Samen aanjagen van vernieuwing

Sectoraal transitieprogramma Cbw

Alleen ga je sneller, samen kom je verder

Auteur(s): Ed de Vries

Versie: 1.1 sec
Datum: 21 augustus 2026
Kenmerk:

Inhoudsopgave

1 Inleiding

De digitale weerbaarheid van onderwijs- en onderzoeksinstellingen is een voorwaarde voor de continuïteit van onderwijs, onderzoek en maatschappelijke dienstverlening. De afhankelijkheid van digitale infrastructuur, cloud-voorzieningen, ketenpartners en internationale samenwerking, in combinatie met de hoge waarde en risico's van kennis, onderzoek en data, maakt deze instellingen een aantrekkelijk doelwit voor criminele- en statelijke actoren met aanvallen zoals ransomware, spionage en data exfiltratie of manipulatie.

Met de inwerkingtreding van de Cyberbeveiligingswet (Cbw) worden wettelijke verplichtingen op het gebied van registratie, meldplicht en zorgplicht geïntroduceerd. De Cbw vraagt om structurele borging, risico-gebaseerd werken en continu aantoonbare beheersing en legt nadrukkelijk bestuurlijke verantwoordelijkheid bij het bestuur.

Voor hoger onderwijs- en onderzoeksinstellingen die onder de wet vallen, verschuift het kader daarmee van het sectorale toetsingskader (SURFaudit) naar expliciete wettelijke eisen. Waar instellingen zich tot nu toe verantwoordden binnen sectorale afspraken, geldt straks naleving van wettelijke verplichtingen en extern toezicht. Dit betekent dat van instellingen een verdergaande mate van samenhang, besturing en aantoonbaarheid wordt gevraagd dan tot nu toe gebruikelijk was.

Deze opgave is voor individuele instellingen omvangrijk en complex. Tegelijkertijd hebben HO-instellingen een grotendeels vergelijkbare inrichting van hun bedrijfsvoering, ICT-landschap en informatiehuishouding. Dat maakt het mogelijk – en logisch – om deze professionaliseringsslag niet individueel maar gezamenlijk als sector te organiseren. Daarbij is het van belang om de bestaande samenwerking met de mbo-sector, die niet onder de Cbw valt, te borgen en te betrekken bij de doorontwikkeling van de binnen het hoger onderwijs vereiste aanpassingen. Hiermee wordt de digitale weerbaarheid samenhangend en sectoroverstijgend versterkt.

1.1 Doelstelling

Om de gezamenlijke opgave van de Cbw gestructureerd en doelgericht aan te pakken, wordt binnen de HO-sector intensief samengewerkt in de vorm van een sectorbreed transitieprogramma. Hiermee richt het programma zich op een deel van de bij SURF aangesloten instellingen. Het is de bedoeling om alle ontwikkelde resultaten geschikt te maken en beschikbaar te stellen voor alle leden.

Dit programma is nadrukkelijk opgezet vanuit het principe van sectorale samenwerking. Instellingen binnen het HO concurreren niet op de inrichting van hun bedrijfsvoering, ICT en informatiebeveiliging.

Door gezamenlijk op te trekken in een grotendeels gelijksoortige inrichting (80/20-principe), gebaseerd op de HORA als referentiearchitectuur, is het efficiënter om samen te werken, kennis te delen en sectorale afspraken eenduidig door te voeren.

In de digitale strategie hbo is het thema informatiebeveiliging als een van de acht sectorale samenwerkingsgebieden gedefinieerd. De autonomie van instellingen blijft bestaan via het principe 'comply or explain': instellingen volgen de gezamenlijke lijn, of onderbouwen op

bestuursniveau waarom zij hier gemotiveerd van afwijken. Ook in het tempo van uitvoering blijft deze autonomie bestaan. Wanneer een instelling substantieel achterblijft, geldt eveneens het principe van 'comply or explain'. Het kan andersom ook zo zijn dat instellingen voorlopen op het transitieprogramma, waarbij zij het tempo aan blijven houden dat past bij hun instelling.

Dit programma heeft als doel om in gezamenlijkheid de HO-sector te ondersteunen bij:

- de registratie- en meldplicht bij inwerkingtreding van de Cbw;
- de zorgplicht, uiterlijk 36 maanden na inwerkingtreding van de Cbw;
- en het daarvoor realiseren van een werkend Information Security Management System (ISMS) gebaseerd op ISO/IEC 27001:2022.

De ontwikkelde resultaten dienen ook geschikt te zijn voor andere instellingen die vrijwillig dit traject willen volgen.

1.2 Scope en doelgroep

De scope van het transitieprogramma omvat alle bij SURF aangesloten hoger onderwijs- en onderzoeksinstellingen (HO/WO) die onder de Cbw zijn aangewezen.

Parallel hieraan werkt mbo-digitaal binnen het programma Cyberveiligheid aan een eigen roadmap voor mbo-instellingen, waaronder de inrichting van een cyberweerbaarheidspool. Hoewel mbo-instellingen niet onder de Cbw zijn aangewezen, kent deze aanpak inhoudelijk sterke overeenkomsten met het transitieprogramma in het hoger onderwijs.

Tussen beide trajecten bestaat duidelijke overlap in thema's, aanpak en benodigde hulpmiddelen. Waar dit logisch en waardevol is, wordt actief de samenwerking gezocht. Door kennis, ervaringen, werkwijzen en ontwikkelde hulpmiddelen onderling te delen, kunnen beide programma's elkaar versterken en wordt onnodig dubbel werk binnen de onderwijssector voorkomen. Zo ontstaat, met respect voor sectorspecifieke verschillen, een meer samenhangende en efficiënte aanpak van cyberweerbaarheid binnen het gehele onderwijsdomein.

Instellingen blijven zelf verantwoordelijk voor de uitvoering van maatregelen en de naleving van de wet. Out-of-scope is het behalen van ISO/IEC 27001-certificering.

1.3 Normenkader en hun onderlinge samenhang

Het programma vertrekt vanuit ISO/IEC 27001:2022 en de CIS Controls, omdat deze standaarden aansluiten bij de uitgangspunten van de Cbw en een praktische basis bieden om digitale risico's te beheersen:

- ISO/IEC 27001:2022 biedt een gestructureerd raamwerk om verplichtingen systematisch en aantoonbaar te beheersen (strategisch-tactisch),
- terwijl de CIS Controls concrete maatregelen leveren voor de belangrijkste digitale risico's (operationeel control-framework).

1.4 De tien basismaatregelen in het programma

Onderstaande tabel toont per basismaatregel (BM) van de Cbw-zorgplicht (art. 21 lid 3) in welke werkpakketten deze is geborgd.

