Cybersecurity

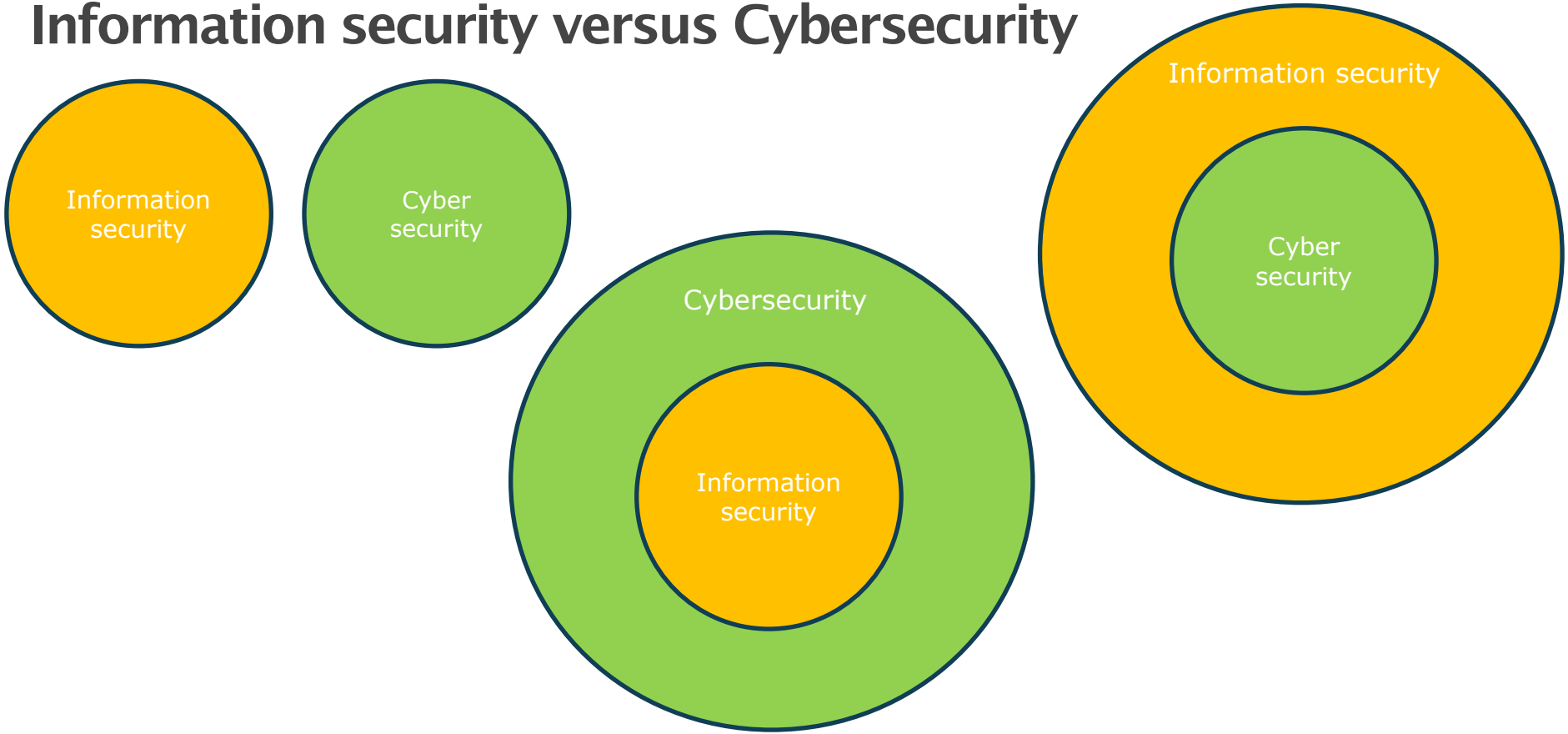
In een Europees speelveld

23 september 2024

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Cybersecurity?

Information security versus Cybersecurity



Definities

- **Information security** [ISO 27000:2020]

  reservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information.

  – *Note 1 to entry: In addition, other properties, such as authenticity (3.6), accountability, non-repudiation (3.48), and reliability (3.55) can also be involved.*

- **Cybersecurity** [# ISO 27000! → ISO/IEC TS 27100:2020 Cybersecurity — Overview and concepts]

  The objective of adequate cybersecurity is to maintain an acceptable level of stability, continuity and safety of entities operating in cyberspace.

