg en relateert aan NEN 7510 (informatiebeveiliging in de zorg), aangevuld met ISO 27001-principes en AVG-vereisten; continuïteit van zorg en patiëntveiligheid wegen hier zwaarder dan strikte vertrouwelijkheid alleen.

CYRA-NDO is bedoeld voor organisaties waar ondermijning een sterk risicoprofiel is en bevat controls – grotendeels maar niet alleen uit ISO27001 – die een keurmerk vormt tegen ondermijnende criminaliteit.

De overlap tussen alle CYRA-varianten zit in de kernprincipes (risicoanalyse, beleid, incidentrespons, leveranciersmanagement en bewustwording); het verschil zit in de prioritering en diepgang van controls: IT en ZORG delen veel governance-controls, OT wijkt technisch sterk af maar deelt het risicodenken, en NDO gebruikt een 10-tal controls met name gericht op ondermijnende criminaliteit (voor specialisten: “insider-risk”).

2.6.3 Hoe de tool te gebruiken? Voor groei en voor certificering

Het gebruik van de tool (van het framework) heeft typisch twee doelstellingen:

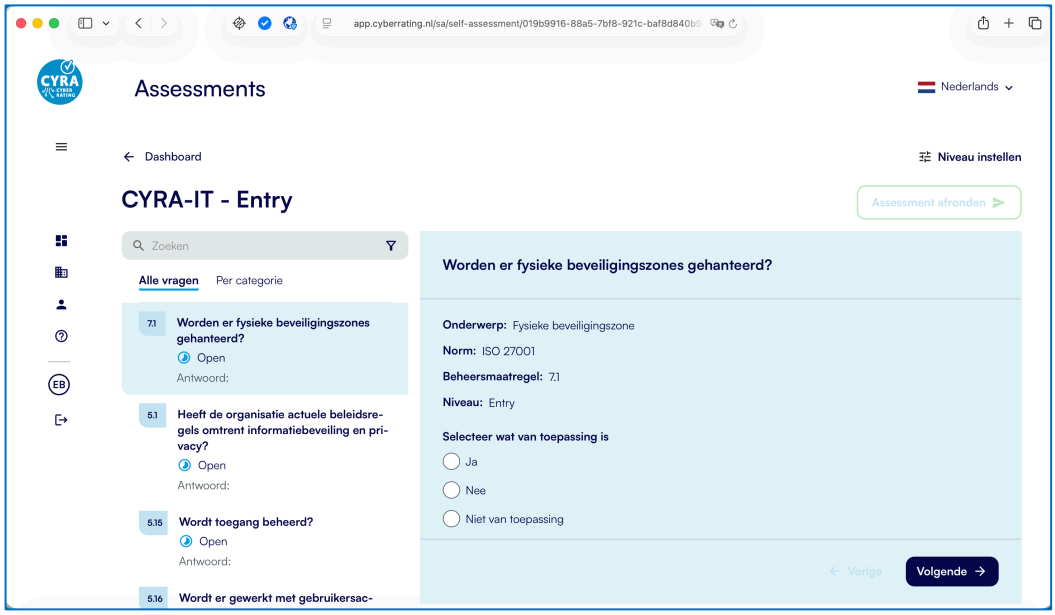
- Gebruik om stap voor stap beter te worden
- Gebruik om een certificaat te behalen

Deze twee doelstellingen kunnen elkaar opvolgen, maar dat hoeft niet per se.

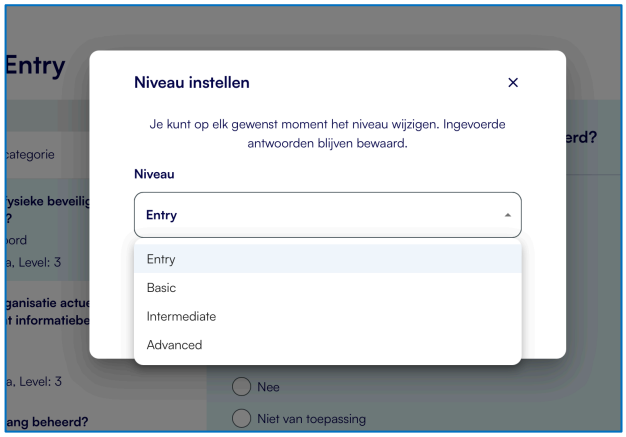
Het gebruik om stap voor stap beter te worden zie je bedrijven groeien op de controls door de Levels 1, level 2 en 3. Elke stap geeft waarde en feedback voor de organisatie, als informatie waar ze staan. Als doelstelling certificeerbaarheid, is naar alle waarschijnlijkheid alleen level 3 relevant. Zelf adviseer ik in dit geval in ieder geval level 1 en 2 niet, immers geeft “ad hoc” of “best effort” niet voldoende comfort aan externen. Alleen “Defined” geeft mij het comfort wat ik verwacht als ik een certificaat op vraag bij een van mijn partners.

2.6.4 Starten van een zelf-assessment via de tool

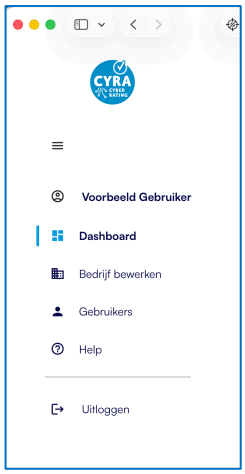
Na het aanmaken van een account kun je een zelf-assessment starten voor CYRA-IT.



Rechtsboven kun je de taal instellen op Engels of Nederlands. Ook kun je rechts het niveau instellen.

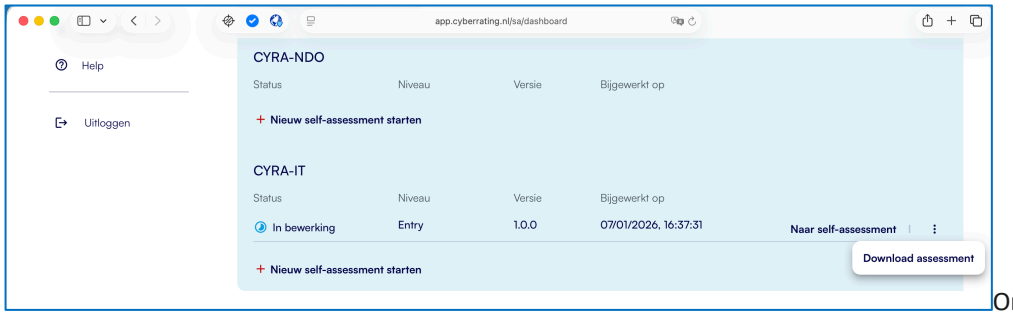


Aan de linkerkant van het menu kun je de gebruikers- en bedrijfsinformatie beheren, het menu wordt beschikbaar als je op de drie streepjes klikt die onder het CYRA logo staan.



Het menu voor de gebruiker “Voorbeeld Gebruiker”. Onder “Dashboard” heb je toegang tot de self-assesments en de abonnementen. Bij “Bedrijf bewerken” staan de bedrijfsgegevens, onder “Gebruikers” kunnen de bedrijfsgebruikers toegevoegd of verwijderd worden en kunnen rollen van gebruikers worden aangepast. Deze optie is alleen beschikbaar voor administrators.

Via “Help” kan er een vraag aan het CCV worden gesteld.



Onder het dashboard kun je naar het self-assessment gaan. Ook kun je het assessment downloaden door op de drie puntjes rechts van het assessment te klikken.

2.7 Blijvend gebruik

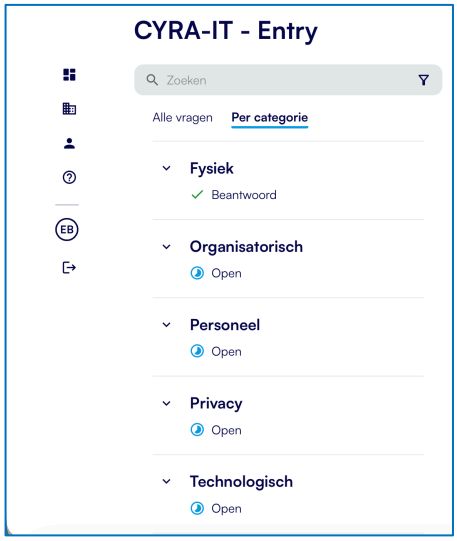
De tool is niet bedoeld voor een eenmalige invuloefening, maar is geschikt voor continue ondersteuning en verbetering van de bedrijfsprocessen. Daarvoor is het nodig dat een organisatie deze ook actief blijft gebruiken. Dit kun je stimuleren door na het aanmaken van de tool een reminder te sturen. Spreek je de ondernemer later opnieuw, bijvoorbeeld tijdens een fysieke afspraak, vraag dan expliciet of hij of zij verder is gekomen en wat dat heeft opgeleverd. Zo help je het gebruik van de tool onderdeel te maken van het normale werkproces, in plaats van een eenmalige actie.

3 De controls

De controls zijn gelieerd aan ISO27001 en ISO27701. Het CCV zorgt er voor dat CYRA 'bijblijft' bij de ISO-ontwikkelingen. Een deskundigenpanel zorgt bij updates van de norm voor een aanpassing in CYRA.

Voor de weergave van de controls, sorteren we de vragen per categorie in de tool.

Selecteer “Per categorie” in de tool.