BM	Basismaatregel	Werkpakket	Onderwerpen
1	Risicoanalyse & beveiliging informatiesystemen	3.4.2 Risicobeoordeling & behandelplan	Risicomanagementbeleid incl. risico bereidheid (risk appetite), Business Impact Analyses, identificatie van kritieke processen en systemen. Uitvoeren van risicoanalyses (dreiging, impact, kans). Centraal risicoregister (incl. classificatie en prioritering). Risicobehandelplannen (mitigeren, accepteren, vermijden, overdragen). Expliciete risico-acceptatie door eerstelijnsmanagement. Monitoring, herbeoordeling en rapportage (PDCA)
2	Incidentbehandeling & verslaglegging	3.2.1 Sectorale 'meldkit' 3.2.2 Uniform meldproces en governance 3.2.3 Oefenen meldproces 3.4.4 Organisatorische maatregelen 3.4.5 Technologische maatregelen	Ontwikkelen en gebruiken sectorale 'meldkit' Uniform meldproces rollen en escalatie (governance). Detectie en signalering (o.a. logging en monitoring). Table-top en praktijksimulaties van meldproces Incidentenbehandeling en coördinatie (IR). Koppeling met BCM en meldplicht Crisisbeheersing en noodcommunicatie Vastlegging, lessons learned en verbeterplannen.
3	Bedrijfscontinuïteit, back-up & noodvoorzieningenplannen	3.4.4 Organisatorische maatregelen 3.4.5 Technologische maatregelen	Business Continuity Management (BCM). Business Continuity Plan (BCP). Koppeling BCM./BCP aan BIA. IT continuity en Disaster Recovery Plans (DRP). Backup-strategoe, herstelprocedures en periodiek testen. Crisisbeheersing en noodcommunicatie
4	Beveiliging toeleveringsketen	3.4.4 Organisatorische maatregelen 3.4.5 Technologische maatregelen	Leveranciers- & ketenrisicomanagement Veilige verwerving van diensten en systemen. Third party risk management (TPRM), beoordeling van assurance verklaringen. Contractuele beveiligingseisen en security agreements. Right to audit en periodieke herbeoordeling.
5	Beveiliging verwerving, ontwikkeling & onderhoud netwerk en systemen	3.4.5 Fysieke & technologische maatregelen	Security by design and default Veilige ontwikkeling en verwerving. Wijzigingenbeheer (secure change). Asset- en configuratiebeheer Hardening, baselines en patchbaarheid. Netwerkbeveiliging en segmentatie
6	Effectiviteit van maatregelen en beheersen van risico's	3.4.2 Risicobeoordeling & behandelplan 3.4.4 Organisatorische maatregelen 3.4.5 Technologische maatregelen	Beoordelen effectiviteit van maatregelen Gebruik van actuele dreigingsinformatie Kwetsbaarhedenbeheer en patchmanagement Logmanagement en analyse Periodieke reviews en bijsturing (PDCA) Input voor audits, managementreview en verantwoording
7	Bewustzijn, opleiding & training	3.4.3 Mensen, middelen & documentatie 3.3.1 Cbw-training	Beschikbaarheid van middelen en competenties Cyberhygiëne en algemeen bewustzijn Rol-specifieke opleidingen (bijv. IT, onderzoek, management) CBW-training voor bestuurders en leidinggevenden
8	Cryptografie & encryptie	3.4.5 Technologische maatregelen	Toepassing cryptografie en encryptie (data-at-rest / in-transit) Sleutelbeheer en lifecycle management
9	Personeelsbeveiliging,	3.4.4 Organisatorische maatregelen	Personele beveiliging (in-, door- en uitstroom) Gedragsregels en geheimhoudingsverplichtingen

	toegangsbeleid & assetbeheer	3.4.5 Technologische maatregelen	Informatieclassificatie en verwerkingsregels Datalevenscyclus (bewaartermijnen, archivering, vernietiging) Toegangsbeleid en autorisatiestructuur Identity & access management (technisch) Asset- en configuratiebeheer Fysieke toegang en beveiligde zones
10	MFA, beveiligde & noodcommunicatie	3.4.5 Technologische maatregelen	Multi-factor authenticatie (MFA) Beveiligde communicatiekanalen Noodcommunicatie ter ondersteuning van incident- en crisisbeheersing

2 Programma op hoofdlijnen

Het programma bestaat uit vier parallelle, onderling afhankelijke streams die inhoudelijk onderscheidend zijn maar in de uitvoering nauw verweven.

De eerste stream richt zich op de registratieplicht: het tijdig en correct registreren van de instelling als entiteit in het Cbw-register. De tweede stream omvat de meldplicht: het inrichten van een werkend meldproces, inclusief een sectorale meldkit, uniforme werkwijze en governance voor het herkennen, classificeren en melden van significante incidenten. De derde stream ondersteunt bestuurders met een op de Cbw toegesneden training, zodat zij hun wettelijke verantwoordelijkheden aantoonbaar kunnen invullen. De vierde en omvangrijkste stream richt zich op het inrichten van een werkend ISMS op basis van ISO/IEC 27001, waarmee tegelijkertijd de zorgplicht structureel wordt geborgd en aantoonbaar beheerd. In hoofdstuk 3 zijn deze streams verder uitgewerkt.

2.1 Uitgangspunten

Het programma rust op vier uitgangspunten die richting geven aan de inrichting en uitvoering van de aanpak.

Risicogebaseerde aanpak
Centraal staat een risicogestuurde benadering, waarbij instellingen op basis van hun eigen risicoprofiel bepalen welke maatregelen prioriteit hebben en hoe deze passend worden ingericht. Niet het afvinken van maatregelen staat voorop, maar het aantoonbaar beheersen van relevante risico's.

Werken binnen gezamenlijke sectorale kaders
Instellingen werken binnen gezamenlijk afgesproken referentiekaders, gebaseerd op internationaal erkende standaarden zoals ISO/IEC 27001, ISO/IEC 27002 en de CIS Controls. Deze kaders bieden houvast en zorgen voor een grotendeels geharmoniseerde inrichting, terwijl ruimte blijft voor instellingsspecifieke keuzes.

'Comply or explain'-mechanisme
Instellingen passen de gezamenlijk afgesproken uitgangspunten toe, of lichten gemotiveerd toe waarom in hun specifieke context een andere afweging is gemaakt. Dit mechanisme bewaakt de gezamenlijke lijn, met respect voor autonomie.

Sectorale samenwerking en kennisdeling
Samenwerking tussen instellingen is een belangrijk uitgangspunt. Kennis, ervaringen, hulpmiddelen en best practices worden actief gedeeld binnen de sector. Instellingen met meer ervaring ondersteunen instellingen die nog stappen moeten zetten. Daarnaast wordt samengewerkt met het programma Cyberveiligheid van de mbo-sector, zodat ook sectoroverstijgend kennis, producten en ervaringen worden gedeeld en benut.
Hierdoor wordt versnelling gerealiseerd en wordt dubbel werk voorkomen.

De focus van het programma ligt nadrukkelijk op het implementeren en duurzaam borgen van maatregelen. Bestuurlijke betrokkenheid is daarbij een voorwaarde: het management blijft gedurende het gehele programma verantwoordelijk voor voortgang, prioritering en besluitvorming. Om efficiëntie en consistentie te waarborgen, sluit het programma aan bij bestaande middelen en kennis van het Security Expertise Centrum (SEC).

