CIIO De certificeerder voor de professionele dienstverlening

Digitale inloopsessie ISO 27001:2022 Transitie

De certificeerder voor de professionele dienstverlening

Huishoudelijke mededelingen

- De sessie wordt opgenomen (als bewijs voor de RvA,): Svp aangeven indien bezwaar tegen opnames
- Microfoon op mute
- Vragen stellen door virtueel handje op te steken (maar even roepen mag ook :))
- Presentatie wordt gedeeld en mag verspreid worden

CIIO De certificeerder voor de professionele dienstverlening

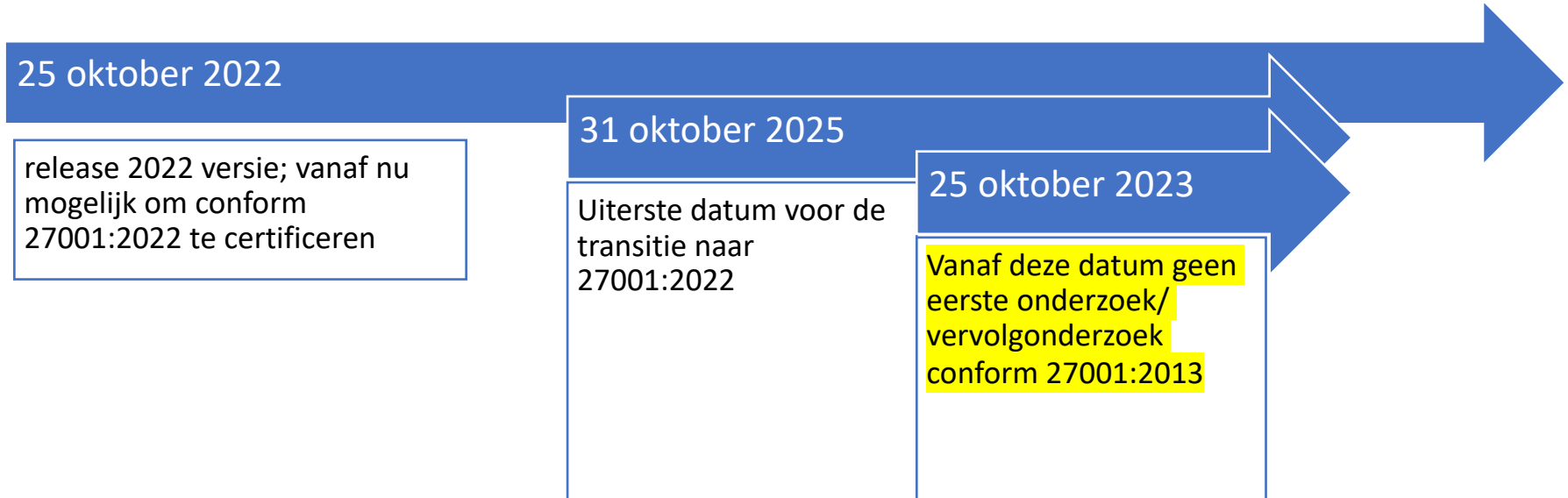
Inhoud

Deel I: Introductie transitie *)
Deel II: Wat te verwachten en een aantal best practices
Deel III: Deep dive op de nieuwe beheersmaatregelen

*) er wordt in dit kader over zowel transitie als overgang gesproken. Beide termen hebben dezelfde betekenis

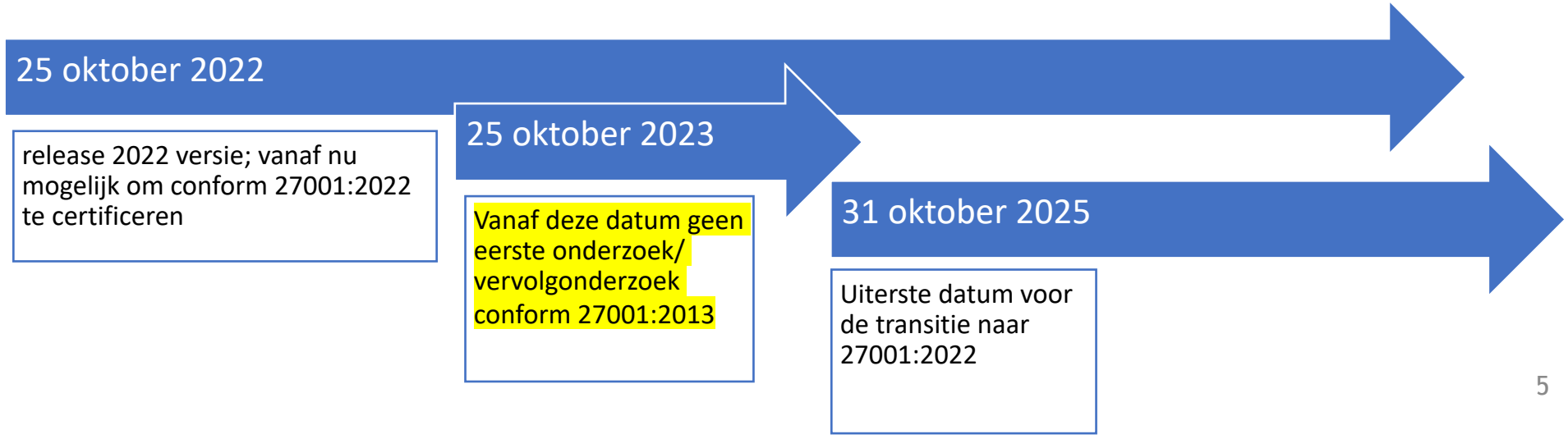
Deel I: Introductie transitie

- In 2022 zijn de 2700**2**:2022 en 2700**1**:2022 gepubliceerd (NL en Engelse versie).
- CIIO is per 1 februari 2023 geaccrediteerd door de Raad voor Accreditatie voor ISO 27001:2022.
- De in de ISO 27001:2022 doorgevoerde aanpassingen zullen door de NEN ook moeten worden doorgevoerd in NEN 7510; nog onbekend is wanneer dit gereed is, maar de verwachting is dat dat in **2024** zal zijn.
- Transitie-periode voor de klant is **maximaal** 3 jaar na publicatie van de nieuwe ISO 27001:2022 (zie ook volgende slide voor details!)
- De transitie is **verplicht**. Indien 3 jaar na publicatie van NL 27001:2022 het ISMS niet voldoet aan de ISO 27001:2022, wordt het certificaat geschorst hetgeen inhoudt dat de klant niet meer is gecertificeerd voor ISO 27001.



Deel I: Introductie transitie

- Transitie-periode voor de klant is **maximaal** 3 jaar na publicatie van de nieuwe ISO 27001:2022
- **MAAR**: momenteel onduidelijkheid vanwege verschil in de transitie regels voor certificerende instellingen - IAF MD 26:2022 - en de online Rva informatie omtrent de transitie.
- Discussiepunt betreft tot aan welke datum een vervolgonderzoek (VO / hercertificering) mag worden uitgevoerd volgens de OUDE norm (ISO 27001:2013).
- IAF : tot 25 oktober 2025
  RvA: tot 25 oktober 2023
- Uitspraak in Q1 2023 verwacht; voor nu gaan we uit van "worst case scenario", dus geen VO na 25 oktober 2023



Deel II:
Wat te verwachten en een aantal best practices

- In overleg met CIIO (de Teamleider) wordt de transitie-periode afgestemd en het transitie onderzoek ingepland;
- Er is minimaal 0,5 dag extra tijdsbesteding nodig voor het transitie onderzoek (verplichting vanuit de RvA/ IAF MD 26:2022). De Teamleider bepaalt de daadwerkelijk benodigde extra tijdsbesteding;
- De transitie kan tijdens een regulier gepland onderzoek worden uitgevoerd.
- Op verzoek van de klant kan ook een Speciaal Onderzoek worden uitgevoerd.
- Het transitie onderzoek mag eventueel remote uitgevoerd worden. De Teamleider bepaalt per geval of dat daadwerkelijk mogelijk is.
- ISO 27001:2013 Certificaten die vanaf nu worden uitgegeven, zijn MAXIMAAL geldig tot 25 oktober 2025.