  – *Areas of concern for cybersecurity include:*

    a) stability and continuity of society, organizations and nations;

    b) property (including information) of people and organizations; and

    c) human lives and health.

Wat betreft “Safety”?

- ISO/IEC Guide 51:2014(en) Safety **aspects** — Guidelines for their inclusion in standards
  - Safety = freedom from risk (3.9) which is not tolerable
  - Tolerable risk – level of risk (3.9) that is accepted in a given context based on the current values of society
  - (3.9) Risk – combination of the probability of occurrence of **harm** (3.1) and the severity of that **harm**

En wat zegt de cybersecurity regelgeving?

- REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA …. and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – Article 2 (a)

  ‘cybersecurity’ means the activities necessary to protect network and information systems, *the users* of such systems, *and other persons* affected by *cyber threats*;

Eenduidig

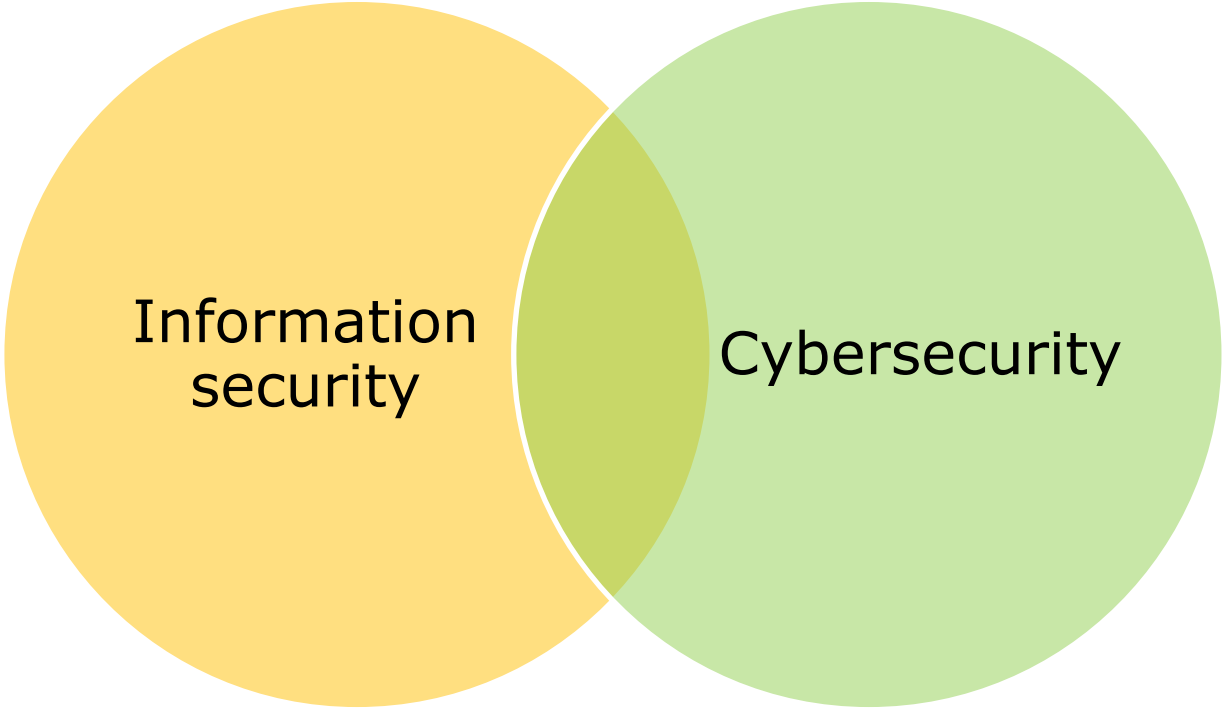
- NIS2
- CER
- AI Act
- eIDAS (update)
- DORA
- Machine Directive
- CRA (Cyber Resilience Act)
- Cyber Solidarity Act
- ….

Relatie informatiebeveiliging en cybersecurity?