De uitwerking van de streams en werkpakketten laat zien hoe een geharmoniseerde inrichting er in de praktijk uit kan zien. Deze zijn niet bedoeld als individueel stappenplan, maar als gedeelde richting voor de sector. Instellingen kunnen op onderdelen faseren of bestaande keuzes respecteren (bijvoorbeeld recent vastgesteld beleid), maar nemen wel deel aan de gezamenlijke uitwerking en kennisdeling.

2.2 Kritische succesfactoren

Naast de uitgangspunten zijn er factoren die bepalen of het programma daadwerkelijk effect heeft en de doelstellingen behaalt. Bestuurlijk commitment is hierbij essentieel: bestuurders moeten actief betrokken zijn, besluiten nemen en middelen beschikbaar stellen. Ook transparantie en onderlinge verantwoording tussen instellingen dragen bij aan succes, omdat ze kennisdeling versterken en leren van ervaringen mogelijk maken.

Praktische toepasbaarheid is een andere belangrijke succesfactor. Werkpakketten, templates, formats en handreikingen moeten direct inzetbaar zijn in de dagelijkse praktijk, zodat instellingen snel stappen kunnen zetten in de implementatie van de Cbw-verplichtingen en het ISMS.

Tot slot is continuïteit in uitvoering belangrijk: gedurende de looptijd van ongeveer 36 maanden moet de implementatie consistent worden voortgezet, zodat maatregelen niet tijdelijk blijven maar structureel worden geborgd.

2.3 De motor van het programma

De voortgang van het programma wordt gedragen door een reeks fysieke werksessies waarin instellingen actief werken aan hun eigen implementatie. De sessies worden voorbereid door SURF met input van de CISO beraden en vinden circa elke drie maanden plaats, met een hogere frequentie in de opstartfase wanneer de funderende keuzes over scope, governance en risicobeoordeling worden gemaakt. Iedere sessie start met de terugkoppeling van het huiswerk

uit de vorige sessie en sluit af met het definiëren van concrete vervolgacties voor de volgende periode. Tussen de sessies voeren instellingen werkpakketten uit die bijdragen aan de bouwblokken van de zorgplicht en de inrichting van het ISMS.

De sessies volgen de fasen van ISO/IEC 27001:2022 als leidraad — van context en risicobeoordeling via implementatie naar evaluatie en verbetering. De Cbw-zorgplichtvereisten zijn per fase expliciet gekoppeld, zodat instellingen door het inrichten van een werkend ISMS tegelijk aantoonbare compliance met de Cbw realiseren.

De voortgang en aantoonbaarheid van maatregelen worden gespiegeld aan de eisen van ISO/IEC 27001:2022 en de tien basismaatregelen van de Cbw-zorgplicht.

2.4 GAP-analyse als vertrekpunt

Voorafgaand aan de eerste werksessie, voeren alle deelnemende instellingen een gestandaardiseerde GAP-analyse[1] (nulmeting) uit. Met 'gestandaardiseerd' wordt bedoeld dat alle deelnemende instellingen zichzelf langs dezelfde inhoudelijke meetlat, de tien basismaatregelen van de Cbw-zorgplicht, beoordelen. Deze analyse vormt het inhoudelijke vertrekpunt van het programma en geeft inzicht in de mate waarin de tien basismaatregelen van de zorgplicht passend, samenhangend en aantoonbaar zijn ingericht en bestuurd.

De GAP-analyse is nadrukkelijk geen checklist van losse maatregelen of documenten, maar een instrument om vast te stellen in hoeverre een instelling 'in control' is op maatregelniveau. Daarbij wordt gekeken naar de werking van beleid, processen, rollen, technische voorzieningen en governance in hun onderlinge samenhang, volgens de PDCA-gedachte van ISO/IEC 27001:2022.

De uitkomsten van deze analyse vormen:

- het startpunt voor de werksessies;
- de basis voor prioritering van werkpakketten binnen de instelling;
- en gedurende het programma de meetlat voor voortgang en aantoonbaarheid.

2.4.1 Doel en uitgangspunten

De GAP-analyse heeft als doel inzicht te geven in de mate waarin de tien basismaatregelen uit de zorgplicht structureel, risicogestuurd en bestuurlijk aantoonbaar functioneren.
De analyse richt zich op de effectieve besturing en werking van deze basismaatregelen en niet op het afvinken van individuele controls, normen of documenten. De centrale vraag is telkens:

> *In hoeverre functioneert deze basismaatregel als samenhangend geheel binnen de instelling, en waar is versterking nodig?*

2.4.2 Scope en beoordelingsniveau

De analyse wordt uitgevoerd per basismaatregel (BM 1–10). Iedere basismaatregel wordt beschouwd als een samenhangend maatregelcluster, bestaande uit:

- beleid en kaders,
- processen en werkwijzen,
- rollen en verantwoordelijkheden,

[1] OCW gaat nog duiding geven aan de zorgplicht. Dit kan van invloed zijn op de GAP-analyse.

- technische voorzieningen,
- en governance en sturing.

Bovengenoemde individuele onderdelen worden niet als zelfstandig PDCA-object beoordeeld, maar in hun bijdrage aan de werking van de basismaatregel als geheel.

2.4.3 Beoordeling volgens PDCA-cyclus

Per basismaatregel wordt beoordeeld in hoeverre de volledige PDCA-cyclus functioneert:

- Plan
  Of passende beleidsmatige kaders, uitgangspunten en verantwoordelijkheden zijn vastgesteld en of risicogestuurde keuzes zijn gemaakt over scope en ambitieniveau.
- Do
  Of processen, organisatorische maatregelen en technische voorzieningen daadwerkelijk zijn ingericht, belegd en toegepast.
- Check
  Of monitoring, logging, evaluatie, toetsing, audits, oefeningen of reviews plaatsvinden op de werking van de maatregel als geheel.
- Act
  Of bevindingen uit de Check-fase leiden tot aantoonbare bijsturing en verbetering van maatregelen, processen, beleid of prioriteiten.

2.4.4 Meet- en waarderingsmodel

De GAP-analyse kent geen totaalscores of rapportcijfers. Per basismaatregel wordt per PDCA-fase kwalitatief beschreven in hoeverre de maatregel is ingericht, toegepast, geëvalueerd en bijgestuurd. De beschrijvingen dienen primair ter ondersteuning van het gesprek over risico's, proportionaliteit en verbeterprioriteiten binnen de context van de instelling. Zij zijn nadrukkelijk niet bedoeld als benchmark of normatieve eindscore tussen instellingen.

2.4.5 Weergave en gebruik van de resultaten

Per basismaatregel wordt vastgelegd:

- een PDCA-profiel (Plan/Do/Check/Act) met toelichting;
- een kwalitatieve duiding van de mate van beheersing;
- concrete verbeterpunten gericht op het versterken van ontbrekende zwakkere PDCA-fasen.

Instellingen die al beschikken over eerdere audits, maturity-metingen of zelfevaluaties kunnen deze gebruiken als input, maar vullen deze GAP-analyse alsnog in ten behoeve van onderlinge vergelijkbaarheid binnen het programma.