Impact voor certificaathouders NEN 7510

- Voor klanten met **alleen** NEN 7510 is de impact van de ISO 27001:2022 publicatie nihil; deze klanten blijven conform de huidig geldende NEN 7510 norm beoordeeld worden, totdat de nieuwe NEN norm gepubliceerd wordt. Naar verwachting geldt ook dan een overgangstermijn van 3 jaar.
- Met klanten die voor zowel NEN 7510 als ISO 27001 gecertificeerd zijn, zal CIIO in overleg treden om de mogelijkheden door te bespreken;

Onderwerpen transitie-onderzoek

Bron/ eisen: IAF MD 26:2022 :

De volgende onderwerpen zullen (minimaal) aan de orde komen tijdens het transitie onderzoek:

Het transitie onderzoek omvat, maar is niet beperkt tot:

- *de gap-analyse van ISO/IEC 27001:2022, evenals de noodzaak van wijzigingen in het ISMS van de klant;*
- *het actualiseren van de Verklaring van Toepasselijkheid (VvT);*
- *indien van toepassing, het actualiseren van het risicobehandelplan;*
- *de implementatie en effectiviteit van de nieuwe of gewijzigde controles gekozen door de klant.*

Actielijstje overgang ISO 27001:2022 voor gecertificeerde organisaties

Voorafgaande aan het overgangsonderzoek:

- Voer een gap analyse uit op ISO 27001:2013 en ISO 27001:2022; grootste verschil zit 'm in de Annex A; Let daarbij (ook) op de in ISO 27001:2022 Annex A samengevoegde beheersmaatregelen. Het kan voorkomen dat daarin ISO 27001:2013 Annex A beheersmaatregelen zijn samengevoegd waarvan 1 of meerdere wel, en 1 of meerdere niet in scope waren;
- Kijk of er behoefte is aan extra training, bijvoorbeeld voor de interne auditors;
- Voer opnieuw (aantoonbaar) 6.1.3.c uit: vergelijk de vastgestelde beheersmaatregelen uit het risico behandelplan met (de nieuwe ISO 27001:2022!!) Annex A om te verifiëren dat alle noodzakelijke beheersmaatregelen zijn geïmplementeerd;
- Zijn er nieuwe beheersmaatregelen vastgesteld: doe de risicoanalyse opnieuw en herijk je risico-behandelplan;
- Indien van toepassing: implementatie van nieuwe of gewijzigde beheersmaatregelen;
- Herzie de Verklaring van Toepasselijkheid;
- Voor dit alles heeft de klant maximaal 3 jaar de tijd na publicatie van de ISO 27001:2022 norm (zie slide 5 voor de discussie omtrent de uiterste datum van de VO)
- Tip: Maakt de organisatie gebruik van een ISMS tool: Vergeet de leveranciers van het ISMS tool niet te vragen wanneer de tool ISO 27001:2022 proof wordt
- Tip 2: Hou de certificaten van je eigen leveranciers extra in de gaten de komende jaren; na 25 oktober 2025 voldoet een ISO 27001:2013 gecertificeerde organisatie NIET meer en wordt dan als NIET gecertificeerd beschouwd

Best practices

- ISO 27002 Information Security Controls Gap Analysis Tool (bij gebrek aan beter…)
- Mogelijke verdeling / clustering van ISO 27001:2022 beheersmaatregelen voor de interne audit

CIIO De certificeerder voor de professionele dienstverlening

So far so good?

Deel III: De verschillen

Belangrijkste wijzigingen ISO 27001:2022:

- Aantal wijzigingen/ aanvullingen in H4 – H10 (zie **bijlage A** – Verschillen H4 – H10); geen wijzigingen met grote impact
- GEEN verplichte documentatie meer vanuit de Annex A
- Annex A verschillen: zie de tabellen in de norm
- Andere volgorde en indeling van beheersmaatregelen in de Annex A;
- Van indeling naar onderwerp (bijvoorbeeld A.9 – Logische Toegang en A.17 – beschikbaarheid) naar indeling naar 4 categorieën –processen/ organisatie, mensen, technologie en fysieke beveiliging;
- In vergelijking met de oude editie neemt het aantal maatregelen in de Annex A van ISO/IEC 27002:2022 af van 114 maatregelen in 14 clusters naar 93 maatregelen in 4 clusters (categorieën);
- Samengevoegde maatregelen: zie bijlage B van deze presentatie.
  Let bij het samenvoegen op de wel/ niet in scope beheersmaatregelen
- Nieuwe beheersmaatregelen: zie bijlage B van deze presentatie.

Bijlage A - Verschillen in H4 - H10

De verschillen – de belangrijkste op een rijtje (wijzingen met impact

- ISO/IEC 27001:2022
  Information security, cybersecurity and privacy protection — Information security management systems — Require

Impact: Geen

De verschillen - Titel van de norm

- ISO/IEC 27001:2013
  Information technology —Security techniques —Information security management systems — Requirements

- ISO/IEC 27001:2022
  Information security, cybersecurity and privacy protection — Information security management systems — Require

Impact: Geen

De verschillen - 4.2

- ISO/IEC 27001:2013

4.2 Understanding the needs and expectations of interested parties

- The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

- ISO/IEC 27001:2022

4.2 Understanding the needs and expectations of interested parties

- The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

Impact: Beperkt. Je zou bijvoorbeeld ook kunnen aangeven welke requirements er NIET worden afgedekt

De verschillen - 4.4

- ISO/IEC 27001:2013

4.4 Information security management system

- The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

- ISO/IEC 27001:2022

4.4 Information security management system

- The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

Impact: Geen. Met de aanvulling wordt het belang van het hebben en onderhouden van processen benadrukt.

De verschillen - 6.1.3.c

- ISO/IEC 27001:2013

6.1.3.c

Note 1; Annex Contains a comprehensive list of control objectives and controls. Users of this international standard are directed to Annes A to ensure that no necessary controls are overlooked

Note 2; Control Objectives are implicitly in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives ans controls may be needed

- ISO/IEC 27001:2022

6.1.3.c

Note 2: Annex contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked

Note 3: The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

Impact: Geen. In de 2022 versie is het nu duidelijker gemaakt dat Annex A niet een lijst met verplichte maatregelen betreft, maar gebruikt moet worden om te verifiëren dat er geen maatregelen zijn vergeten nadat de maatregelen die uit de risicoanalyse/ eisen van externe stakeholders zijn gekomen.

De verschillen – 6.2

- ISO/IEC 27001:2013

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

- ISO/IEC 27001:2022

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

Impact: Geen. Met de aanvulling wordt het belang van het monitoren en vastleggen van security doelstellingen benadrukt. Dit punt wordt afgedekt vanuit de directiebeoordeling waarbij o.a. aantoonbaar moet worden gereflecteerd op het voldoen aan de IB doelstellingen.

De verschillen 6.3 (nieuw)

- ISO/IEC 27001:2013
  -

- ISO/IEC 27001:2022
  6.3 Planning of changes
- When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

Impact: Beperkt. Dit gaat over het beheerst doorvoeren van wijzigingen aan het ISMS.

CIIO De certificeerder voor de professionele dienstverlening

De verschillen - 8.1

- ISO/IEC 27001:2013

8.1 Operational planning and control The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.
The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
The organization shall ensure that outsourced processes are determined and controlled.

- ISO/IEC 27001:2022

8.1 Operational planning and control
The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:
— establishing criteria for the processes;
— implementing control of the processes in accordance with the criteria.
Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.
The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

Impact: Beperkt. Het stellen van eisen aan processen kan bv met behulp van Key performance Indicatoren (KPI – hiermee kijk je terug, de waarde zegt iets over de kwaliteit van het beheersmaatregelen) of Key Risico Indicatoren (dit heeft een "voorspellende waarde"). Voorbeeld KPI: alle prio 1 incidenten worden geëvalueerd. Voorbeeld KRI: % stijging van het aantal prio 1 incidenten in periode X.

De verschillen – 9.1

- ISO/IEC 27001:2013

9.1 Monitoring, measurement, analysis and evaluation

…

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

- ISO/IEC 27001:2022

9.1 Monitoring, measurement, analysis and evaluation

…

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

Impact: Beperkt. Als het goed is, is er een overzicht van alle activiteiten/ metingen die je uitvoert om de prestaties en doeltreffendheid van het ISMS te evalueren. Denk aan bijvoorbeeld een operationele planning waarin je gedurende het jaar activiteiten hebt gepland zoals restore test, periodieke review autorisaties etc. Door op de resultaten van deze monitoring te reflecteren, wordt de cyclus “afgesloten”.

De verschillen – 9.2 en 9.3 (structuur)

- ISO/IEC 27001:2013

9.2 Internal audit
9.3 Management review

- ISO/IEC 27001:2022

9.2 Internal audit
9.2.1 General
9.2.2 Internal audit programme
9.3 Management review
9.3.1 General
9.3.2 Management review inputs
9.3.3 Management review results

+new input for Management review:
c) changes in needs and expectations of interested parties that are relevant to the information security management system

Impact: Beperkt. Mbt de nieuwe input voor de management review, zou je deze eis expliciet kunnen toevoegen aan het template van de directiebeoordeling. In wezen wordt aan deze eis voldaan met het uitvoeren van de (jaarlijkse) review op de context en stakeholders. De uitkomst van de review, met eventuele wijzigingen die daaruit naar voren komen, moeten expliciet in de directiebeoordeling vermeld worden.