- ISO/IEC TS 27100:2020 Cybersecurity — Overview and concepts
  - Breach of information security in cyberspace can cause a cybersecurity incident. This means that the information security risks are viewed as **cyber risks** in the context of cybersecurity.
  - Relationship:
    - Cyberspace as a field of risk sources for an ISMS;
    - ISMS in support of cybersecurity;
    - Cybersecurity framework (ISO 27110);
    - Cybersecurity and safety;
    - Cyber insurance.
- Cybersecurity framework development guidelines (ISO/IEC TS 27110:2021,IDT)

  Annex A (informative) Considerations in the creation of a cybersecurity framework

Cybersecurity



Cybersecurity als maatregel

Cybersecurity framework

- ISO/IEC TR 27103:2018(E) Security techniques — Cybersecurity and ISO and IEC Standards

  functions, or high-level descriptions of desired outcomes, which are concurrent and continuous

  - *Identify;*
  - *Protect;*
  - *Detect;*
  - *Respond;*
  - *Recover.*
- NIST : Framework for Improving Critical Infrastructure Cybersecurity (version 1.1)
  - *Identify;*
  - *Protect;*
  - *Detect;*
  - *Respond;*
  - *Recover.*

Developments

- The NIST Cybersecurity Framework (CSF) 2.0 [26 February 2024]
  - *Govern: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.*
  - *Identify: The organization's current cybersecurity risks are understood.*
  - *Protect: Safeguards to manage the organization's cybersecurity risks are used.*
  - *Detect: Possible cybersecurity attacks and compromises are found and analyzed.*
  - *Respond: Actions regarding a detected cybersecurity incident are taken.*
  - *Recover: Assets and operations affected by a cybersecurity incident are restored.*

Remark: Where is risk management?

Developments

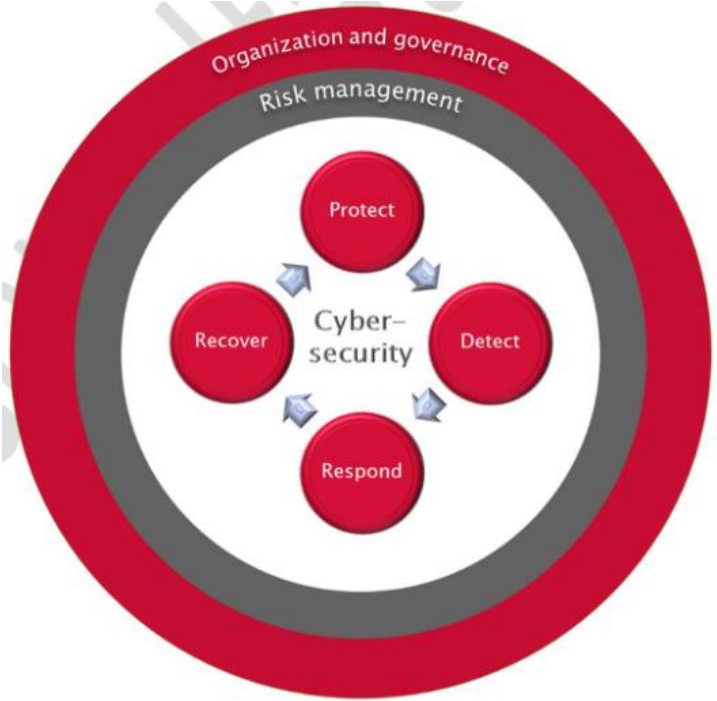
- The NIST Cybersecurity Framework (CSF) 2.0 [26 February 2024]
  - *Govern: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored*
  - *Identify: The organization's current cybersecurity risks are understood.*
  - *Protect: Safeguards to manage the organization's cybersecurity risks are used.*
  - *Detect: Possible cybersecurity attacks and compromises are found and analyzed.*
  - *Respond: Actions regarding a detected cybersecurity incident are taken.*
  - *Recover: Assets and operations affected by a cybersecurity incident are restored.*

NOREA Cybersecurity Assessment

Update vragenlijst en handreiking:

1. De vragen zijn aangepast zowel voor de ICR (bepaling impact) als de CSA (bepaling beheersing).
2. De Excel tool bevat nu 7 standaarden zoals ISO27002, NIST CSF, Cobit en DNB GP IB. Diverse standaarden zijn bijgewerkt naar de nieuwste versie, oude en niet meer relevante standaarden zijn verwijderd.
3. Het toevoegen van een dashboard in de spreadsheet:
4. Diverse berekeningen voor het bepalen van de scores.