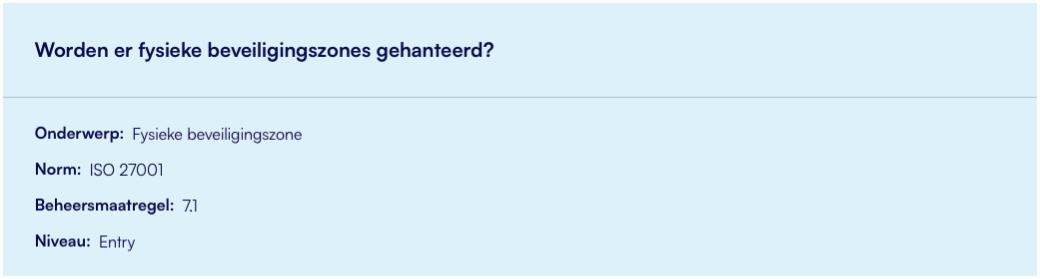


Er zijn 5 categorieën met vragen. In het overzicht kun je zien welke categorie al beantwoord is en welke niet. Als je de categorie uitklapt, kun je zien op welk level elke control is beantwoord, zoals in de volgende paragraaf te zien is

3.1 Fysiek

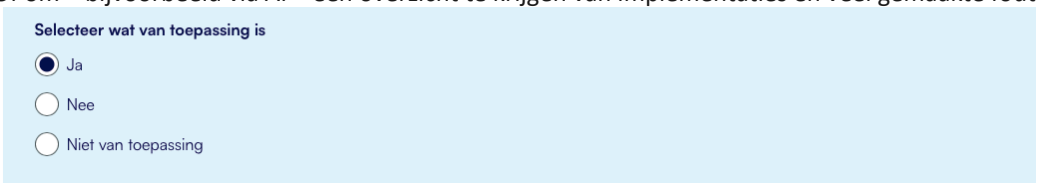
De categorie Fysiek heeft 1 control.

3.1.1 Uitleg control adhv 7.1: fysieke beveiligingszones



Per control wordt aangegeven welke relatie het heeft met een norm en een beheersmaatregel (hier: ISO 27001 en beheersmaatregel 7.1) en in welke CYRA-niveau (hier: entry) het zit.

De beheersmaatregel kan gebruikt worden om best practices of details online over op te zoeken via het internet. Of om – bijvoorbeeld via AI – een overzicht te krijgen van implementaties en veel gemaakte fouten.

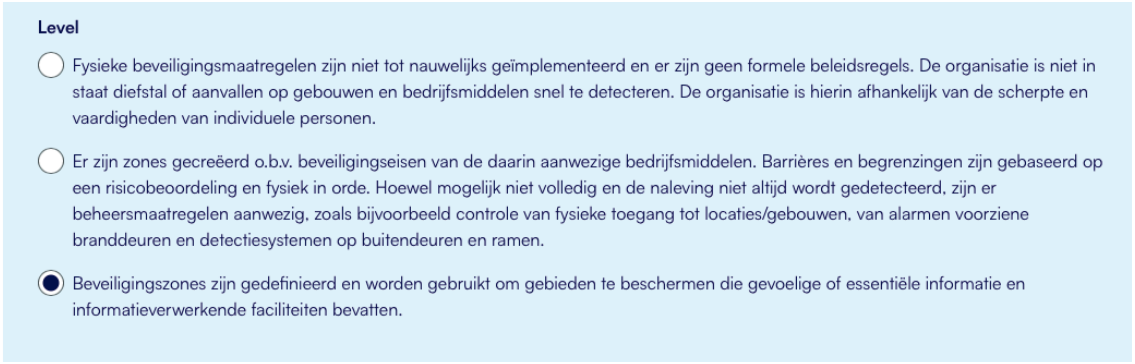


Per control kan worden weergegeven of het:

- Niet van toepassing is →
  hier wordt een verklaring van niet-toepasbaarheid (Statement of Applicability, SoA) gevraagd.

- Nee →
  De organisatie hier niet aan voldoet.

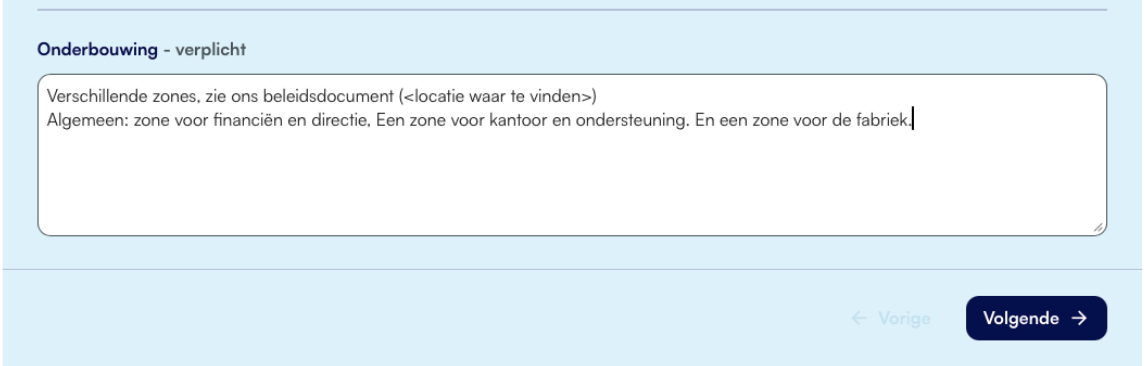
- Ja →
  De organisatie hier aan voldoet. Pas als "Ja" is geselecteerd kan een level worden gekozen.



Wil je aan CYRA entry level 3 voldoen, moet je op alle controls van CYRA entry, op level 3 voldoen – of aangeven op welke controls dit 'niet van toepassing' is.

Het bovenste genoemde antwoord is level 1 (ad hoc), het middelste genoemde antwoord is level 2 (best effort) en de onderste is level 3 (defined).

Noem in de verplichte onderbouwing altijd hoe dit aangetoond kan worden. Dit vereenvoudigt de audit.



Voor de fysieke beveiliging is het nodig dat de beveiligingszones gedefinieerd zijn die overeenkomen met de gebieden om deze te beveiligen.

Denk ook aan het volgende: staan er monitoren in de fabriekshal die de voortgang laten zien? Hebben deze een verbinding met het netwerk op kantoor? Of zijn deze netwerken gescheiden?

Vaak heb je als bedrijf al zones op het gebied van brandbeveiliging. In de praktijk is dat vaker anders ingedeeld als ICT. Kijk hoe de mensenstroom is. Publieke zones mag iedereen komen, dan heb je de kantooromgeving en de fabrieksomgeving. Je begint waar iedereen mag komen en gaat dan naar heel specifiek. Let ook op de bijzondere ruimtes, zoals een archiefruimte.

3.2 Organisatorisch

De organisatorische categorie bevat 7 controls.

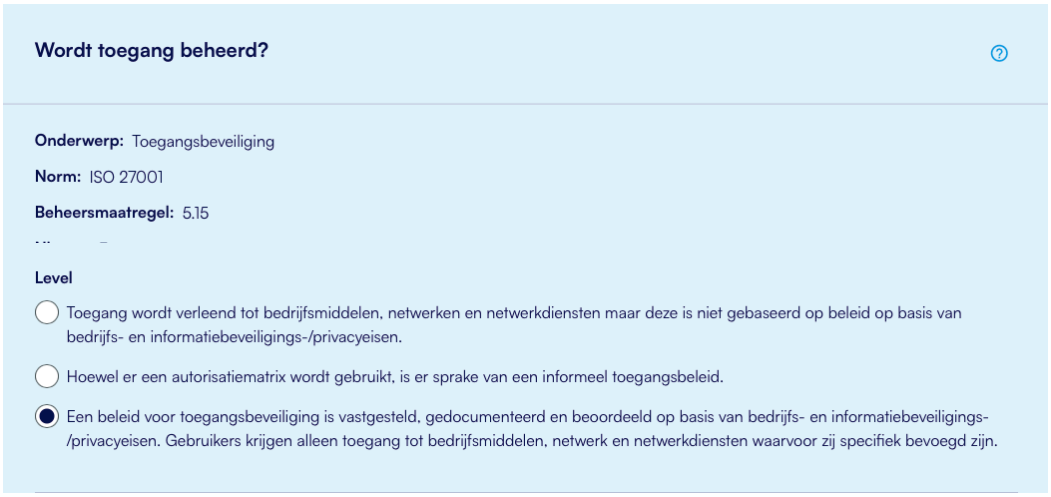
De lay-out van de tool is voor deze controls hetzelfde als getoond in de paragraaf over fysieke beveiliging. Hieronder staan de beschrijving van de volwassenheidslevels (level 1: ad hoc, level 2: best effort, level 3: defined) beschreven, zoals ze genoemd zijn in het openbare overzicht van de CYRA controls, te vinden op:

https://hetccv.nl/app/uploads/2025/12/CYRA250807_Tabel-Levels_ENG.pdf

Deze maatregel geeft aan dat het beleid zelf onder toezicht en controle staat van de directie en dat deze ook daadwerkelijk beschikbaar wordt gemaakt aan degenen die er mee te maken krijgen. Dit is meestal een paragraaf in het beleidsdocument zelf waarbij duidelijk aangeeft wie welke actie neemt en met welke frequentie.

Wees telkens met het noemen van wat je moet doen heel specifiek, bijvoorbeeld: bij wie met je incidenten melden. Noem alle rollen, IT-beheerder, externe partner, medewerkers. Voor de personen die je traint: laat je ook hun eigen rol (bv “ISO” of “Kwaliteit”) meenemen.

Zorg ervoor dat het beleid goedgekeurd is door de directie en wees ook in staat dat te laten zien.



Wordt er gewerkt met gebruikersaccounts?

Onderwerp: Registratie en uitschrijving van gebruikers

Norm: ISO 27001

Beheersmaatregel: 5.16

Level

- ○ 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.

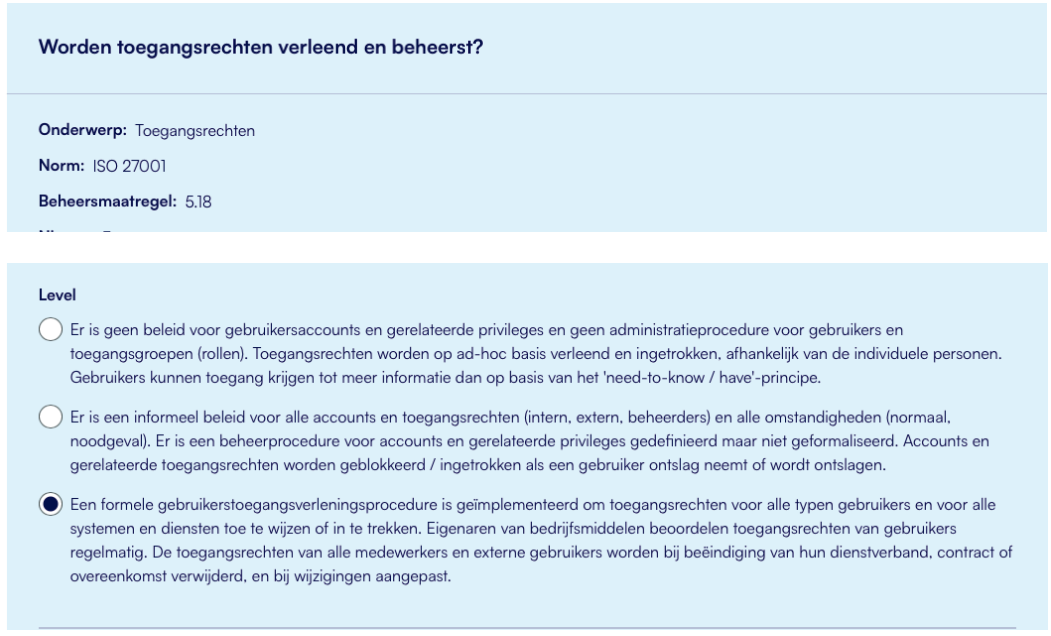
  Alle hierboven genoemde zaken zijn vastgelegd in procedures en aantoonbaar toegepast.

“Hoe zorg je dat alleen de juiste mensen, op het juiste moment, met de juiste identiteit toegang krijgen – en die toegang ook weer verliezen?”.

Maak één vast proces voor aanmelden en afmelden, het liefst niet afhankelijk van een persoon in de organisatie. Best practice: HR of management triggert, IT voert uit.

- Start dienstverband → trigger voor account-aanmaak
- Einde dienstverband → trigger voor directe account-blokkade
- Functiewijziging → herbeoordeling van rechten

Gedeelde accounts ondermijnen deze control volledig, maak daarvoor een unieke identiteit voor iedere gebruiker. En als uitzonderingen nodig zijn (bijvoorbeeld service accounts), benoem dit expliciet voor een specifiek doel en beoordeel deze periodiek.



Worden toegangsrechten verleend en beheerst?

Onderwerp: Toegangsrechten

Norm: ISO 27001

Beheersmaatregel: 5.18

Level

- ○ 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.

Leg per functie vast welke toegangsrechten nodig zijn en ken deze rechten alleen toe na expliciete goedkeuring van management of proceseigenaar. Zorg dat toegangsrechten direct worden aangepast of ingetrokken bij

functiewijziging of uitdiensttreding. Voer periodiek (bijv. maandelijks of jaarlijks) een controle uit op alle toegangsrechten en leg vast dat deze controle is uitgevoerd.

Heeft de organisatie verantwoordelijkheden m.b.t. informatiebeveiliging en privacy vastgesteld?

Onderwerp: Rollen en verantwoordelijkheden bij informatiebeveiliging en privacy

Norm: ISO 27001

Beheersmaatregel: 5.2

Level

- ◯ 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.

Leg duidelijk vast wie waarvoor verantwoordelijk is op het gebied van informatiebeveiliging, inclusief beslissingsbevoegdheid en escalatie. Zorg dat deze verantwoordelijkheden bekend zijn bij betrokken medewerkers en aansluiten bij hun rol in de organisatie. Herzie de rolverdeling periodiek en bij organisatorische veranderingen, zodat verantwoordelijkheden actueel en uitvoerbaar blijven.

Wordt de dienstverlening van leveranciers gemanaged?

Onderwerp: Monitoring van, beoordeling van en beheer van veranderingen in de dienstverlening van leveranciers

Norm: ISO 27001

Beheersmaatregel: 5.22

Level

- ◯ 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.

Op level 3 betekent leveranciersmanagement niet automatisch dat je zelf leveranciers moet auditen. In veel gevallen is het voldoende om een certificaat of auditrapport van de leverancier op te vragen. Let daarbij goed op de scope van dat certificaat: niet alle leveranciers laten al hun diensten certificeren. Je moet kunnen aantonen dat juist de dienst die jij afneemt binnen de gecertificeerde scope valt.

Leveranciers hoeven ook niet zelf aan tafel te zitten bij deze gesprekken. Wat je wél moet kunnen aantonen, is dat je – op basis van je risicoanalyse – bewust bepaalt welke leveranciers kritisch zijn en hoe je die controleert. Als je ervoor kiest om bepaalde leveranciers niet actief te toetsen, moet dat een bewuste managementkeuze zijn, inclusief inzicht in de mogelijke gevolgen.

Een pragmatische aanpak is om eerst vast te leggen wat je nu al doet aan leveranciersbeheer. Pas daarna kijk je of het risicoprofiel van specifieke leveranciers aanleiding geeft om extra maatregelen te nemen. Zo bouw je voort op bestaande praktijk in plaats van een theoretisch ideaalbeeld.

Is de organisatie voorbereid op het beheer van beschikbaarheid, integriteit en vertrouwelijkheid van informatie tijdens calamiteiten?

Onderwerp: Informatiebeveiliging in ongunstige situaties

Norm: ISO 27001

Beheersmaatregel: 5.29

Level

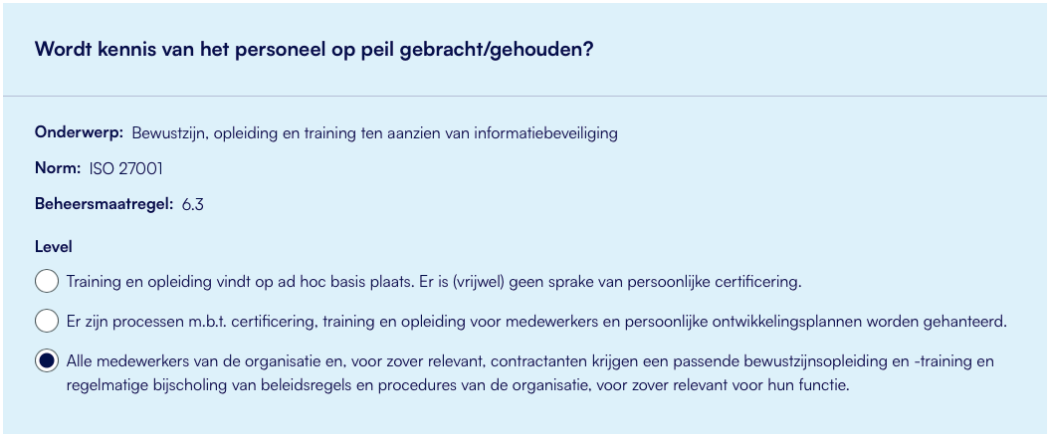
- ○ Enkele ongunstige situaties (crisis/rampen) zijn in beeld maar niet geformaliseerd in processen, procedures of beheersmaatregelen. De organisatie acteert in die gevallen reactief en leunt op specifieke personen.
- ○ Eisen voor informatiebeveiliging zijn vastgesteld en vertaald naar processen, procedures 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.

Kun je de vertrouwelijkheid van de informatie bij calamiteiten (cyberincidenten) garanderen? Ook als je gebruikmaakt van externe leveranciers?

3.3 Personeel

De categorie personeel bevat 4 controls.

Leg uit hoe je medewerkers screent, per rol bij indiensttreding. Als dat nodig is, natuurlijk, wat met name voor MKB niet voor elke rol het geval zal zijn. Vraag je VOG op?



Wordt kennis van het personeel op peil gebracht/gehouden?

Onderwerp: Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

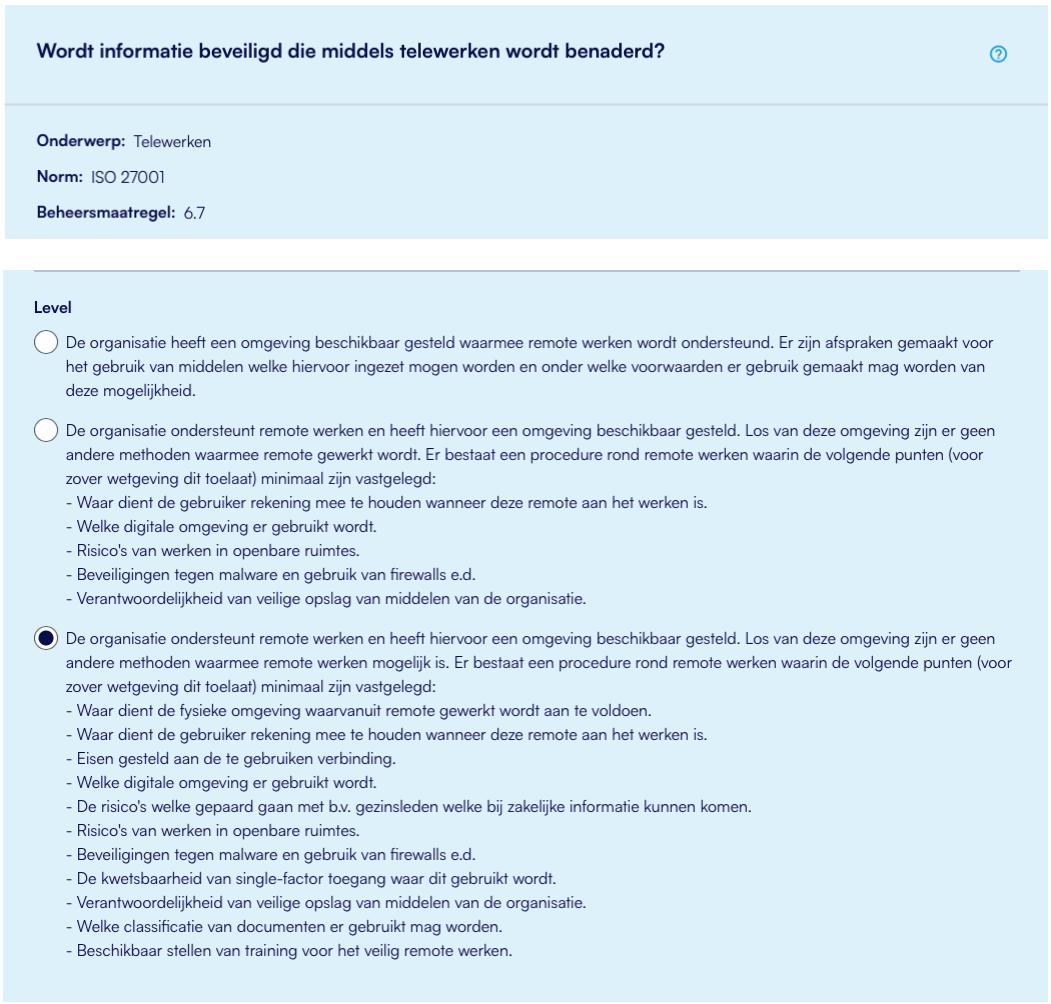
Norm: ISO 27001

Beheersmaatregel: 6.3

Level

- ○ 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.
- ● Alle medewerkers van de organisatie en, voor zover relevant, contractanten krijgen een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Hou je bij wie training heeft gevolgd?



Wordt informatie beveiligd die middels telewerken wordt benaderd?

Onderwerp: Telewerken

Norm: ISO 27001

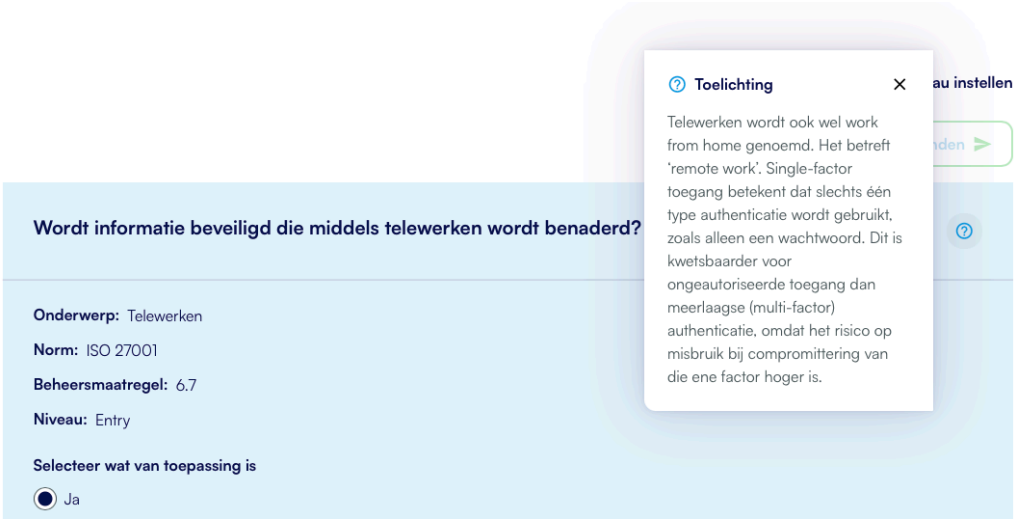
Beheersmaatregel: 6.7

Level

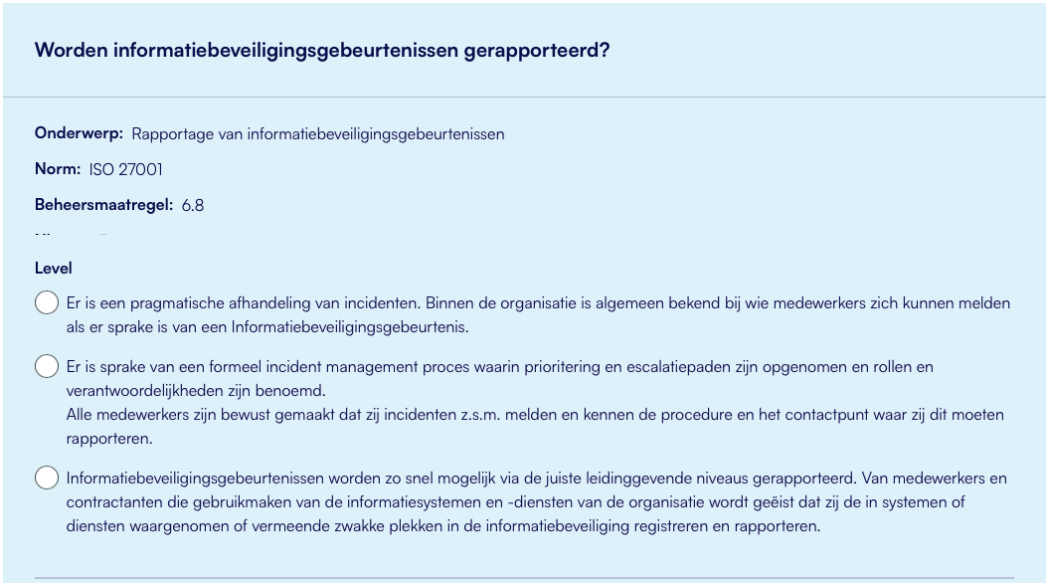
- ○ De organisatie heeft een omgeving beschikbaar gesteld waarmee remote werken wordt ondersteund. Er zijn afspraken gemaakt voor het gebruik van middelen welke hiervoor ingezet mogen worden en onder welke voorwaarden er gebruik gemaakt mag worden van deze mogelijkheid.
- ○ De organisatie ondersteunt 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.

Staat hier iets over in bijvoorbeeld het personeelshandboek? Bijvoorbeeld dat bij thuiswerken er een headset gedragen moet worden en/of videoconferentie dat je alleen in een ruimte moet zitten.

3.3.1 Helpfunctie, voorbeeld bij 6.7: toegang op afstand



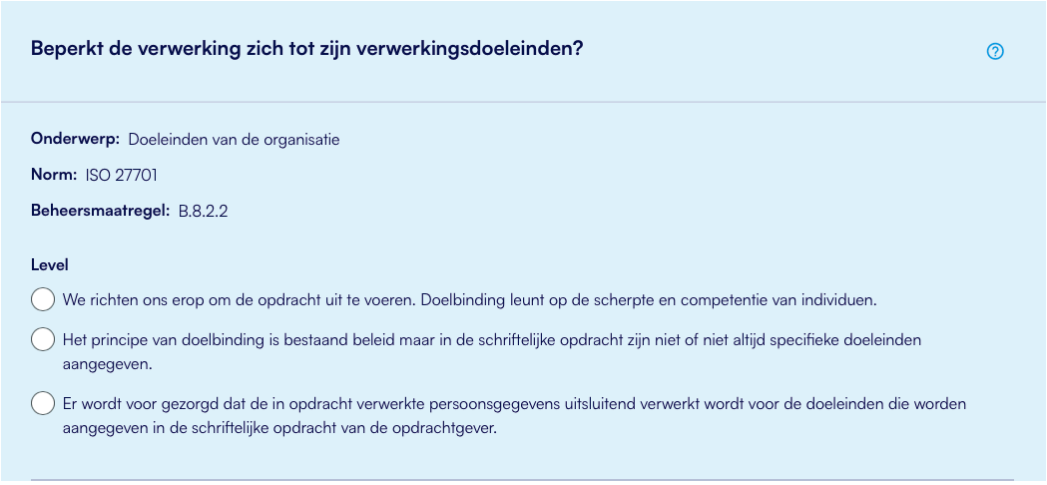
Er zijn controls waar hulp bij geboden wordt, zoals bij de wat gedateerde term “telewerken”. Deze term is opgenomen in CYRA omdat het overeeenkomt met de woordkeus in ISO27001, maar behoeft wel wat uitleg. Als je op het ? klikt, krijg je een toelichting – indien beschikbaar.



Heb je een crisisteam: wie zit daarin en wat zijn de procedures? Hebben die personen; externe leverancier, directie, toegang tot de gegevens en blijft dan ook de vertrouwelijkheid gegarandeerd?
Matrix om incidenten vast te leggen kan al heel simpel in een .xls overzicht: Incident, actiehouder en vervolgstap. B.v. vullen met een verkeerd verzonden mailtje.

3.4 Privacy

De categorie privacy bevat 2 controls, hieronder weergegeven.
Deze controls komen uit ISO 27701, gelieerd aan de AVG (privacy wetgeving).

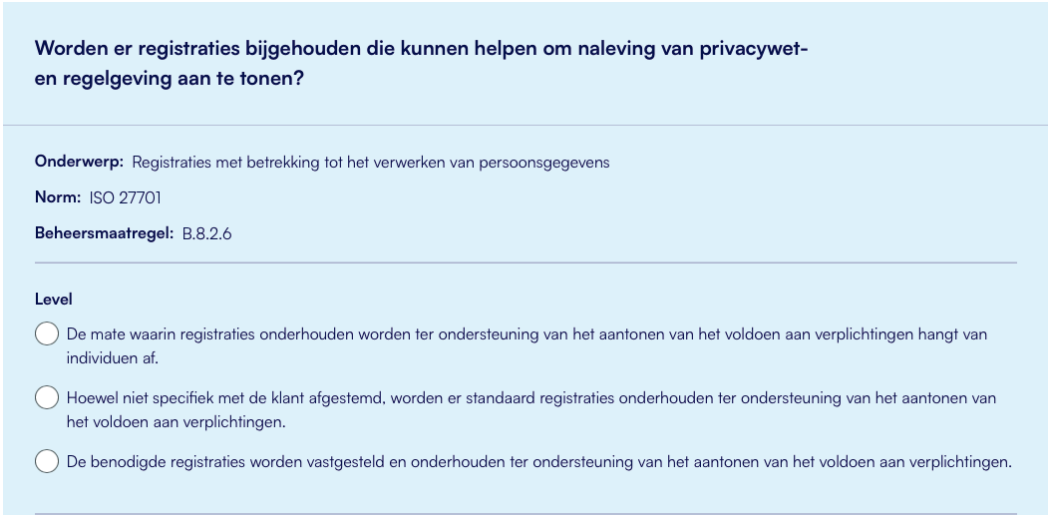


Geef per contract aan waar specifieke informatie wel of niet voor gebruikt mogen worden.

We hebben het hier ook specifiek over persoonsgegevens. Is dat in het contract opgenomen met de medewerkers? Zijn er verwerkersovereenkomsten?

Denk ook aan het volgende: Bij een externe organisatie die personeelsgegevens en administratie verwerkt, spreek ook af dat alle gegevens na 7 jaar daar uit het systeem verwijderd worden.

Ook een tip - van een van de trainers - let op de cookies en de website. Soms worden de cookies al geplaatst voordat toestemming wordt gegeven (en dat mag niet volgens AVG).



Worden er registraties bijgehouden die kunnen helpen om naleving van privacywet- en regelgeving aan te tonen?

Onderwerp: Registraties met betrekking tot het verwerken van persoonsgegevens

Norm: ISO 27701

Beheersmaatregel: B.8.2.6

Level

- ◯ 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.

Waar staan de verwerkersovereenkomsten opgeslagen? En hoe zorg je ervoor dat deze blijft voldoen aan verplichtingen?

3.5 Technologisch

De categorie technologisch bevat 10 controls, hieronder weergegeven.

Technologisch

Open

8.15 **Wordt er gebruik gemaakt van logbestanden?**
Open
Antwoord: Ja

8.20 **Wordt informatie op het netwerk beheerd?**
Open
Antwoord: Ja

8.21 **Wordt de veiligheid van netwerkdiensten vastgesteld?**
✓ Beantwoord
Antwoord: Ja, Level: 3

8.24 **Wordt versleuteling (cryptografie) toegepast?**
Open
Antwoord:

8.25 **Wordt er security by design toegepast bij softwareontwikkeling?**
Open
Antwoord:

8.26 **Speelt informatiebeveiliging een rol in de aanschaf/ontwikkeling van (nieuwe) applicaties?**
Open
Antwoord:

8.32 **Worden veranderingen in informatieverwerkende faciliteiten en systemen beheerst uitgevoerd?**
Open
Antwoord:

8.5 **Wordt gecontroleerd of gebruikers die toegang hebben tot informatiesystemen zijn wie ze claimen te zijn?**
Open
Antwoord:

8.7 **Wordt de organisatie beschermd tegen malware?**
Open
Antwoord:

8.8 **Worden technische kwetsbaarheden voorkomen?**
Open
Antwoord:

Wordt er gebruik gemaakt van logbestanden?

Onderwerp: Genereren, bewaren en beoordelen van logbestanden

Norm: ISO 27001

Beheersmaatregel: 8.15

Level

- ○ Er vindt geen actief gebruik van logbestanden plaats. Wanneer logs worden gegenereerd, gebeurt 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 worden gewist of niet-identificeerbaar gemaakt, zoals gespecificeerd is in het bewaarschema.

Wie heeft toegang tot de logbestanden? Hoe worden deze behandeld / doorgenomen?
Als via ERP systemen privacy gegevens ingezien wordt, wordt dat gelogd?

Wordt informatie op het netwerk beheerd?

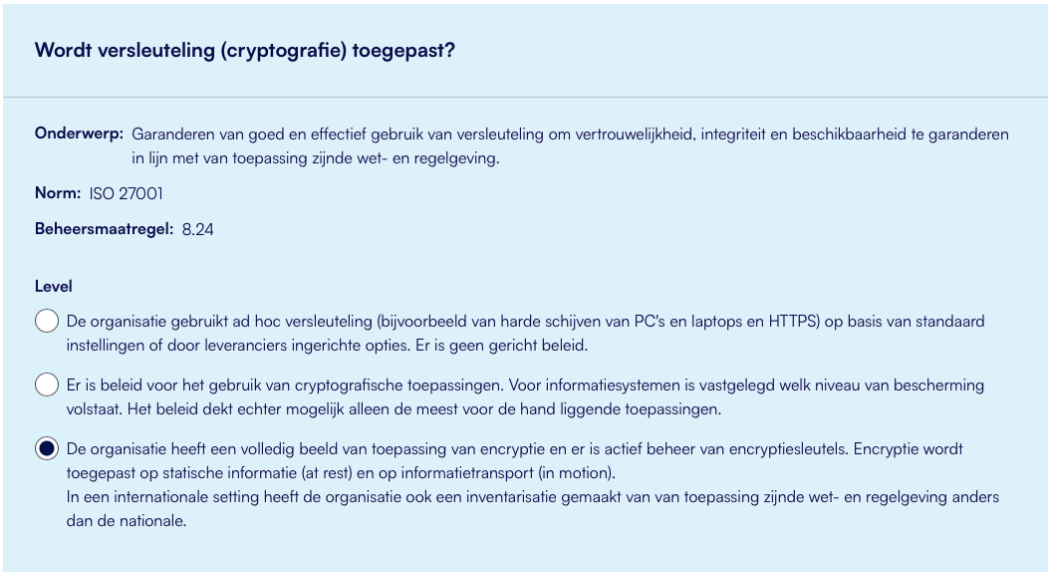
Onderwerp: Beschermen van informatie in netwerken en ondersteunende systemen

Norm: ISO 27001

Beheersmaatregel: 8.20

Level

- ○ 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 tot 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, geüpdated, gelogd en gemonitord. Systemen worden zodanig ingericht dat ze zo onkwetsbaar mogelijk zijn (hardening). Er vindt mogelijk actieve controle op ongeoorloofde toegang plaats (Intrusion Detection).



Een praktische MKB-aanpak is om standaard versleuteling te gebruiken die al in bestaande systemen zit, zoals schijfversleuteling op laptops, TLS voor e-mail en HTTPS voor webapplicaties.
Leg vast wanneer en waarvoor versleuteling verplicht is (bijv. laptops, back-ups, cloudopslag met klantdata) en kies daarbij gangbare, bewezen algoritmes via leveranciersinstellingen, niet via maatwerk.

Zorg dat sleutelbeheer niet persoonsafhankelijk is (bijv. centraal beheer of herstelprocedure) en accepteer bewust dat je géén eigen cryptografie ontwerpt.

Wordt er security by design toegepast bij softwareontwikkeling?

Onderwerp: Beleid voor beveiligd ontwikkelen

Norm: ISO 27001

Beheersmaatregel: 8.25

Level

- ◯ 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.

Deze is alleen relevant bij het ontwikkelen van eigen software en systemen. Voor bedrijven die geen ontwikkeling zelf doen, zal dit “niet van toepassing” zijn.

Speelt informatiebeveiliging een rol in de aanschaf/ontwikkeling van (nieuwe) applicaties?

Onderwerp: Informatiebeveiligingseisen in ontwerp en aanschaf van applicaties

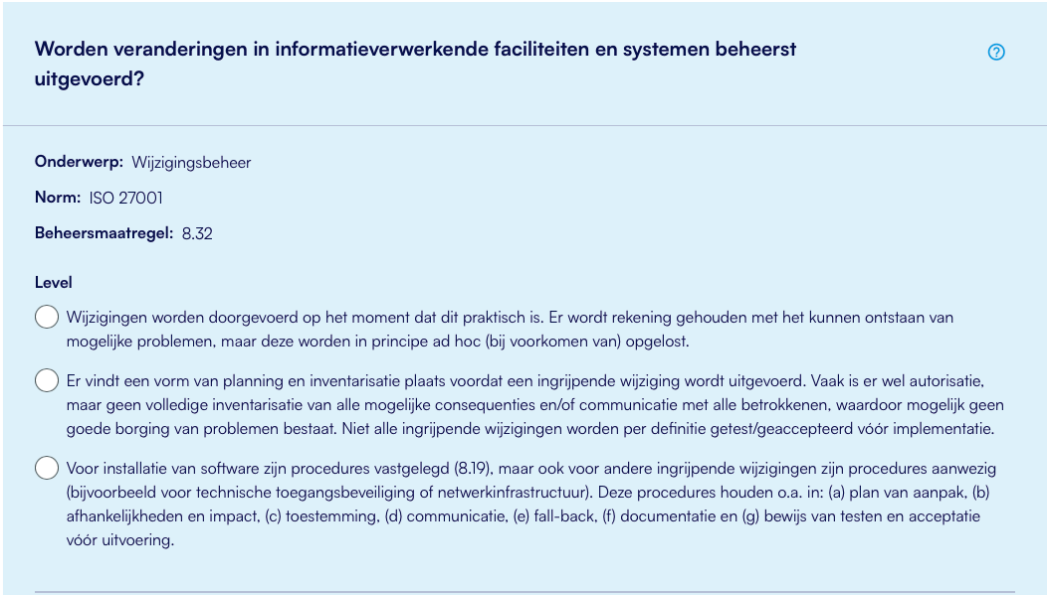
Norm: ISO 27001

Beheersmaatregel: 8.26

Level

- ◯ 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 wettelijke 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

Worden veiligheidseisen meegenomen bij de aanschaf van nieuwe applicaties of machines? En bij updates?



Worden veranderingen in informatieverwerkende faciliteiten en systemen beheerst uitgevoerd?

Onderwerp: Wijzigingsbeheer

Norm: ISO 27001

Beheersmaatregel: 8.32

Level

- ◯ 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 communicatie 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.

Een werkbare best practice voor het MKB is om alle wijzigingen aan systemen of applicaties vooraf vast te leggen, inclusief wat er verandert, waarom, en wat het risico is voor informatiebeveiliging. Laat een tweede persoon of het management akkoord geven bij wijzigingen met impact (bijv. updates, nieuwe software, rechtenwijzigingen), zodat beslissingen niet individueel en impliciet worden genomen. Evalueer na de wijziging kort of deze correct is uitgevoerd en geen nieuwe risico's heeft geïntroduceerd, en leg ook die check vast.

Wordt gecontroleerd of gebruikers die toegang hebben tot informatiesystemen zijn wie ze claimen te zijn?

Onderwerp: Beveiligde inlogprocedures

Norm: ISO 27001

Beheersmaatregel: 8.5

Niveau: Entry

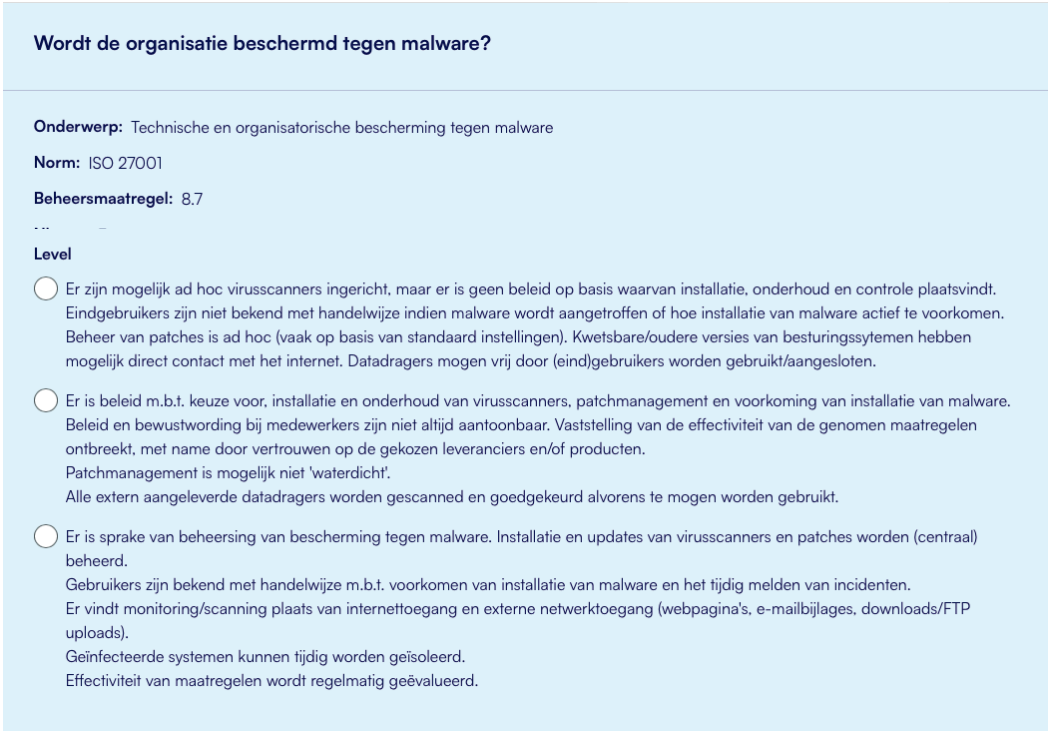
Selecteer wat van toepassing is

- ◉ Ja
- ◯ Nee
- ◯ Niet van toepassing

Level

- ◯ 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 door 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 daarvan wordt autorisatie verleend. Er is monitoring aanwezig om (on)succesvolle loginpogingen te signaleren en/of te blokkeren (o.a. brute force pogingen). Het kunnen onderscheppen van logons (sniffers, camera's, keyloggers) wordt vermeden. Inactieve sessies worden afgesloten.

Een praktische MKB-best practice is om voor alle systemen met gevoelige informatie sterke authenticatie te gebruiken. Leg vast welke authenticatiemethode per systeem verplicht is (bijv. wachtwoord + MFA voor cloud en beheeraccounts) en voorkom gedeelde accounts.
Controleer periodiek of deze instellingen nog actief zijn en pas ze direct aan bij uitdiensttreding of rolwijziging.



Wordt de organisatie beschermd tegen malware?

Onderwerp: Technische en organisatorische bescherming tegen malware

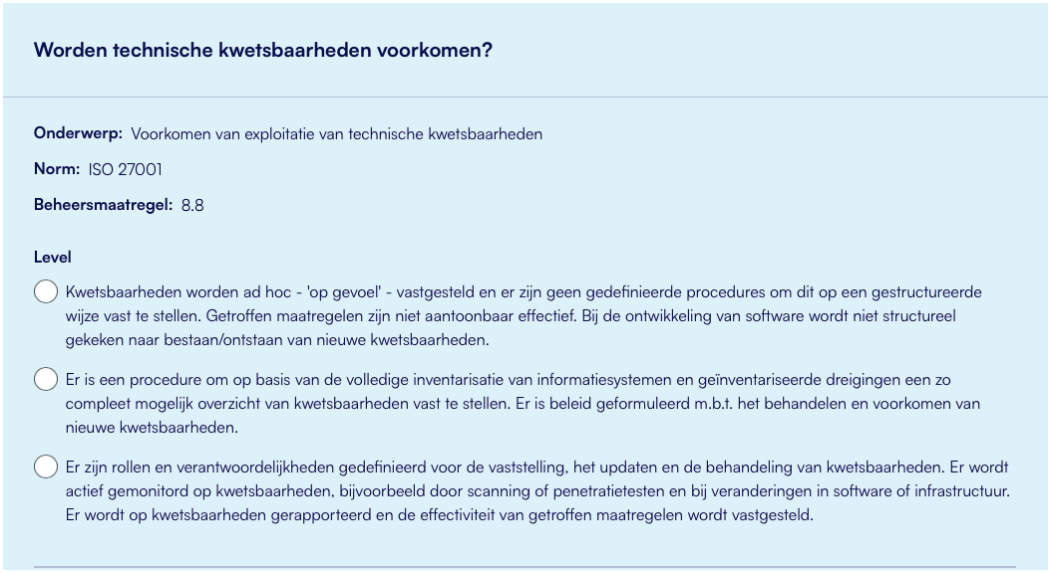
Norm: ISO 27001

Beheersmaatregel: 8.7

Level

- ◯ 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 met 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.

Tegen malware beschermen is niet een incidenteel iets. Doe dit structureel en leg je beleid vast op een dusdanige manier dat je de mensen kunt aanwijzen die er verantwoordelijk voor zijn.



Worden technische kwetsbaarheden voorkomen?

Onderwerp: Voorkomen van exploitatie van technische kwetsbaarheden

Norm: ISO 27001

Beheersmaatregel: 8.8

Level

- ◯ 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.

Technische kwetsbaarheden voorkomen vereist een patch- en updatebeleid. Een patch- beleid moet passen bij je eigen bedrijf. Dit ligt vaak wel in de aansturing van je IT afdeling (intern of extern). Een updatebeleid is bijvoorbeeld dat je ICT-er elke update installeert op het moment dat deze uitkomt, binnen 2 werkdagen. Doe dit structureel en leg je beleid vast op een dusdanige manier dat je de mensen kunt aanwijzen die er verantwoordelijk voor zijn.

4 FAQs

Hieronder staan een aantal FAQ's (Frequently Asked Questions), veelgevraagde vragen en hun antwoorden.

4.1 Wanneer voldoe je aan een control?

Je voldoet aan een control als je een maatregel hebt geïmplementeerd, deze hebt vastgelegd én werkt zoals je het hebt vastgelegd. De gekozen maatregelen moeten daarbij proportioneel zijn: passend bij de risico's en de afhankelijkheid van de organisatie.

Zo kan een klein bedrijf dat beperkt afhankelijk is van IT prima kiezen voor maandelijkse software-patching. Maandelijks is immers ook een vaste en aantoonbare frequentie.
Voor een organisatie die sterk afhankelijk is van IT ligt dat anders. Daar is het logisch om wekelijks te controleren of er patches beschikbaar zijn en kritieke patches direct te installeren zodra de leverancier aangeeft dat dit noodzakelijk is.

Een auditor kijkt hierbij vooral naar twee dingen:

- Proportionaliteit – past de maatregel bij het risicoprofiel?
- Borging – is de uitvoering vastgelegd en niet afhankelijk van één persoon?

De ondernemer bepaalt uiteindelijk de prioriteiten en de acceptabele risico's, maar moet zich er bewust van zijn dat die keuzes ook gevolgen hebben voor het risico dat de organisatie accepteert.
Uiteindelijk bepaalt de ondernemer zelf wel risico acceptabel is. Niet de auditor. En ook – als het goed is ingeregeld – niet de uitvoerende ICT partij, of deze nu intern of extern is. De auditor controleert wel of het risico past bij je organisatie en je risicoanalyse.

4.2 Waar let een auditor op?

Om aan een norm te voldoen moet je in ieder geval de procedure opschrijven en een eigenaar toekennen. Iemand die je echt aan kunt wijzen.

Een auditor let er op of je voldoet aan de vraag. Lees de vraag daarom heel goed. Gehoorde vragen tijdens een audit:

- Welk beleid is er? Welke procedures zijn er?
- Waar is dat vastgelegd? (bijvoorbeeld in een informatiebeveiligingsbeleiddocument?)
- Kun je me dat laten zien? Kan iemand anders me dat laten zien?

Of

- Hoe doe je dat?
- Heb je hier iets van op papier staan?

4.3 Hoe zit het met de verklaring van niet-toepasbaarheid?

Er bestaat een 'verklaring van niet-toepasbaarheid', waarmee je voor een control aangeeft dat deze "nvt" oftewel "niet van toepassing" is. Deze verklaring kun je in de onderbouwing weergeven op het moment dat je "Niet van Toepassing" als antwoord op een control geeft.

Hierin staat waarom een control nvt is verklaard en waarop dit besluit is gebaseerd, bijvoorbeeld gerelateerd aan de context of de risicoanalyse.

Voorbeelden waaruit een contextbeschrijving blijkt dat een control 'nvt' is:
Geen productieomgeving → geen industriële besturingssystemen
Geen thuiswerk → geen remote access controls
Geen eigen servers → geen fysieke serverruimte

Voorbeelden waaruit de risicoanalyse blijkt dat een control 'nvt' is:
Geen draagbare media → risico "verlies USB-sticks" bestaat niet
Geen klantdata → privacy-gerelateerde controls niet relevant

Bestuurlijke beslissing
Een "nvt" beantwoording is geen technische keuze, maar een managementbesluit.

Enkele gemaakte fouten (en waarom auditors ze afkeuren)
- "De IT'er vond het niet nodig"
  -> Een "nvt" beantwoording is geen technische keuze, maar een managementbesluit.
- "Niet van toepassing want te duur"
  → Kosten zijn geen geldige reden
- "Niet relevant voor MKB"
  → Organisatiegrootte is geen argument
- "Nog niet geïmplementeerd"
  → Dat is non-compliance ("nee"-beantwoording), geen "nvt"

4.4 Is certificering noodzakelijk?

"We zijn compliant, maar niet gecertificeerd"
Dat betekent: je volgt (delen van) de norm, maar hebt geen extern bewijs.
Dat is prima, zolang er geen extern bewijs nodig is. Je gebruikt CYRA dan vooral om zelf inzicht te krijgen.

Mocht je – in de toekomst – wel extern bewijs nodig hebben, kun je altijd nog op dat moment een certificaat aanvragen. Let daarbij wel op het framework die je gebruikt: extern bewijs moet wel onafhankelijk worden gegeven en niet door dezelfde organisatie als die het framework exploiteert. Gebruik daarom CWB (NIS-2), CYRA, ISO27001 of NIST-CSF.

4.4.1 De tool tijdens certificering

De tool wordt niet alleen gebruikt voor het bedrijf zelf, ook voor de certificerende instantie. Bij een audit-aanvraag wordt de input 'bevroren'. Het bedrijf moet dus de input vervolmaken voordat ze een audit aanvragen. De bevroren input wordt door de certificerende instantie – door de auditor – gebruikt om controles uit te voeren. De auditor controleert alleen of je aantoonbaar de antwoorden hebt gegeven. Bv je hebt level 3 aangegeven bij een control met een onderbouwing, dan controleert de auditor de onderbouwing en geeft aan of je compliant bent of niet. Eventueel een suggestie voor vervolg of een opmerking indien die niet afbreuk doet aan bovenstaande.

Als je niet compliant bent, krijg je geen certificaat. De auditor zal niet zeggen "je hebt level 3 ingevuld dat is niet juist, maar voor level 2 krijg je wel een certificaat".

4.5 Hoe lang is een certificaat geldig?

Een CYRA-certificaat is 2 jaar geldig

4.6 Hoe zorgen we ervoor dat we medewerkers ook daadwerkelijk mee krijgen?

Er bestaan verschillende beproefde methoden om medewerkers mee te krijgen in informatiebeveiliging. Het uitvoeren van een penetratietest of phishing-simulatie en medewerkers daar vooraf over informeren of actief bij betrekken, zorgt in de praktijk vaak voor meer begrip en bewustzijn van de noodzakelijke maatregelen.

Door risico's concreet en ervaarbaar te maken, verschuift informatiebeveiliging van een abstract IT-onderwerp naar iets wat medewerkers direct herkennen in hun eigen werk. Dat kan ook door het organiseren van een cyberoefening of training voor medewerkers.
Als deze specifiek wordt ingezet, vergroot het de acceptatie en naleving van afspraken aanzienlijk.

Ook helpt het – randvoorwaardelijk wellicht – dat management/directie het goede voorbeeld laat zien.

4.7 Autorisatiematrix

Een autorisatiematrix is een eenvoudig overzicht waarin staat wie wat mag binnen systemen, applicaties en gegevens. Het doel is niet "alles dichttimmeren", maar ongewenste toegang voorkomen en fouten beperken. De kern is het *need-to-know*-principe: medewerkers krijgen alleen rechten die zij nodig hebben voor hun werk.
In MKB-omgevingen gaat dit vaak mis doordat rechten "erbij blijven hangen" bij functiewissels, tijdelijke oplossingen permanent worden, of omdat één persoon (bijvoorbeeld de directeur of IT-beheerder) overal toegang toe heeft zonder noodzaak. Dat vergroot de kans op datalekken, fraude en audit-afkeur. Een goede autorisatiematrix maakt deze risico's zichtbaar en bespreekbaar.

Een autorisatiematrix is een overzicht dat de vertaling maakt van:

Functie - Rollen - Welke permissies daarbij horen in welke pakketten

Een autorisatiematrix is geen statisch papieren exercitie. Als hij niet wordt gebruikt bij indiensttreding, functiewijziging en uitdiensttreding, is hij inhoudelijk waardeloos.
Naast de matrix zelf hoort er ook een proces bij voor aanvragen van extra rechten en uitzonderingen. Bijvoorbeeld een werkplaatsmedewerker die de rol van inkoper er bij krijgt heeft twee rollen. Bij het proces hoort ook een jaarlijkse

controle: klopt het nog?
Ook moet beschreven worden wanneer de rechten weer weg gaan.

Toelichting:

- *Beheerrechten* zijn gescheiden van inhoudelijke toegang. IT kan beheren, maar niet meelezen.
- De directie heeft geen standaard beheerrechten. Dat is een bewuste keuze, niet een automatisme.
- HR- en financiële gegevens zijn afgeschermd, ook voor leidinggevenden.
- Productiemedewerkers hebben geen toegang tot kantoorapplicaties die zij niet nodig hebben.

Voorbeeld autorisatiematrix voor Brasholt Hekwerk B.V.

Rol / Functie	E-mail	ERP (orders)	Financiële administratie	HR-dossiers	Productie-systeem	Beheerrechten
Directie	Lezen/ Schrijven	Lezen	Lezen/ Goedkeuren	Lezen	Geen toegang	Geen
Informatiebeveiligings- coördinator (IBC)	Lezen/ Schrijven	Geen	Geen	Geen	Geen toegang	Lezen/ Goedkeuren
Administratie	Lezen/ Schrijven	Lezen/ Schrijven	Lezen/ Schrijven	Geen	Geen toegang	Geen
HR	Lezen/ Schrijven	Geen	Geen	Lezen/ Schrijven	Geen toegang	Geen
Functionaris gegevensbescherming (FG)	Lezen/ Schrijven	Geen	Geen	Lezen	Geen toegang	Geen
Productiemedewerker	Lezen/ Schrijven	Geen	Geen	Geen	Lezen/ Schrijven	Geen
Teamleider Productie	Lezen/ Schrijven	Lezen	Geen	Geen	Lezen/ Schrijven	Geen
IT-beheer	Beheer-rechten	Beheer-rechten	Beheer-rechten	Beheer-rechten	Beheer-rechten	Volledig

Bij indiensttreding geeft HR aan IT aan wanneer de persoon in dienst komt. De afdelingsmanager geeft aan welke rollen een nieuwe medewerker – en dus welke bijbehorende permissies - hoort te krijgen. Dit wordt goedgekeurd door de directie.
De directie is ook in staat om IT beheer te controleren, net als de informatiebeveiligingscoordinator. Bij uitdiensttreding en/of bij einde contract van externen geeft HR een seintje aan IT, die ervoor zorg draagt dat bij de datum uitdiensttreding de rechten van de desbetreffende persoon worden ingetrokken. Jaarlijks gaat IBC beheer een controle uitvoeren op de systemen en ingestelde rechten.

Als er een – tijdelijke – uitzondering gemaakt moet worden, kan dit aangevraagd worden bij IBC die - na een controle met positief resultaat door de directie – dit ten uitvoer zal laten brengen door IT. Deze uitzonderingen worden hieronder bijgehouden en automatisch teruggetrokken indien niet meer nodig.

Lijst uitzonderingen:

Wie	id	Aanvullende permissies	Einde datum
Stagiair Bennie	bennie@brasholt.nl	HR lezen	31-12-2026
Externe consultant van leverancier tbv ERP	jitse@brasholt.nl	ERP lezen,schrijven & beheerrechten	31-07-2026

Typische MKB-fouten (waar een auditor doorheen prikt)

- “Iedereen heeft alles, want dat is makkelijk.”
- Geen onderscheid tussen lezen, schrijven en goedkeuren.
- De autorisatiematrix bestaat, maar wordt niet bijgewerkt of bijgehouden.
- Externe IT-partijen hebben meer toegang dan nodig en zonder einddatum.

4.8 Wat na het behalen van een certificaat?

En hoe nu verder? Wat gaat het proces zijn nadat we het CYRA certificaat hebben behaald?

Waarschijnlijk is er in het beleid opgeschreven dat de risico’s periodiek worden geanalyseerd, net als de te nemen maatregelen, net zoals na een incident. Dit is verklaard en beschreven onder control 5.1. Dit zorgt ervoor dat het geheel levend blijft.

4.9 Wat als ik vragen over een toepassing krijg, terwijl de controls van CYRA vooral principe-gebaseerd zijn?

Vragen over concrete toepassing zijn geen probleem, maar een leermoment. Hier zit het verschil tussen jou als trainer en jou als consultant, die de problemen van de organisatie oplost.

CYRA-controls zijn principe-gebaseerd om organisaties te dwingen bewust, proportioneel en context-afhankelijk te handelen. Jouw rol is niet om het principe te vervangen door een oplossing, maar om het denkproces te begeleiden dat tot een passende oplossing leidt.

En de vraag*"Maar wat moet ík dan concreet doen in mijn organisatie?"* levert een spanningsveld op. Dat spanningsveld is normaal — en zelfs gewenst. De vraag *"Als het niet exact staat voorgeschreven, doe ik het waarschijnlijk fout." Is onzekerheid, geen norm-eis*.

Als je een framework hebt die wél exacte maatregelen zou voorschrijven dan heeft het de volgende onwenselijke eigenschappen:

- zou het te rigide zijn; voor sommige bedrijven te veel eisen, voor andere te weinig,
- veroudert het snel,
- en verschuift verantwoordelijkheid van de ondernemer naar het raamwerk.

Principe-gebaseerd werken dwingt de organisatie om zelf na te denken over risico's en keuzes. Dat is precies wat level 3 (defined) vraagt.

Hoe ga je hier praktisch mee om als trainer?
Gebruik de vertaalslag in drie stappen / drie vragen waarmee je de trainee helpt:

1. Wat is het principe?
   (bijv. "beveiliging is proportioneel aan het risico")
2. Wat is hier het concrete risico in deze organisatie?
   (bijv. uitval van productie, datalek, afhankelijkheid van leverancier)
3. Welke maatregel is hier proportioneel en uitvoerbaar?
   (bijv. maandelijkse patching, wekelijkse check, externe monitoring)

Niet jij geeft het antwoord, maar je helpt de trainee het antwoord te formuleren.

4.10 Onzekerheid over de vraagstelling: wat als er meerdere onderwerpen in 1 vraag zit?

De combinatie van verschillende onderwerpen in 1 vraag zorgt voor nogal wat discussie. En begrijpelijk als je onzeker bent over hoe dit aan te pakken.
Neem als trainer de vraag er bij. De vragen uit de tool geven soms een voorbeeld en soms een opsomming. Behandel elke zin separaat. Let altijd op de proportionaliteit voor de organisatie, zie ook voorgaande paragraaf.

4.11 Heb je voorbeelden van beleidsdocumenten?

Er zijn voldoende voorbeelden online, bijvoorbeeld bij het NCSC (www.ncsc.nl). Door te zoeken op specifieke controls en norm kun je ook deelinvullingen opzoeken. Het internet staat vol met voorbeelden voor (deel)implementaties.

Let er altijd op dat kopiëren van beleid van anderen het risico heeft dat je of te veel of te weinig of niet de juiste maatregelen neemt. Ga altijd weer uit van je eigen risicoanalyse.

4.12 Wat kost een certificaat?

De kosten voor certificering zijn indicatief als volgt: CYRA Entry circa € 1.000, ISO 27001 circa € 10.000 (via een gecertificeerde instelling).

Voor het behalen van een certificaat neem je contact op met een van de onafhankelijke certificatie-instellingen:

https://hetccv.nl/keurmerken/cybersecurity/cyra/certificatie-instellingen-cyra/

Certificaatniveau	Kosten
Certificaat Entry	€ 100,–
Certificaat Basic	€ 175,–
Certificaat Intermediate	€ 250,–
Certificaat Advanced	€ 300,–
Opslag voor Normenkader Digitale Ondermijning	€ 10,–

4.13 Hoe ga je om met een bestaande situatie waarin documenten niet geclassificeerd zijn?

Hoe kun je documenten labellen zonder dat we alle documenten moeten herzien? Op dit moment is alles voor iedereen toegankelijk.

Suggestie. Schrijf eerst op hoe je het wilt hebben: welke rollen heb je in je organisatie en welke gebruikers horen daarbij? Welke rollen mogen bij welke informatie? Vervolgens kun je gebruik maken van een slim ingerichte drive/fileserver door specifieke folders toegankelijk te maken voor specifieke rollen. Je hoeft hiermee niet alle documenten te herzien, maar wel de locatie waaruit ze gehaald kunnen worden.

Dit kun je verwoorden in de autorisatiematrix.
Vervolgens zet je alle documenten in een ‘archief’ en plaats je alleen de documenten terug in de drive/fileserver die nodig zijn voor de specifieke rollen. Op basis van een “piep”systeem, kun je meerdere terugzetten dan wel – door middel van de uitzonderingenlijst van de autorisatiematrix – tijdelijke permissies toekennen.

4.14 Heb ik met dit – of een ander – certificaat zekerheid?

Zekerheid tegen hacks en digitale ongelukjes:
Een certificaat geeft aan dat je de principes juist hebt geïmplementeerd. Je moet het natuurlijk ook in de praktijk uitvoeren om een zekere mate van veiligheid te hebben. En dan beschermt een certificaat nog altijd niet tegen alle vormen van cybercriminaliteit. Het geeft alleen aan dat je bewust enkele risico’s accepteert en maatregelen hebt genomen tegen andere.

Zekerheid om aan wetten te voldoen:

Op het moment van schrijven is de cyberweerbaarheidswet nog niet aangenomen. Wat we wel weten is dat de overheid risicogebaseerd ondernemingen zal auditen, zoals ook de wet risicogebaseerd ingestoken is.
Het nadeel is dat je daarmee nooit zeker weet dat een bedrijf hetzelfde inschattingsvermogen als een auditor heeft en de zekerheid nooit gegeven kan worden. Maar dat lijkt vooral een theoretische discussie, met een juiste voorbereiding in de lijn 'risicoanalyse', 'aantoonbaar genomen maatregelen', ben je met zekerheid goed voorbereid om het gesprek aan te gaan. Per slot van rekening kent een ondernemer het bedrijf het beste.

Zekerheid tegen aansprakelijkheid van andere organisaties:
Aansprakelijkheden van andere organisaties / bedrijven voor incidenten en geleden schade is steeds meer een onderdeel van contracten. Waarbij de aantoonbaarheid van een oorzaak lastig is, zeker in geval van gevolgen van hybride of digitale oorlogsvoering. Door een juiste formulering en contractueel te verwijzen naar certificaten kan voldoende comfort in de maatregelen worden gegeven die, mist juridisch juist geformuleerd, je kan vrijwaren van aansprakelijkheid.

Bijlage A: Overzicht frameworks

Het CWB (NIS-2) Framework is een framework van de auditdienst van het rijk. Het is bedoeld voor bedrijven die rechtstreeks onder de Cyberbeveiligingswet vallen, danwel als kritische, dan wel als belangrijke entiteit.

In de cyberbeveiligingswet staat een verantwoordelijkheid voor de keten genoemd. Hier worden de bedrijven/partners bedoeld waar een directe relatie mee wordt onderhouden.

Zowel CYRA als de NIS2-QM komen het meest voor op de Nederlandse markt. CYFUN is van Belgische origine. De ISO27001 wordt veel in Europa gebruikt en de NIST-CSF in de verenigde staten.

Framework	Type	Scope	Ondersteuning
CYRA-IT	ISO-MKB	IT-omgevingen, MKB	NCSC-NL
NIS2-QM	ISO-MKB	NIS2-compliance	NL markt
CYFUN	ISO-MKB	Belgisch MKB	-
ISO 27001	Volledig	Alle organisaties	NCSC-NL
NIST CSF	Volledig	Alle organisaties	NCSC-NL
CWB (NIS-2) Framework	Volledig	Kritische/belangrijke entiteiten	Auditdienst Rijk / NCSC-NL

Sector- en scenario-specifieke frameworks:

Framework	Sector
BIO-2	Overheid
CSIR	Rijkswaterstaat
NEN7510	Zorg
CYRA-ZORG	MKB variant voor NEN7510/Zorg
IEC62443	Operational Technology
CYRA-OT	MKB variant voor IEC62443/OT
Digital Criminal Infiltration	Ondermijning
TISAX	Automotive
ABDO/ABRO	(Zakendoen met) Defensie/Rijksoverheid