De verschillen – 10 (structuur)

- ISO/IEC 27001:2013

10.1 Nonconformity and corrective action
10.2 Continual improvement

- ISO/IEC 27001:2022

10.1 Continual improvement
10.2 Nonconformity and corrective action

Impact: Geen. Het betreft geen nieuwe eisen maar een herstructurering van bestaande eisen.

Bijlage B – Nieuwe beheersmaatregelen in Annex A

Verschillen - samengevoegde maatregelen

Samengevoegde beheersmaatregelen ;

Compactere en (soms) meer logische indeling (bijvoorbeeld de samenvoeging van de in 2013 versie verspreide onderdelen op change management/ wijzigingsbeheer in beheersmaatregel - 8.32

ISO/IEC 27002 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and associated assets
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.31	18.1.1, 18.1.5	Identification of legal, statutory, regulatory and contractual requirements
5.36	18.2.2, 18.2.3	Compliance with policies and standards for information security
6.8	16.1.2, 16.1.3	Information security event reporting
7.2	11.1.2, 11.1.6	Physical entry controls
7.10	08.3.1, 08.3.2, 08.3.3	Storage media
8.1	06.2.1, 11.2.8	User endpoint devices
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.24	10.1.1, 10.1.2	Use of cryptography
8.26	14.1.2, 14.1.3	Application security requirements
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management

Verschillen - nieuwe maatregelen

Nieuwe beheersmaatregelen in de Annex A

ISO/IEC 27002 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.7	New	Threat intelligence
5.23	New	Information security for use of cloud services
5.30	New	ICT readiness for business continuity
7.4	New	Physical security monitoring
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.16	New	Monitoring activities
8.23	New	Web filtering
8.28	New	Secure coding

A.5.7 Threat intelligence (informatie en analyse over dreigingen)

Beheersmaatregel: Informatie met betrekking tot IB-dreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren

* Definitie Gartner: *Threat intelligence is het verzamelen van informatie en deze te ordenen en te analyseren om trends te identificeren (sectoren die vaak doelwit zijn, gebruikte middelen en methodes, enz.). Deze profilering maakt het mogelijk om het beveiligingsbeleid te optimaliseren om beter te kunnen anticiperen op verschillende incidenten*

Deze controle vereist dat u informatie over bedreigingen verzamelt en deze analyseert, zodat u de juiste mitigerende maatregelen kunt nemen. Deze informatie kan gaan over bepaalde aanvallen, over methoden en technologieën die de aanvallers gebruiken en/of over aanvalstrends. U dient deze informatie intern te verzamelen, maar ook uit externe bronnen zoals leveranciersrapporten, aankondigingen van overheidsinstanties, enz.

Best practices

1. “threats bibliotheek”: BSI **IT-Grundschutz Catalogues**https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf?__blob=publicationFile&v=4
   NADEEL: Geen SDLC aspecten
2. Website NCSC

5.23 – Information security for use of cloud services (informatiebeveiliging voor het gebruik van clouddiensten)

Beheersmaatregel: Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de IB eisen van de organisatie te worden opgesteld.

Essentie: dit is een verdieping op de reeds “bekende” beheersmaatregelen uit (voorheen) A.15 die nu in 5.19 tm 5.22 staan. **Belangrijke toevoeging in ISO 27002 in beheersmaatregel 5.23: Exit strategy**

A.15 controls - 2013 version

New in 2022 version

5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services

5.23 – Information security for use of cloud services - vervolg

Voorbeeldvragen m.b.t. de exit strategy:

- Is de mate van afhankelijkheid met de leverancier vastgesteld / is er een risico analyse gemaakt voordat je met deze leverancier in zee ging
- Als er een grote afhankelijkheid is, is er dan nagedacht over alternatieven en hoe snel is het mogelijk over te stappen naar een alternatief?
- Zijn er afspraken gemaakt over de exit, bijvoorbeeld overdracht van data (hoe lang hebben we daarvoor, in welk formaat krijgen we die data, ook de backups etc); houd rekening met de retentie van de data, ook die van de verwerker. Bijvoorbeeld in geval van wettelijke termijn van van bv financiële gegevens.
- Voor een belangrijk deel al afgedekt met een verwerkersovereenkomst.
- Zie ook onderdeel 5.30 m.b.t. het afsluiten van een Escrow met een Cloud leverancier.

5.30 – ICT Readiness for business continuity (ICT gereedheid voor bedrijfscontinuiteit)

Beheersmaatregel: De ICT-gereedheid beheert te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen

Essentie: In de ISO 27001:2013 – onderdeel A.17 – lag de nadruk op de continuïteit van IB tijdens een calamiteit en was er een beheersmaatregel opgenomen over redundantie. In de nieuwe norm is de relatie tussen ICT beschikbaar en continuïteit van de bedrijfsprocessen explicieter gemaakt.

Overwegingen:

- Business stelt vast wat de kritieke activiteiten zijn, wat daarvan de maximale uitval is (in uren/ dagen), en welke afhankelijkheid bestaat met middelen waaronder ICT. Dit kan bv op basis van bijvoorbeeld een Business Impact Analyse of een Analyse Kritieke Activiteiten.
- Voor de ICT middelen wordt de Recovery Time Objective (RTO) en Recovery Point Objective (RPO) vastgesteld
- Vervolgens vaststellen of de ICT middelen hieraan kunnen voldoen; in geval ICT (deels) is uitbesteed moet de RTO/ RPO overeengekomen/ vastgelegd worden met de leverancier(s)

7.4 – Physical Security Monitoring (monitoren van fysieke beveiliging)

Beheersmaatregel: Het gebouw en terrein behoort voortdurend te worden gemonitoord op onbevoegde fysieke toegang.

Dit is, naar de mening van CIIO, niet heel veel anders dan wat al vanuit ISO 27001:2013, onderdeel A.11 werd gevraagd: Afhankelijk van uw risico's moet u mogelijk alarmsystemen of videobewaking implementeren; je zou ook kunnen besluiten om een niet-technische oplossing te implementeren, zoals een persoon die het gebied observeert (bijvoorbeeld een bewaker).

Overwegingen:
- Procedures voor het opvragen van camerabeelden
- Bewaartermijnen camerabeelden
- Toegang tot bedieningspaneel alarm
- Wijzigingsprocedure alarmcodes, eventueel irt IDU proces
- Houden procedures rekening met stroomuitval?
- Batterijen van druppel-lezers?
- Als Domotica wordt gebruikt ihkv physical security – borgen van IB: vulnerability en change management van (beveiligings)apparatuur, opgenomen in gesegregeerd netwerk? En opnemen in je CMDB (zie volgende slide)

CIIO De certificeerder voor de professionele dienstverlening

8.9 – Configuration Management (configuratiebeheer)

Beheersmaatregel: Configuraties, **met inbegrip van beveiligingsconfiguraties** van hardware, software, diensten en netwerken behoren te worden vastgelegd, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.

Lijkt heel erg op ISO 27001:2013, onderdeel A.8.1.1 (inventarisatie van bedrijfsmiddelen), maar nu wordt “security configurations” expliciet benoemd

Essentie: het beheren van “security gerelateerde systeeminstellingen” of de “security baseline” van IT componenten (firewalls, servers etc). Hiervoor worden vanuit de leverancier meestal best practices aangeleverd.

Ook zijn er onafhankelijke/ commerciële best practices zoals de CIS (Center for Information Security) Benchmarks. CIS levert ook tooling voor monitoring op afwijkingen van de baseline.

Overwegingen:

- I.r.t. Change Management – regressietesten op de security baseline na een (grote) wijziging (niet per ongeluk terug naar(onveilige) fabrieksinstellingen?)
- Procedures rondom known errors met betrekking tot fabrieks-instellingen (google it!) – bekend voorbeeld uit de pre-historie is SCADA
- Is het (monitoren op) aanpassen van de geïmplementeerde baseline geborgd (kan terugkomen in onderdeel “monitoring handeling van admins”)
- Procedure om bewust af te wijken van de baseline – mitigerende maatregel (bv: netwerksegmentatie,…)

8.10 – Information deletion (wissen van informatie)

Beheersmaatregel: In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer nodig is

In essentie: het veilig verwijderen van gegevens na het verlopen van de (wettelijke) MAXIMALE bewaartermijn. Bekendste voorbeeld: CV's

Overwegingen;

- Methode voor data deletion getest? - hoe weet je zeker dat de gegevens niet teruggehaald worden
- Hoe borg je dat een restore van een database niet leidt tot het (onbedoeld) terugzetten van verwijderde records
- Data kwaliteit: indien er meerdere registraties zijn waarin data wordt opgeslagen, welke registratie is dan leidend voor het bepalen van de retentie-termijn en hoe houd je de registraties synchroon (data/informatie management)
- In geval er gebruikt gemaakt wordt van batch jobs voor het automatisch opruimen van data na het verstrijken van de maximale bewaartermijn, controleer je dan regelmatig de werking van deze batchjobs (change management op de batchjobs ingericht?)
- Verzoek van belanghebbende voor het verwijderen van data: is er een proces ingericht voor controleren van identiteit van de aanvrager? Wie geeft toestemming/ wie voert legal toets uit? Hoe weet je in welke registraties de belanghebbende eventueel nog meer voorkomt (toch handig, zo'n verwerkingsregister ☺) ?
- Als sharepoints in projectverband gebruikt worden: procedure voor toegang (ook van buitenaf?) op die Sharepoints en het (tijdig) opruimen van die Sharepoints nadat het project afgerond is (vaak bij organisatie advies bureaus een "hardnekkig probleem")
- Denk ook aan omgevingen als Outlook, Bureaublad, Downloadmap, waar in prullenbakken informatie van jaren terug kan zijn opgeslagen

8.11 – Data masking (maskeren van gegevens)

Beheersmaatregel: Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.

Essentie volgens 27002: het toepassen van technieken zoals pseudonimiseren en anonimiseren van persoonsgerelateerde gegevens om de identiteit van belanghebbenden te beschermen.

Maskeren kan ook door (delen van) informatie af te schermen voor niet geautoriseerde gebruikers.

Overwegingen:

- Welke stappen worden doorlopen bij het pseudonimiseren en anonimiseren van gegevens? Volg de hele “keten” van origineel naar eindresultaat. Worden in dat proces kopieën van het origineel gemaakt als tussenstap in het anonimiseren; waar blijven die kopieën dan? Prullenmand / download map ook leeg?
- I.g.v. pseudonimisatie; processen rondom het beheer van het “sleutelbestand”

CIIO De certificeerder voor de professionele dienstverlening

8.12 – Data Leakage Prevention (voorkomen van gegevenslekken)

Beheersmaatregel: Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.

Essentie: Weet je waar welke data staat met welke classificatie, wie weet je wie daar toegang toe heeft en via welke route(s) vertrouwelijke data gedeeld kan worden?

Overwegingen:

- Preventief: het beheersen van het maken van downloads/ kopieën van/uit databases (worden bijvoorbeeld Power BI Tools gebruikt?)
- Detectief: monitoren van datastromen (bv geen bijlages in mail toestaan zonder “extra laag van security”, scannen op bv BSN nummer)
- Indien platform voor data-uitwisseling wordt gebruikt zoals cryptshare o.i.d.: vergeet niet het beheer van dat platform veilig in te richten/ uit te voeren (logische toegang etc)
- In Azure mooie “standaard” oplossingen beschikbaar. Toetsvraag : change management rondom de inrichting daarvan.

8.16 – Monitoring activities (monitoren van activiteiten)

Beheersmaatregel: Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële IB incidenten te evalueren.

Lijkt heel erg op A.12.4.1 (gebeurtenissen registreren) uit ISO 27001:2013, alleen is het inrichten van de logfiles (8.15) en het daadwerkelijk bekijken/ analyseren van de logging nu los van elkaar in een maatregel opgenomen.

8.23 – Web filtering (toepassen van webfilters)

Beheersmaatregel: De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken

Essentie: toegang tot onbetrouwbare websites voor medewerkers (gedeeltelijk) blokkeren/ beheersen.

8.28 – Secure Coding (veilig coderen)

Beheersmaatregel: Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.

In ISO 27001:2013 versie was A.14.1.1 “Beleid voor veilig ontwikkelen” erg globaal; nu is de (aandacht voor) IB tijdens het ontwikkelen van code explicieter gemaakt in de norm.
Bij CIIO onderzoeken gingen we al in op secure coding.