NOREA Reporting Initiative - NRI



Impact

Uitdagingen in het managen van cybersecurity

- Scope bepaling
  - Nieuwe assets of andere weging mate van kritiek zijn;
  - Beperking tot “cyberspace” of uitbreiding met “cyberspace”;
  - Interactie met andere organisaties in de keten.
- Nieuwe kwaliteitscriteria?:
  - Safety component in “Cybersecurity” = information security met een plus;
  - Ander beeld voor “continuïteit”?
- Geeft nieuwe perspectieven op risico’s die een plaats moeten krijgen in risicomanagement!
  - Cyber risks # cybersecurity risks;
  - Focus op impact op personen, organisaties en/of landen, maar tot hoever? ;
  - Welke bedreigingen en kwetsbaarheden waarvoor nieuwe of aanvullende maatregelen;
  - Aanpassen en/of aanvullen op ISMS of een Cybersecurity management systeem?
- Produkten versus diensten? Of diensten versus producten?

Kansen

- Adresseren van cybersecurity:
  - Organisaties meer aandacht voor impact op maatschappij;
  - Cyber Risico's raakt individuen : "meer vertrouwen" als er aandacht voor is en transparantie wordt betracht;
  - Security by design;
  - Onderstrepen van het ketenperspectief;
  - "bridging safety and security".
- Verantwoorden over:
  - Opties voor een meer geïntegreerde benadering van security;
  - Handvat voor horizontale verantwoordingen;
  - Management krijgt meer houvast voor haar governance / risk / compliance taken;
  - Kleinere communicatiekloof tussen maatschappij en organisaties.
- Bevestiging vertrouwen (audit + conformity assessment)

EU regelgeving?

1. Rol van “presumption of compliance” New Legislative Framework (NLF)

- improves market surveillance
- rules to better protect both consumers and professionals from unsafe products, including those imported from outside the EU. In particular, this applies to procedures for products which can pose danger to health or the environment;
- sets clear and transparent rules for the accreditation of conformity assessment bodies;
- boosts the quality of and confidence in the conformity assessment of products through stronger and clearer rules on the requirements for the notification of conformity assessment bodies;
- clarifies the meaning of CE marking and enhances its credibility;
- establishes a common legal framework for industrial products in the form of a toolbox of measures for use in future legislation. This includes definitions of terms commonly used in product legislation, and procedures to allow future sectorial legislation to become more consistent and easier to implement.

https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

1st implementatie : Cybersecurity + NLF!

- Radio Equipment Directive (RED) vraagt om standaarden met requirements
- Standaardisatie verzoek (SR) van EC naar …
- Resultaat:

NEN-EN 18031-1:2024 Common security requirements for radio equipment : delen 1 tot en met 3

Gevolgd door standaarden voor

- Cyber Resilience Act
- AI Act
- Machine directive
- …..