2.4.6 Vertrouwelijkheid en sectorbeeld

De GAP-analyse wordt uitgevoerd vóór de eerste werksessie, uiterlijk vier weken voorafgaand aan de start van het programma. De individuele resultaten blijven binnen de instelling.
Op basis van de aangeleverde analyses wordt een geanonimiseerd sectorbeeld opgesteld. Dit beeld laat patronen, veelvoorkomende hiaten en gedeelde aandachtspunten zien en wordt gebruikt als gezamenlijk vertrekpunt tijdens de openingssessie.

2.4.7 De GAP-analyse als meetlat gedurende het programma

Halverwege het programma en aan het einde van het programma wordt dezelfde analyse herhaald. De vergelijking met de oorspronkelijke uitkomsten maakt de ontwikkeling per basismaatregel en per PDCA-fase zichtbaar.

De GAP-analyse vervult daarmee niet alleen een diagnostische rol bij aanvang, maar fungeert gedurende het gehele programma als instrument voor sturing, prioritering en bestuurlijke aantoonbaarheid.

3 Streams en werkpakketten

Het programma bestaat uit vier parallelle, onderling afhankelijke stromen die in de tijd logisch zijn gefaseerd rond de inwerkingtreding van de Cbw (T0).

Elke stream is uitgewerkt in werkpakketten. Een werkpakket heeft een eigenaar, een meetbaar resultaat, globale planning en een expliciete koppeling naar het toepasselijke normenkader.

Leeswijzer
In de tabellen wordt gewerkt met T-aanduidingen in **maanden** ten opzichte van het moment waarop de Cyberbeveiligingswet in werking treedt.

- **T0** = maand van inwerkingtreding van de Cbw (startpunt van de wettelijke verplichtingen)
- **T0 + 2** = twee maanden ná inwerkingtreding
- **T0 – 3** = drie maanden vóór inwerkingtreding

Alle genoemde aantallen hebben betrekking op **kalendermaanden** ten opzichte van T0.

3.1 Stream 1: Registratieplicht

3.1.1 Registreren als entiteit in het Cbw-register

Werkpakket	Resultaten	Normkoppeling	Planning
Registreren in Cbw-register	Correcte registratie in Cbw-register. Geborgd proces voor actualisatie van gegevens.	Cbw: Hfst. 10, 11 en 12	Voor T0

3.2 Stream 2: Meldplicht

3.2.1 Sectorale ‘meldkit’

Werkpakket	Resultaten	Normkoppeling	Planning
Ontwikkelen sectorale ‘meldkit’	Beschikbare ‘meldkit’ die instellingen direct kunnen toepassen bij incidenten.	Cbw: Hfst. 8	Voor T0

3.2.2 Uniform meldproces en governance

Werkpakket	Resultaten	Normkoppeling	Planning
Uniform meldproces	Duidelijk sectorbreed afgestemd proces voor melden van incidenten.	Cbw: Hfst. 8	Voor T0
Governance	Vastgelegde interne governance waarmee tijdige en juiste melding binnen de instelling is geborgd.	Cbw: Hfst. 8	Voor T0

3.2.3 Oefenen meldproces

Werkpakket	Resultaten	Normkoppeling	Planning

Table-top meldproces	Geoefend meldproces met concrete verbeteracties per instelling.	Cbw: Hfst. 8	Voor T0

3.3 Stream 3: Cbw-training voor bestuurders

3.3.1 Cbw-training

Werkpakket	Korte beschrijving	Resultaat	Planning
Ontwikkelen Cbw-training	Beschikbare Cbw-training overeenkomstig	Cbw: art. 24	Voor T0
Volgen Cbw-training	Bestuurders (en hoger management) opgeleid en gecertificeerd.	Cbw: art. 24	T0 – T0+12

3.4 Stream 4: Implementatie werkend ISMS incl. borging zorgplicht

3.4.1 Context & strategie

Werkpakket	Resultaten	Normkoppeling	Planning
Context & Scope	ISMS-scope en kritieke diensten vastgesteld. Context- en stakeholderanalyse gedocumenteerd. Bestuurlijk vastgestelde ISMS-scope.	ISO 27001: 4.1 · 4.2 · 4.3 · 4.4 ISO 27002: 5.1 Cbw: art. 21 lid 1 Cbb: art. 2	T0 – T0+2
Informatiebeveiligingsbeleid & governance	Bestuurlijk vastgesteld IB-beleid. Rollen, verantwoordelijkheden en rapportagestructuur ingericht. Governance operationeel.	ISO 27001: 5.1 · 5.2 · 5.3 ISO 27002: 5.1 · 5.2 · 5.3 · 5.4 Cbw: art. 21 · art. 23 Cbb: art. 2	T0 – T0+2
Compliance-register	Actueel compliance-register als formeel ISMS-document. Alle toepasselijke wettelijke, regelgevende en contractuele eisen geïnventariseerd. Basis voor VvT-volledigheidscheck.	ISO 27001: 4.2 · 6.1.3 ISO 27002: 5.31 · 5.36 Cbw: art. 21 · art. 22 Cbb: art. 2–12 Zorgplicht BM: 1–10	T0 – T0+3
Proportionaliteitsonderbouwing	Proportionaliteitsmatrix gedocumenteerd. Afweging stand van techniek, kosten en blootstelling per risicocategorie vastgelegd. Verbonden aan risicoregister en VvT.	ISO 27001: 6.1.2 · 6.1.3 ISO 27002: 5.1 Cbw: art. 22 Cbb: art. 2 · art. 13 Zorgplicht BM: 1–10	T0 – T0+3

3.4.2 Risicobeoordeling & behandelplan

Werkpakket	Resultaten	Normkoppeling	Planning
Risicomanagementbeleid	Bestuurlijk vastgesteld risicomanagementbeleid. Methodiek, acceptatiecriteria en procedures voor risicoanalyse vastgelegd.	ISO 27001: 6.1.1 · 6.1.2 · 8.2 ISO 27002: 5.1 Cbw: art. 21 Cbb: art. 2 · art. 3 Zorgplicht BM: 1	T0+1 – T0+3
Risicobeoordeling & behandelplan	Gedocumenteerd risicoregister.	ISO 27001: 6.1.2 · 6.1.3 · 8.2 · 8.3 ISO 27002: 5.7	T0+2 – T0+5

	Vastgesteld behandelplan met acceptatiecriteria. Concept-VvT opgesteld.	Cbw: art. 21 · art. 22 Cbb: art. 3 · art. 4 Zorgplicht BM: 1	
Beleid effectiviteitsbeoordeling	Bestuurlijk vastgesteld effectiviteitsbeleid. Methodiek, cadans en verantwoordelijkheden voor periodieke meting vastgelegd. Basis voor KPI/KRI-meting (zie 3.4.6).	ISO 27001: 6.1 · 9.1 ISO 27002: 5.1 Cbw: art. 21 · art. 23 Cbb: art. 12	T0+2 – T0+4

3.4.3 Mensen, middelen & documentatie

Werkpakket	Resultaten	Normkoppeling	Planning
Documentatiestructuur ISMS	Werkende ISMS-documentatiestructuur. Beleid, procedures en registraties ingericht. Versie- en archiefbeheer operationeel.	ISO 27001: 7.5.1 · 7.5.2 · 7.5.3 ISO 27002: 5.37 Cbw: art. 21 Cbb: art. 2	T0+3 – T0+8
Middelen & competenties	Middelenallocatie vastgesteld. Competentiematrix opgesteld. Competentiegaten geïdentificeerd en aanpak belegd.	ISO 27001: 7.1 · 7.2 ISO 27002: 6.3 Cbw: art. 23 Cbb: art. 3 Zorgplicht BM: 10	T0+3 – T0+8
Cyberhygiëne & bewustzijn (algemeen)	Werkend bewustzijnsprogramma voor al het personeel. Aantoonbare basishygiëne. Meetbare trainingsresultaten.	ISO 27001: 7.3 ISO 27002: 6.3 Cbw: art. 21 Cbb: art. 3 · art. 9 Zorgplicht BM: 10	T0+4 – T0+22
Cyberopleidingen (specifieke rollen)	Formeel aangewezen beveiligingsrollen. Actueel opleidingsplan. Aantoonbare rol-specifieke trainingsresultaten.	ISO 27001: 7.2 · 7.3 ISO 27002: 6.3 Cbw: art. 21 · art. 24 Cbb: art. 3 · art. 9 Zorgplicht BM: 10	T0+4 – T0+22

3.4.4 Organisatorische & mensgerichte maatregelen

Werkpakket	Resultaten	Normkoppeling	Planning
Personele beveiliging	Formeel vastgestelde beveiligingsgevoelige rollen. Aantoonbare procedures voor screening en in-, door- en uitstroom. Koppeling aan toegangsbeheer en teruggave bedrijfsmiddelen geborgd.	ISO 27001: 8.1 ISO 27002: 6.1 · 6.2 · 6.4 · 6.5 · 6.6 Cbw: art. 21 · art. 22 Cbb: art. 5 · art. 9 Zorgplicht BM: 8	T0+4 – T0+10
Gedragsregels & geheimhouding	IB-verplichtingen vastgelegd in arbeidsvoorwaarden of aanvullende overeenkomsten.	ISO 27001: 8.1 ISO 27002: 6.2 · 6.4 · 6.6 Cbw: art. 21 Cbb: art. 5	T0+4 – T0+10

	Geheimhoudingsovereenkomsten ingericht voor relevante functies en externe partijen. Disciplinaire procedure vastgesteld en gecommuniceerd.	Zorgplicht BM: 8	
Informatieclassificatie & verwerkingsregels	Formeel vastgesteld classificatieschema. Verwerkingsregels per classificatieniveau. Alle assets gekoppeld aan een classificatieniveau. Grondslag voor toegangsbeleid, encryptie, logging en BCM-prioritering.	ISO 27001: 8.1 ISO 27002: 5.9 · 5.10 · 5.11 · 5.12 · 5.13 · 5.14 Cbw: art. 21 · art. 22 Cbb: art. 6 Zorgplicht BM: 1 en 8	T0+5 – T0+9
Toegangsbeleid & autorisatiestructuur	Formeel vastgesteld toegangsbeleid. Autorisatiestructuur op basis van least privilege en need-to-know. Scheiding van taken (SoD) gedocumenteerd. Periodieke toegangs- en autorisatiereviews als staand beheerproces belegd.	ISO 27001: 8.1 ISO 27002: 5.3 · 5.15 · 5.16 · 5.17 · 5.18 Cbw: art. 21 · art. 22 Cbb: art. 6 · art. 7 Zorgplicht BM: 8 en 9	T0+6 – T0+12
Incidentenbeheer, BCM & meldplicht	Formeel vastgesteld incidentbeheerbeleid incl. interne meldprocedure. Rollen, escalatielijnen en koppeling externe meldplicht geborgd. Formeel vastgesteld BCM-beleid.	ISO 27001: 8.1 ISO 27002: 5.24 · 5.25 · 5.26 · 5.27 · 5.28 · 5.29 · 5.30 Cbw: art. 14 · art. 15 · art. 21 Cbb: art. 10 · art. 12 Zorgplicht BM: 3 en 4	T0+6 – T0+22
Telewerken & mobiel werken	Formeel vastgesteld telewerk- en mobielwerkbeleid. Beveiligingseisen voor remote access en BYOD gedocumenteerd en gecommuniceerd.	ISO 27001: 8.1 ISO 27002: 6.7 Cbw: art. 21 · art. 22 Cbb: art. 6 · art. 7 Zorgplicht BM: 8 en 9	To+6 – T0+12
Leveranciers- & ketenbeveiliging	Formeel vastgesteld leveranciers- en ketenbeleid. Beveiligingseisen opgenomen in standaardcontracten en aanbestedingen. Actueel leveranciersoverzicht voor kritieke processen. Aantoonbaar werkend beoordelingsproces per leverancierscategorie.	ISO 27001: 8.1 ISO 27002: 5.19 · 5.20 · 5.21 · 5.22 · 5.23 Cbw: art. 21 · art. 22 Cbb: art. 8 Zorgplicht BM: 5	T0+9 – T0+30
Dreigingsinformatie	Operationeel dreigingsinformatieproces. Vastgelegde bronnen, beoordelingscadans en verantwoordelijken.	ISO 27001: 8.1 ISO 27002: 5.7 Cbw: art. 21 Cbb: art. 11 Zorgplicht BM: 1 en 6	T0+9 – T0+30

	Aantoonbare terugkoppeling naar risicoregister en kwetsbaarhedenbeheer.		

3.4.5 Fysieke & technologische maatregelen

Werkpakket	Resultaten	Normkoppeling	Planning
Asset & configuratiebeheer	Actuele assetinventaris per classificatieniveau (hardware, software, cloud, data). Veilige basisconfiguraties (hardening) vastgesteld en aantoonbaar toegepast op kritieke systemen. Wijzigingsbeheerproces ingericht als staand beheerproces (ITIL SACM/change management).	ISO 27001: 8.1 ISO 27002: 8.8 · 8.9 · 8.10 Cbw: art. 21 · art. 22 Cbb: art. 6 · art. 9 Zorgplicht BM: 2, 6 en 8	T05 – T0+12
Fysieke toegang & beveiligde zones	Formeel vastgesteld fysiek toegangsbeleid voor kritieke ruimten. Fysieke beveiligingsperimeter en toegangscontrole aantoonbaar geïmplementeerd. Procedures voor werken in beveiligde zones vastgelegd. Procedure veilig verwijderen en hergebruiken apparatuur en media ingericht.	ISO 27001: 8.1 ISO 27002: 7.1 · 7.2 · 7.3 · 7.4 · 7.5 · 7.6 · 7.7 · 7.8 · 7.9 · 7.10 · 7.11 · 7.12 · 7.13 · 7.14 Cbw: art. 21 · art. 22 Cbb: art. 5 Zorgplicht BM: 8	T0+6 – T0+12
Toegang & identiteit (technisch)	MFA operationeel op kritieke omgevingen. PAM-oplossing ingericht voor bevoorrechte accounts. Technische handhaving toegangsrechten aantoonbaar (endpoints, sessies, autorisatiebeheer).	ISO 27001: 8.1 ISO 27002: 8.1 · 8.2 · 8.3 · 8.4 · 8.5 · 8.6 Cbw: art. 21 · art. 22 Cbb: art. 6 · art. 7 Zorgplicht BM: 8 en 9	T0+6 – T0+12
Cryptografie & encryptie	Cryptografiebeleid technisch geïmplementeerd. Sleutelbeheerproces operationeel. Encryptie van data-at-rest en data-in-transit aantoonbaar toegepast op kritieke omgevingen.	ISO 27001: 8.1 ISO 27002: 8.24 Cbw: art. 21 · art. 22 Cbb: art. 7 Zorgplicht BM: 7	T0+6 - T0+12
Netwerkbeveiliging & segmentatie	Netwerksegmentatie aantoonbaar gerealiseerd op basis van classificatieniveaus. Beheer van netwerktoegang (intern, extern, remote) en netwerkdiensten ingericht als staand beheerproces.	ISO 27001: 8.1 ISO 27002: 8.20 · 8.21 · 8.22 Cbw: art. 21 · art. 22 Cbb: art. 6 Zorgplicht BM: 2 en 8	T0+9 – T0+18

	Beveiligde netwerkcommunicatie geïmplementeerd.		
Logmanagement, monitoring & detectie	Logbeleid vastgesteld en geborgd. Logging en centrale monitoring operationeel op kritieke omgevingen. SOC/SIEM ingericht en gedocumenteerd. Koppeling detectie naar incidentrespons aantoonbaar. Technische grondslag voor forensische bewijsverzameling ingericht.	ISO 27001: 8.1 ISO 27002: 8.15 · 8.16 · 8.17 Cbw: art. 21 · art. 22 Cbb: art. 10 · art. 11 Zorgplicht BM: 3 en 6	T09 + T0+15
Veilige ontwikkeling & verwerving	Secure-development-procedures gedocumenteerd en geborgd in het ontwikkelproces. Beveiligingstests als onderdeel van release- en wijzigingsproces. Beveiligingseisen opgenomen in standaardcontracten voor software, hardware en diensten	ISO 27001: 8.1 ISO 27002: 8.25 · 8.26 · 8.27 · 8.28 · 8.29 · 8.30 Cbw: art. 21 · art. 22 Cbb: art. 8 Zorgplicht BM: 2 en 5	T0+9 – T0+18
Kwetsbaarheden & patchmanagement	Werkend kwetsbaarheden- en patchmanagementproces. Patchcadans, CVSS-triage en tooling vastgesteld. Aantoonbare opvolging van kritieke kwetsbaarheden binnen vastgestelde termijnen.	ISO 27001: 8.1 ISO 27002: 8.8 · 8.19 Cbw: art. 21 · art. 22 Cbb: art. 9 · art. 10 Zorgplicht BM: 6	T0+9 – T0+30
Crisisbeheersing & noodcommunicatie	Formeel vastgesteld crisisbeheersingsplan. Noodcommunicatieplan (out-of-band) opgesteld. IR, BCM en externe meldplicht geïntegreerd in één crisisproces. Periodieke crisisoefeningen uitgevoerd en gedocumenteerd.	ISO 27001: 8.1 ISO 27002: 5.26 · 5.29 · 5.30 Cbw: art. 14 · art. 21 Cbb: art. 10 · art. 12 Zorgplicht BM: 3 en 4	T0+12 – T0+30

3.4.6 Meten, beoordelen & verklaren

Werkpakket	Resultaten	Normkoppeling	Planning
KPI / KRI meting & monitoring	Werkende KPI/KRI-meting per maatregel. Eerste meetresultaten beschikbaar. Periodieke rapportage aan bestuur/directie ingericht.	ISO 27001: 9.1 ISO 27002: 5.36 Cbw: art. 21 · art. 23 Cbb: art. 12 Zorgplicht BM: 1–10	T0+15 – T0+30
Interne audit	Auditprogramma vastgesteld. Interne audit uitgevoerd conform ISO 27001 clausule 9.2.	ISO 27001: 9.2.1 · 9.2.2 ISO 27002: 5.35 Cbw: art. 21 · art. 23	T0+16 – T0+22

	Auditrapport met bevindingen en verbeteracties opgeleverd.	Cbb: art. 12	
Management reviews	Tussentijdse managementreview gedocumenteerd. Formele directiebeoordeling uitgevoerd. Bestuurlijk vastgestelde verbeteracties. Opvolgingsacties belegd.	ISO 27001: 9.3.1 · 9.3.2 · 9.3.3 ISO 27002: 5.35 Cbw: art. 23 Cbb: art. 12	T0+16 – T0+24
Verklaring van Toepasselijkheid	Bestuurlijk vastgestelde VvT. Volledigheidscheck alle Cbw/Cbb-controls afgerond. Proportionaliteitsonderbouwing definitief gedocumenteerd.	ISO 27001: 6.1.3 ISO 27002: thema 5–8 Cbw: art. 21 · art. 22 Cbb: art. 2–12 · art. 13 Zorgplicht BM: 1–10	T0+19 – T0+24
Zelfevaluatie & bestuurlijke rapportage	Zelfevaluatie uitgevoerd. Uitkomsten bestuurlijk gerapporteerd. 30-dagen-plan voor resterende acties richting T0+36 opgesteld. Instelling aantoonbaar in control.	ISO 27001: 9.1 · 9.3 ISO 27002: 5.35 · 5.36 Cbw: art. 21 · art. 23 Cbb: art. 12 · art. 13 Zorgplicht BM: 1–10	T0+28 – T0+30

3.4.7 Verbeteren, testen & borgen

Werkpakket	Resultaten	Normkoppeling	Planning
Stresstest	Realistisch scenario (bijv. ransomware met ketencomponent) gesimuleerd en geëvalueerd. IR, detectie, BCM, crisisbeheersing en meldplicht integraal getest. Bevindingen gedocumenteerd en deelnemers getraind.	ISO 27001: 10.1 · 10.2 ISO 27002: 5.26 · 5.29 · 5.30 Cbw: art. 14 · art. 21 Cbb: art. 11 · art. 12 Zorgplicht BM: 3 en 4	T0+22 - T0+24
Verbetercyclus	Simulatiebevindingen vertaald naar verbeteracties. Risicoregister en behandelplan geactualiseerd. Verbeteracties belegd en in uitvoering.	ISO 27001: 10.1 · 10.2 ISO 27002: 5.27 Cbw: art. 21 Cbb: art. 4 · art. 12 Zorgplicht BM: 1–10	T0+23 – T0+27
Aantoonbaarheidsdossier	Volledig en toetsbaar ISMS-dossier per Cbw/Cbb-control. Beleid, implementatiebewijzen, KPI-resultaten, VvT en compliance-register gebundeld. Gereed voor toezichthouder, externe audit en/of ISO-certificering.	ISO 27001: 7.5 · 9.1 · 9.2 · 9.3 ISO 27002: 5.36 Cbw: art. 21 · art. 23 · art. 25 Cbb: art. 2–12 Zorgplicht BM: 1–10	T0+27 – T0+30
Borgingsplan na programma	Eigenaarschap en verantwoordelijkheden voor continuering ISMS vastgelegd.	ISO 27001: 10.1 · 9.3 ISO 27002: 5.1 Cbw: art. 21 · art. 23 Cbb: art. 2 · art. 12	T0+28 – T0+30

	Jaarlijkse cadans (managementreview, auditcyclus, risicoherziening) belegd. Herzieningstermijn beleidspiramide formeel vastgesteld. ISMS levend na afloop van het programma.		

4 Governance van het transitieprogramma

Een sectoraal transitieprogramma vraagt om een andere vorm van governance dan een traditioneel project. De nadruk ligt niet op formele beheersing maar op gedeelde verantwoordelijkheid, onderlinge stimulering en bestuurlijk eigenaarschap. De aansturing ligt bij de Regiegroep Innovatiezone Cyberveiligheid, die de voortgang van het programma bewaakt, sectorale besluitvorming faciliteert en de verbinding onderhoudt met het programma Cyberveiligheid binnen de mbo-sector, brancheorganisaties, het ministerie van OCW. De Regiegroep vergadert elke twee maanden en ontvangt tussen de vergaderingen periodieke voortgangsrapportages van de programmacoördinator.

De governance van dit programma is faciliterend en verbindend. Zij vervangt geen lokale besluitvorming, maar ondersteunt het gezamenlijk optrekken van instellingen in een grotendeels gelijksoortige inrichting. De regiegroep en brancheorganisaties hebben geen toezichthoudende of besluitvormende rol richting instellingen. Het programma ondersteunt, verbindt, biedt hulpmiddelen en streeft naar het bevorderen van synergie, kennisdeling en onderlinge aanspreekbaarheid binnen de sector. De verantwoordelijkheid voor keuzes, prioriteiten en implementatie ligt volledig bij de instellingen zelf.

4.1 Programmaorganisatie

De dagelijkse aansturing van het programma ligt bij een programmacoördinator, ondersteund door een klein programmateam. De programmacoördinator is verantwoordelijk voor de voorbereiding en begeleiding van de werksessies, de verwerking van de nulmetingen tot een geanonimiseerd sectoroverzicht, de bewaking van de voortgang op de werkpakketten en de rapportage aan de Regiegroep. Het programmateam onderhoudt de verbinding met het Security Expertise Centrum (SEC), de CISO-beraden en het programma Cyberveiligheid (later de mbo Cyberweerbaarheidspool) van de mbo-sector en beheert de gedeelde kennisinfrastructuur van het programma, waaronder de werkpakketten, templates en formats.
Per deelnemende instelling is een contactpersoon aangewezen die als aanspreekpunt fungeert voor de programmacoördinator en de voortgang binnen de eigen instelling coördineert. In de meeste gevallen zal dit de CISO of een functioneel equivalent zijn.

4.2 Rol van bestuur en management

Bestuurders zijn eigenaar van de informatiebeveiligingsrisico's binnen hun instelling en dragen eindverantwoordelijkheid voor de naleving van de Cbw-zorgplicht. Hun actieve betrokkenheid is een kritische succesfactor voor het programma. Concreet vervullen bestuurders de volgende rol:

- Vaststellen van de risicobereidheid en het informatiebeveiligingsbeleid van de instelling.
- Beschikbaar stellen van de benodigde middelen in mensen, tijd en budget.
- Ontvangen van en besluiten nemen op basis van periodieke voortgangsrapportages.
- Deelname aan bestuurlijke peersessies, waarin ervaringen en dilemma's worden gedeeld.
- Volgen van de verplichte Cbw-training volgens artikel 24 van de wet, uiterlijk binnen twee jaar na inwerkingtreding.
- Stimuleren en bewaken van de voortgang op de werkpakketten binnen de eigen organisatie.

4.3 Rol van CSC's en CISO's

De CISO of de medewerker die deze rol vervult is de dagelijkse trekker van het programma binnen de instelling. Zij vertalen de bestuurlijke kaders naar concrete implementatieactiviteiten, bewaken de voortgang op de werkpakketten en zorgen voor de inhoudelijke voorbereiding op de werksessies. Specifiek omvat hun rol het volgende.

De CISO bereidt de nulmeting voor en stelt de top-drie bevindingen op die de instelling inbrengt in de openingssessie. Gedurende het programma beheert de CISO het risicoregister, het behandelplan en de groeiende documentatiestructuur van het ISMS. De contactpersoon (H 4.1) hierboven) is de eerste gesprekspartner van de programmacoördinator bij knelpunten in de uitvoering.

De verantwoordelijk bestuurder treedt op als opdrachtgever en draagt de eindverantwoordelijkheid voor dit traject. De CISO leidt, in nauwe samenwerking met de CSC, de uitvoering en faciliteert de voortgang van de werkpakketten.

De opdrachtgever levert en borgt de benodigde middelen en stelt de technische en operationele expertise beschikbaar die noodzakelijk is voor de uitvoering van de werkpakketten op het gebied van toegangsbeleid, patchmanagement, logmanagement en detectie. De CSC werkt daarbij intensief samen met de CISO. De CISO rapporteert over de voortgang en resultaten aan het bestuur. De rol van de CSC is daarbij gericht op de toekomstige ontwikkeling van de sectorvoorzieningen en de CISO op het 'as is'.

Binnen het sectorale verband nemen CISO's en CSC's actief deel aan inhoudelijke werksessies. Zij dragen bij aan de ontwikkeling en het onderhoud van de gedeelde kennisinfrastructuur en ondersteunen, waar mogelijk, collega-instellingen die zich in een eerdere fase van implementatie bevinden. Daarnaast nemen ook vertegenwoordigers van het programma Cyberveiligheid in de mbo-sector deel aan de werksessies en de ontwikkeling en het onderhoud van de gedeelde kennisinfrastructuur.

4.4 Comply or explain en sectorale verantwoording

Instellingen leggen tijdens de werksessies onderling verantwoording af over de voortgang op de werkpakketten. Dit creëert een professioneel en sociaal mechanisme dat voortgang stimuleert zonder dat het programma een formeel audit- of verantwoordingsinstrument wordt. Het onderscheid is wezenlijk: verantwoording in de sessies is gericht op leren, delen en verbeteren en niet op beoordelen of sanctioneren.

Het centrale mechanisme is 'comply or explain': instellingen werken aantoonbaar aan de werkpakketten, of leggen gemotiveerd uit waarom een specifieke maatregel niet of anders wordt toegepast, gelet op de eigen context en proportionaliteit. Dit sluit aan bij de bedoeling van de Cbw, die passende en evenredige maatregelen vraagt en ruimte laat voor een onderbouwde afweging.

De voortgang op de werkpakketten en het ISMS kan op elk moment worden gespiegeld aan de ISO/IEC 27001:2022 en de 10 basismaatregelen van de Cbw-zorgplicht. Dit geeft bestuurders, CISO's en CSC's zekerheid dat de ingezette verbeteringen aansluiten op de manier waarop later door de Inspectie van het Onderwijs naar naleving zal worden gekeken. Zo ontstaat een situatie

waarin instellingen praktisch werken aan verbetering, tegelijkertijd voorbereid zijn op externe toetsing, en dit alles zonder dat het programma zelf een auditstructuur introduceert.

Wanneer een instelling gedurende langere tijd geen voortgang boekt op essentiële werkpakketten, treedt de programmacoördinator in overleg met de betrokken instelling om oorzaken te achterhalen en ondersteuning te organiseren. Structurele achterblijvers worden gesignaleerd aan de Regiegroep, die bepaalt of aanvullende maatregelen nodig zijn. Het programma kent geen sanctiemechanisme, maar de Regiegroep kan besluiten een instelling intensiever te begeleiden of in het uiterste geval te adviseren zelfstandig externe ondersteuning in te schakelen.

4.5 Sectorale samenwerking

Instellingen bevinden zich op verschillende niveaus van volwassenheid. Dit verschil wordt in het programma benut als een kracht: meer ervaren instellingen ondersteunen instellingen die minder ver zijn, zodat kennis en werkwijzen actief worden gedeeld.

Dit gebeurt op drie manieren. Tijdens de werksessies wisselen instellingen ervaringen uit, bespreken ze dilemma's en geven ze elkaar concrete tips over de uitvoering van werkpakketten. Buiten de sessies worden templates, formats, risicoanalyses en beleidsvoorbeelden gedeeld via de gemeenschappelijke kennisinfrastructuur van het programma. Daarnaast kunnen instellingen op verzoek een meer ervaren collega-instelling raadplegen voor peer coaching bij specifieke implementatievraagstukken.

De sectorale samenwerking is geen vrijblijvende aanvulling, maar een structureel onderdeel van de aanpak. Deze manier van samenwerken sluit naadloos aan bij de digitale strategie van zowel de Vereniging Hogescholen als Universiteiten van Nederland, waarin gezamenlijke ontwikkeling en kennisdeling op het gebied van digitalisering en informatiebeveiliging expliciet als speerpunt zijn benoemd. Daarnaast vertoont deze aanpak duidelijke raakvlakken met het programma Cyberveiligheid van mbo-digitaal, waarin mbo-instellingen eveneens intensief samenwerken aan het versterken van hun cyberweerbaarheid.

Instellingen die al verder zijn bouwen hiermee ook aan hun eigen volwassenheid: het uitleggen en overdragen van kennis verdiept het begrip en verankert werkwijzen binnen de eigen organisatie.

4.6 Borging en continuïteit

Na afloop van het programma beschikt de sector over een gemeenschappelijk referentiekader en een set van gedeelde werkwijzen die blijvend bijdragen aan digitale weerbaarheid. De borging van deze infrastructuur is een expliciete verantwoordelijkheid van de Regiegroep.

Concreet betekent dit dat de ISO/IEC 27001:2022 als blijvend referentie-instrument voor de sector beschikbaar blijft en periodiek wordt geactualiseerd op basis van wijzigingen in wet- en regelgeving of dreigingslandschap. De werkpakketten, templates en formats die gedurende het programma zijn ontwikkeld en aangescherpt, worden beheerd en ontsloten via het SEC. De jaarlijkse zelfevaluatiecyclus, gebaseerd op hetzelfde instrument als de nulmeting, wordt na afloop van het programma voortgezet als regulier onderdeel van de governance van elke deelnemende instelling.

5 Financiële impact van het programma

Dit hoofdstuk beschrijft uitsluitend de financiële impact van het gezamenlijke programma. Voor de financiële impact die samenhangt met de interne implementatie van de Cbw-zorgplicht binnen instellingen wordt verwezen naar de notitie Impact en visie Cbw – CIO-raad (v1.0), waarin deze impact al is onderbouwd en gekwantificeerd.

5.1 Financiële impact voor instellingen (interne implementatie)

De grootste financiële inspanning ligt niet in dit programma, maar binnen de instellingen zelf. Het structureel invulling geven aan de zorgplicht en het realiseren van een werkend ISMS vraagt om investeringen in mensen, processen, techniek en governance. Deze impact is eerder uitgewerkt in de notitie *Impact en visie Cbw – CIO-raad (v1.0)*. Dit programma verandert die impact niet, maar helpt instellingen om deze inspanning efficiënter, meer uniform en met minder dubbel werk te organiseren.

5.2 Financiële impact van het gezamenlijke programma

Deze paragraaf is in versie ‘20260821 v1.1 sec’ bewust leeg gelaten.

5.3 Synergie- en schaalvoordelen

Het gezamenlijk optrekken binnen dit programma levert aantoonbare synergie- en schaalvoordelen op. Door het gezamenlijk ontwikkelen van werkwijzen, formats, handreikingen en werkpakketten:

- wordt dubbel werk binnen instellingen voorkomen;
- wordt kennis sneller gedeeld en toegepast;
- ontstaat een grotendeels uniforme aanpak binnen de sector (80/20-principe);
- kunnen instellingen aanzienlijk efficiënter invulling geven aan hun wettelijke verplichtingen dan wanneer iedere instelling dit afzonderlijk zou organiseren.

De relatief beperkte investering in het programma maakt het mogelijk om de veel grotere interne inspanningen binnen instellingen effectiever en doelmatiger te laten verlopen.

Bijlage 1 Wettelijk kader en referentiekaders

1.1 De NIS2-richtlijn in het kort

De NIS2-richtlijn is Europese wetgeving gericht op het verhogen van de cyberweerbaarheid van essentiële en belangrijke entiteiten. Lidstaten zijn verplicht deze richtlijn om te zetten in nationale wetgeving. Voor Nederland gebeurt dit via de Cyberbeveiligingswet.

NIS2 introduceert onder andere:

- Zorgplicht voor cyberbeveiliging
- Meldplicht voor incidenten
- Bestuurlijke verantwoordelijkheid
- Toezicht en handhaving

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555

1.2 De Cyberbeveiligingswet (Cbw)

De Cyberbeveiligingswet wijst organisaties aan die onder deze verplichtingen vallen. Voor HO/WO-instellingen betekent dit concreet:

- Registratie in het entiteitenregister
- Inrichten van meldprocessen
- Aantoonbaar invulling geven aan de zorgplicht

https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel:36764

1.3 Het Cyberbeveiligingsbesluit (Cbb)

Het Cyberbeveiligingsbesluit werkt de zorgplicht inhoudelijk uit. Hierin staat welke onderwerpen organisaties aantoonbaar moeten beheersen, zoals risicomanagement, incidentrespons, continuïteit en leveranciersbeheer.

https://open.overheid.nl/documenten/6c1cf40d-8b3a-42f6-bd6f-db522cba1046/file

1.4 Waarom de CIS Controls voor maatregelen

Voor HO/WO-instellingen zijn de CIS Controls een praktische en toepasbare operationele set aan maatregelen.

https://learn.cisecurity.org/cis-controls-poster-v8-1

Daarom:

- CIS Controls → concrete maatregelen
- ISO/IEC 27001 → bestuurlijke borging (ISMS)
- ISO/IEC 27002 → richtlijnen voor implementatie

Deze combinatie zorgt voor een werkbare én toetsbare inrichting van de zorgplicht gebaseerd op internationaal erkende standaarden, normen en kaders.