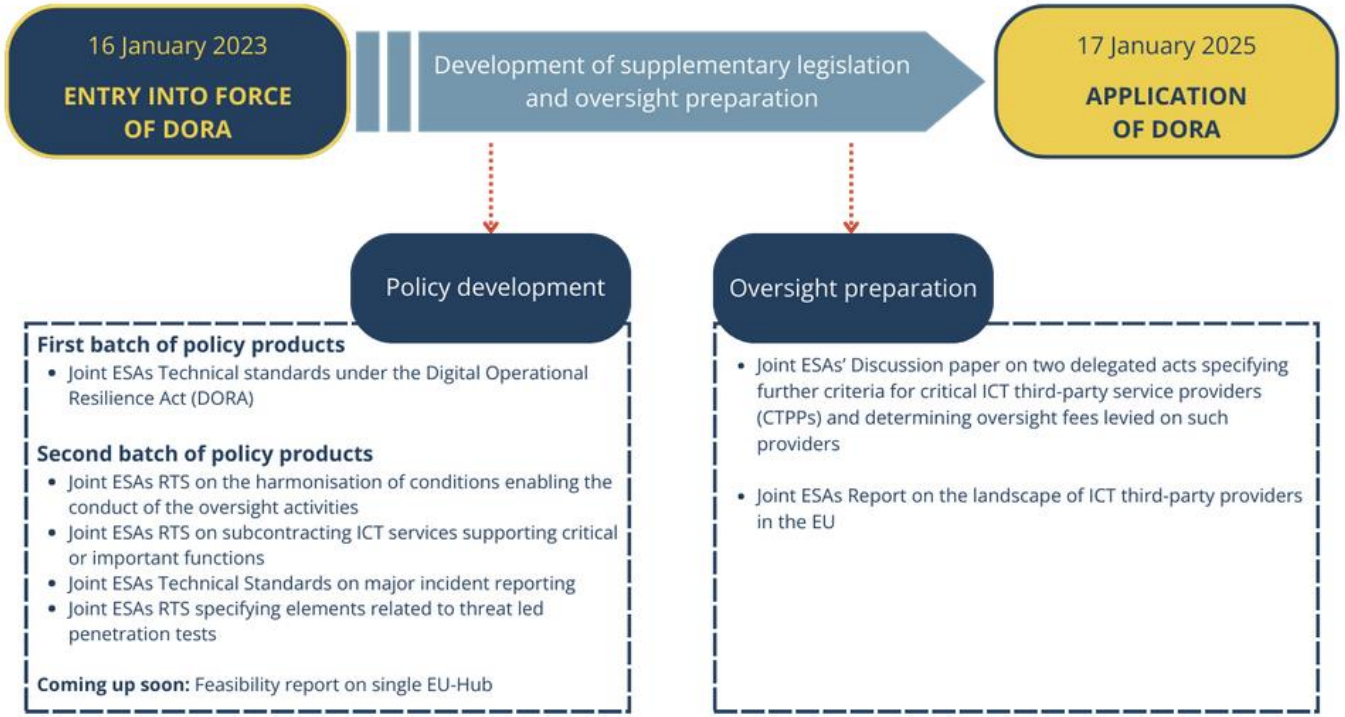
2. Cybersecurity certification framework

- Vastgelegd in de Cybersecurity Act (update is onderhanden) 2019/881
- “Voluntary”
- Maar heeft / krijgt referenties (Machine Directive / Cyber Resilience Act / AI Act / NIS2) voor high risk certificeringsoptie met “presumption of compliance”
- Komt op stoom:
  - EUCC (Common Criteria) [februari 2024 / reeks van standaarden]
  - EUCS (Cloud services) [verwacht Q4 2024 / CEN TS 18027:2024]
  - Onderhanden EU5G (meerdere)
- URWP (Union Rolling Working Plan) geeft plan en prioriteiten
- Update CSA moet proces efficiënter gaan maken
- EUCC momenteel erkent als de “trust” voor “high risk” producten

Highlights Cybersecurity regulatory approach

- Standards!!!!!
- Products versus Services
  - Lifecycle management (intended use)
  - Operating effectiveness
- Risk based
- Issues
  - Incident handling
  - Vulnerability management
  - SBOM (Software Bill of Materials)
  - (Cyber)security by design
  - Reporting / responsibilities / communication with supervisory authorities
  - Competencies and Education
  - Interplay
- ….

3. Supplementary regulation



https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act

Wat zijn hieruit de “take aways”?

Aandacht voor:

- Volg de ontwikkelingen rond (EU) regelgeving!
  - Actuele ontwikkelingen op het terrein van cybersecurity en aanpalende domeinen Jaargang (onder redactie van Rob Bouman) – NOREA Kennisgroep Cybersecurity
  - Wetgevingsoverzicht Online Trust Coalitie (https://onlinetrustcoalitie.nl/publicaties/)
- Volg de standaardisatie!
- Implementatie
  - Vergroot de scope en inhoud van het ISMS met een cybersecurity framework implementatie;
  - Actualiseer de governance en verantwoordingsstructuur;
  - Speciale aandacht voor de (potentiële) impact van cyber risico's binnen risicomanagement;
  - Doorvertalen naar "attack surfaces" en "threats", "vulnerabilities" (attack types).
- Samenwerking en verantwoording
  - Werk aan relatie met toezichthouders;
  - Heb aandacht voor de ketenbenadering en ga samenwerken voor cyberweerbaarheid;
  - Maak Cyberweerbaarheid aantoonbaar.

Bedankt

Voor meer informatie kun je contact opnemen met:

Ruud Kerssens RE RA CISA CRISC

23 september 2024]

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS