Cyberthreats in de boardroom

Een controlekader dat bestuurders begrijpen!

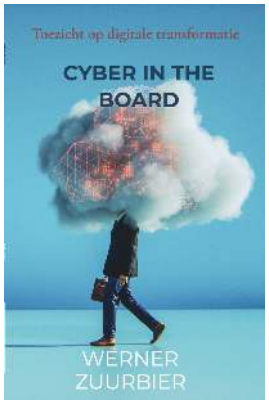
12 November 2025
ISACA Risk event ‘25

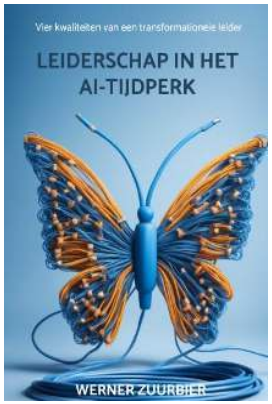
Cenvio

Wie ben ik?

Werner Zuurbier (1971)

- Directeur-bestuurder RSO GERRIT - verbinder van zorg
- Eigenaar Cenvio – advies over digitale transformatie
- Auteur van de boeken “Cyber in the board” en “Leiderschap in het AI-tijdperk”.



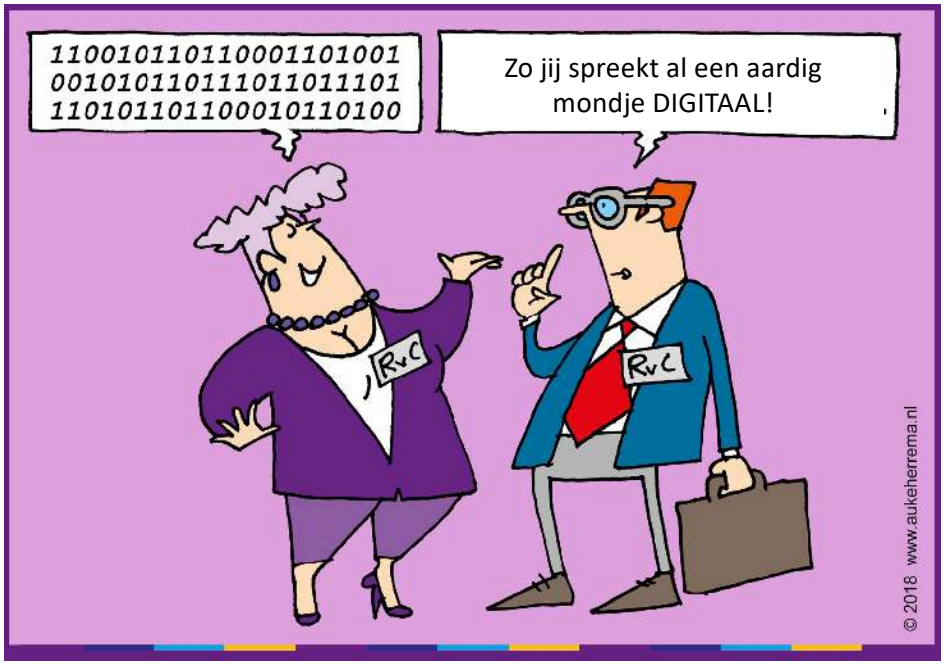


Daarnaast:

- Lid RvC National Academic (verzekeraar Promovendum)
- Lid RvT Huisartsopleiding NL
- Lid RvT Scholen aan Zee

Cenvio

Grote verantwoordelijkheid voor bestuur & toezicht



Persoonlijke aansprakelijkheid rond digitale veiligheid: EU-wetgeving zoals NIS2 of DORA leggen dit expliciet op

- Vertoon voorbeeldgedrag rond bewustzijn risico's
- Bepaal risicobereidheid rond informatiebeveiliging
- Stel security-beleid en jaarplan vast
- Lever voldoende middelen voor risicomitigatie
- Beoordeel rapportages over IT en cybersecurity
- Zie dat leveranciers zich ook houden aan eisen
- Volg trainingen rond digitale veiligheid
- Heb inzicht in actueel dreigingsbeeld
- Check weerbaarheidsscenario's & -plannen
- Doe zelf actief mee aan testen continuïteit

Het (goede?) gesprek over risico's…

• Het risico op een geldboete van de Autoriteit Persoonsgegevens	❌ Dit is een risico-gevolg
• Het risico op een cyberhack	❌ Dit is een risico-oorzaak
• Het risico dat de toegangsbeveiliging niet op orde is	❌ Dit is een niet goed ingerichte beheermaatregel
• Een tekort aan gekwalificeerd security personeel	❌ Dit is een bestaand probleem, geen risico meer
• Het risico op een datalek	✅ Dit is het daadwerkelijke risico

Discussies over onzuivere risico's leiden tot enerzijds blinde vlekken en anderzijds dubbelingen bij het inschatten van de eigen IT-risico's

Cenvio

Stelling

Er zijn 28 inherente technologierisico's.

Niet meer, niet minder…

Cenvio

Technologie Risico Framework

Kans

Dreigingen & Trends

Risico-oorzaak

Interne dreigingen
Vb. menselijke fout, misdragingen door eigen medewerkers, intern of lokaal ongeval, ineffectief leiderschap, technische storing, ziekte, staking

Dreigingen door marktverstoring
Vb. disruptieve tech, industriële spionage en diefstal, moddergooien, overname, faillissement, arbeidsmarktkrapte, economische crisis, lange levertijden toeleveranciers

Dreigingen door natuur & klimaat
Vb. overstroming. storm, brand, pandemie, aardbeving, eruptie, milieuvervuiling

Dreigingen door criminaliteit & terrorisme
Vb. fraude, diefstal, sabotage, aanslag, gijzeling, afpersing, vandalisme

Dreigingen door hackers
Vb. denial of service, account overname, spyware, gegevensmanipulatie

(Geo)politieke dreigingen
Vb. oorlog, statelijke spionage, wet- & regelgeving, activisme, sociale onrust, boycot

Impact

Kwetsbare assets

- Data
- Systemen
- Faciliteiten
- Processen
- Mensen
- Derde partijen
- Strategie

X

Kwaliteitsverlies

- Beschikbaarheid
- Integriteit
- Veiligheid
- Performance

Bedreigde doelen

Risico-gevolg

Direct meetbaar
- Operationeel (uitval, voorraadverlies, onderbroken productie & levering)
- Directe kosten (schade, verloren contracten)
- Indirecte kosten (zoals reparatie- of juridische kosten, contractuele compensatie)
- Compliance (boetes & sancties)

Lastig meetbaar
- Intellectueel eigendom (concurrentievoordeel)
- Reputatie (PR, goodwill, vertrouwen van stakeholders & marktwaarde)

Hogere doelen
- Duurzame planeet
- Burgerrechten
- Individuele privacy
- Gezondheid & veiligheid voor alle levende wezens

Cenvio

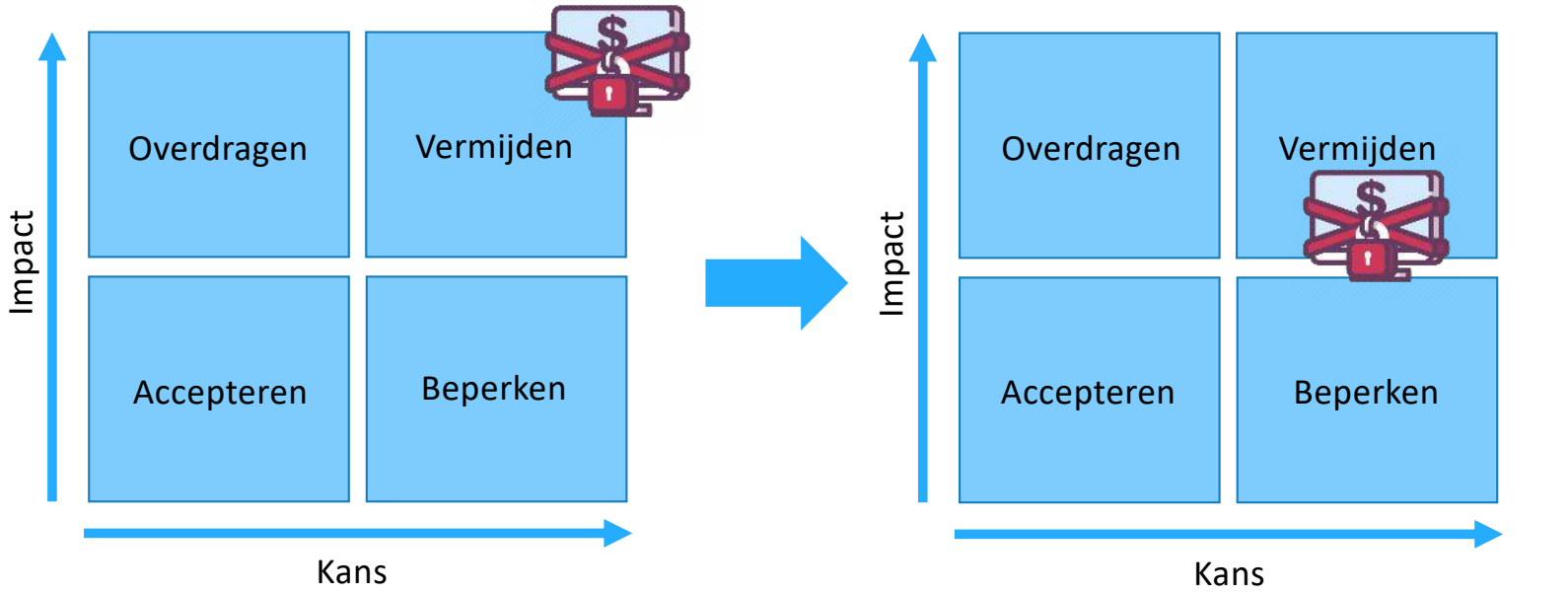
Risk Event Model: 28 inherente technologierisico's

	Beschikbaarheid	Integriteit	Veiligheid	Performance
Data	Onbeschikbare data	Onjuiste of ongeldige data	Gelekte of misbruikte data	Geen tijdige of passende data
Systemen	Onbeschikbaar systeem	Foutief ingericht systeem	Misbruikt of gehackt systeem	Matig werkend systeem
Faciliteiten	Onbeschikbare faciliteit	Onbetrouwbare werking faciliteit	Onveilige faciliteit	Matig resultaat vanuit faciliteit
Processen	Procedure ontbreekt	Slecht procesontwerp	Matige proces-beheersing	Matig resultaat vanuit het proces
Mensen	Tekort aan medewerkers	Kwaadwillende medewerker	Onachtzame medewerker	Falende kennis & vaardigheden
3de partijen	Discontinuïteit partner / dienst	Onbetrouwbare partner / dienst	Non-compliant partner / dienst	Matige kwaliteit partner / dienst
Strategie	Gebrek aan strategische visie	Strategisch verkeerde keuzes	Matige adoptie van de strategie	Matige executie van de strategie

Cenvio

Risicomanagement helpt bestuurders weinig met prioriteren

Vb. Ransomware -> aantasten van de dataveiligheid en databeschikbaarheid



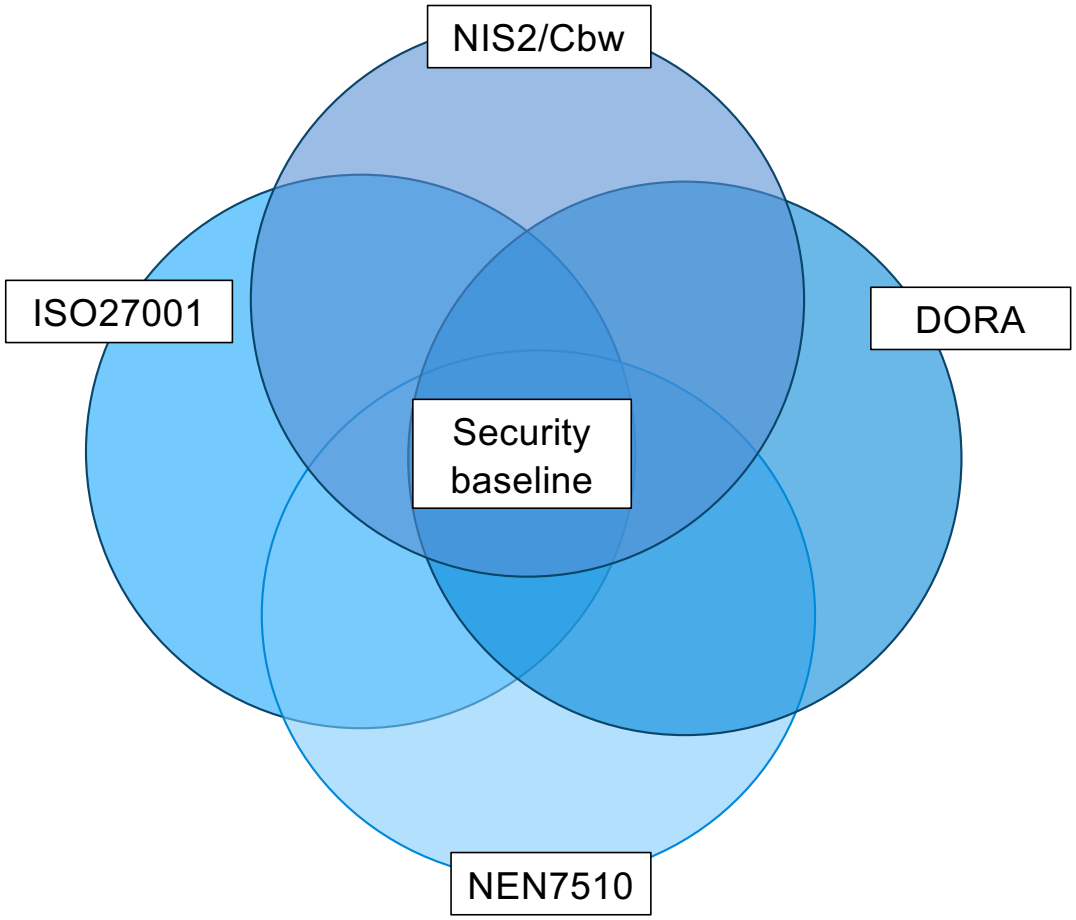
Inherent risico <u>voor</u> maatregelen

Restrisico <u>na</u> mitigerende maatregelen

Heb met bestuurders en toezichthouders daarom het goede gesprek over de effectiviteit van de juiste bekwaamheden voor een optimale weerbaarheid

Cenvio

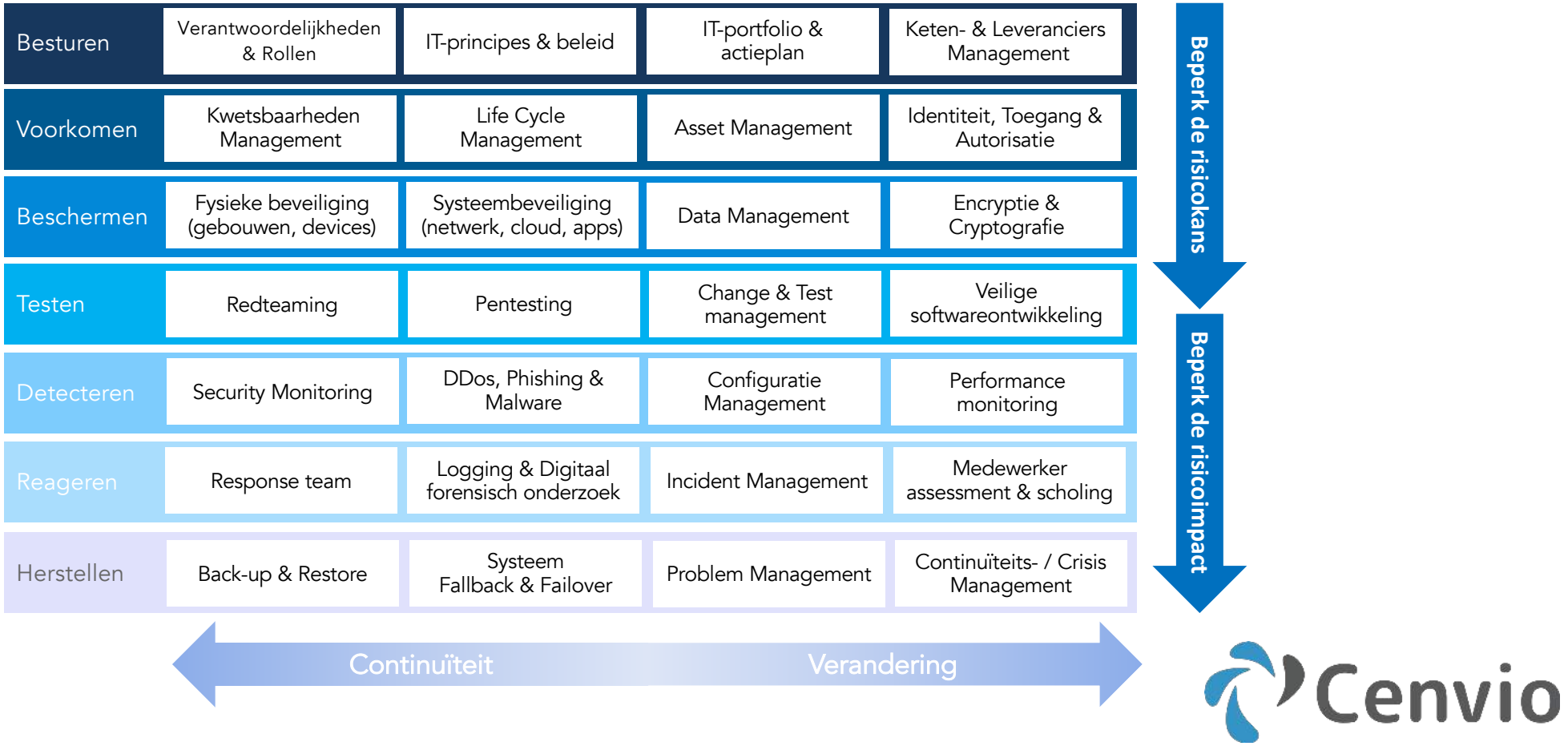
Bestaande frameworks: dezelfde wijn in andere zakken



Control frameworks verschillen op onderdelen en in accenten maar ze delen een “baseline” van 28 bekwaamheden om in control te zijn

Cenvio

IT Capability Model: meta control framework



Cenvio

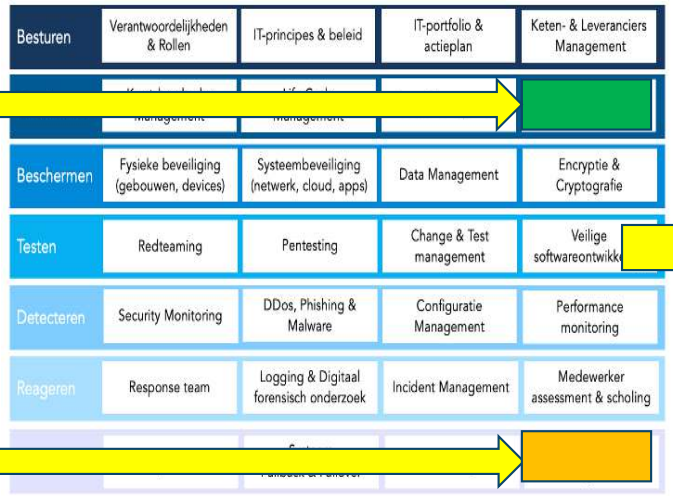
Werking in de praktijk: dashboards op de bestuurstafel

Beheermaatregelen

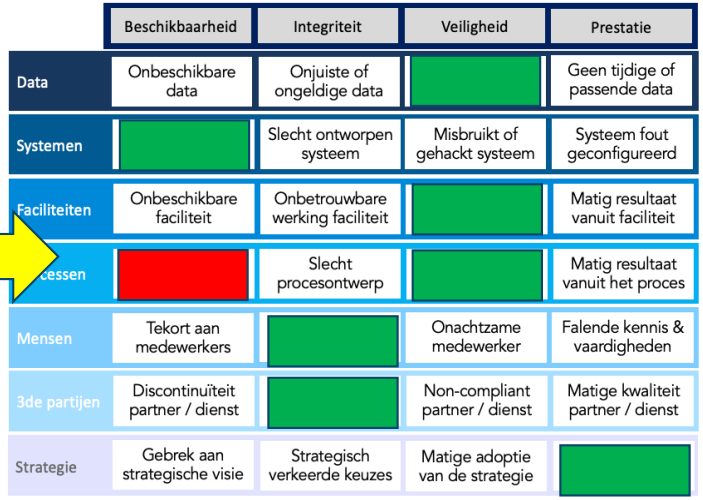
- Wachtwoordenbeleid ✅
- 2F-authenticatie ✅
- Single Sign On ✅
- RBAC / PAM ❌
- Zero trust principes ✅

- Business Continuity Plan ✅
- Crisis Mgt Organisatie ✅
- Crisisoefening ✅
- Crisis communicatie plan ❌
- Disaster Recovery Plan ❌

IT Capability Maturity Dashboard



Risk Event Mitigation Dashboard

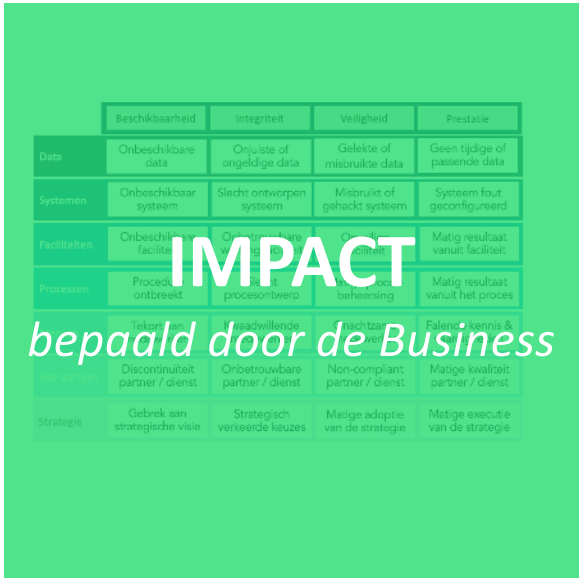


Etc…

- Als de beheermaatregelen binnen een bekwaamheid op orde zijn, is de bekwaamheid op volwassen niveau
- Als een bekwaamheid volwassen is, zijn de risico's die hiermee (deels) worden gemitigeerd, omlaag gebracht
- Meerdere volwassen bekwaamheden brengen samen de risico's terug naar een acceptabel niveau

Het goede gesprek met het bestuur over een actieplan

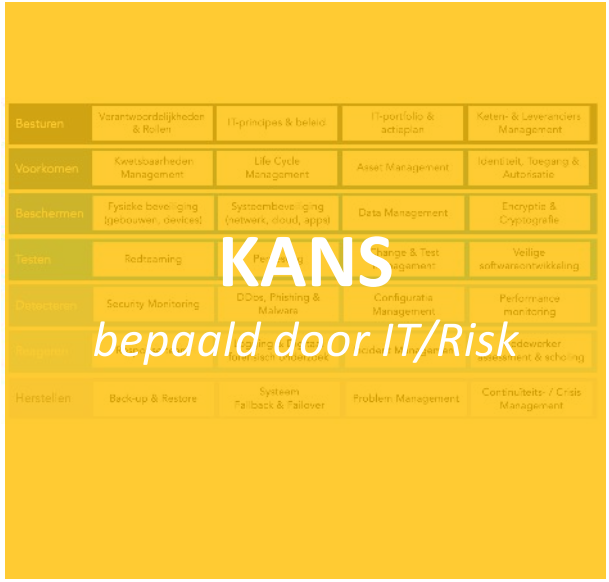
Risk Impact Assessment
(met Risk Event Model)



Doorleven risico's mede op basis van actieve monitoring en ervaringen

X

Maturity Assessment
(met IT Capability Model)



Volwassenheid van de risico-mitigatie toetsen door confrontatie van de risico's met genomen maatregelen

=

Fit-Gap Assessment

Noodprocedures (BCM)

Procedurele IT-maatregelen

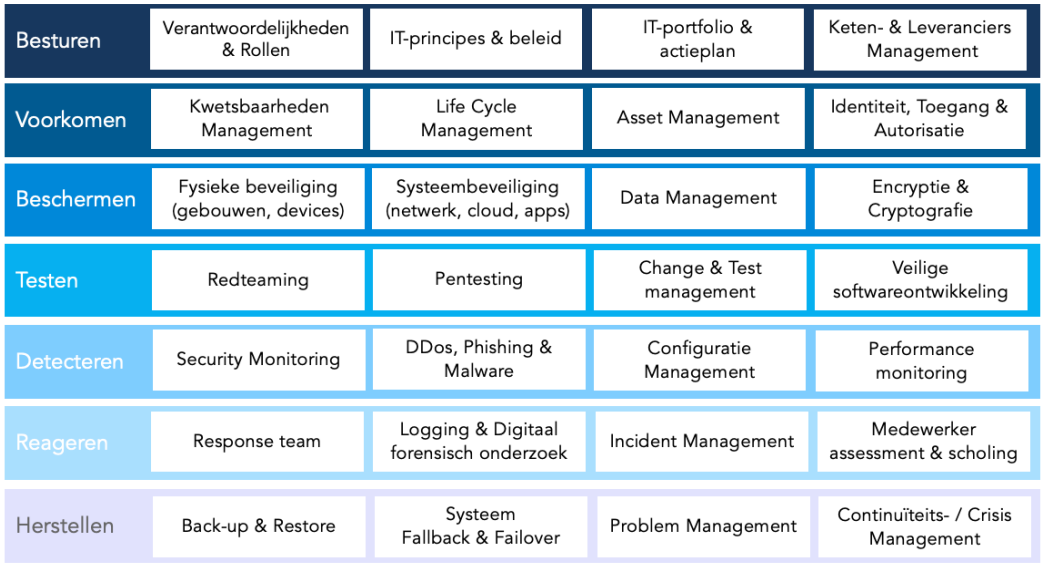
Technische IT-maatregelen

Geaccepteerd restrisico

Risk Action Plan

Cenvio

IT Capability Model ook voor verantwoording aan derden



Self assessment / Interne audit:
- NEN7510
- Horizontaal toezicht
- NIS2

Third Party Memo (TPM) of ISAE3402 opgesteld door accountant:
- Assurance over de (uitbestede) IT diensten

Jaarrekening controle door accountant:
- Betrouwbaarheid en continuïteit van financiële gegevensverwerking

Certificeringen of externe audit:
- DigiD audit
- NEN7510
- ISO27001

mapping

Cenvio

IT Capability Model: mapping op andere frameworks

		Mapping tabel
Capability Name	NIS2	ISO27001:2022 / NEN7510:2024 / BIO2
Verantwoordelijkheden & Rollen Vb. 1	Artikel 20 Governance Bestuur dient genomen beheermaatregelen goed te keuren Bestuur dient toe te zien op de uitvoering van de beheermaatregelen Bestuur kan aansprakelijk gesteld worden bij grove nalatigheid Bestuur dient een opleiding te volgen rond informatiebeveiliging Bestuur dient een soortgelijke opleiding ook aan medewerkers aan te bieden	5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging 5.3 Scheiding van taken 5.4 Managementverantwoordelijkheden 5.5 Contact met overheidsinstanties 5.6 Contact met speciale belangengroepen 5.19 Informatiebeveiliging in leveranciersrelaties 5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten 5.35 Onafhankelijke beoordeling van informatiebeveiliging 6.2 Arbeidsovereenkomst
Keten- en Leveranciers Management Vb. 2	Artikel 21.2d Toeleveringsketenbeveiliging Artikel 21.2i Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa Artikel 24 Europese cyberbeveiligingscertificeringsregelingen Bepaalde ICT-producten, ICT -diensten en ICT -processen kunnen soms EU-certificering vereisen	5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging 5.11 Retourneren van bedrijfsmiddelen 5.14 Overdragen van informatie 5.19 Informatiebeveiliging in leveranciersrelaties 5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten 5.21 Beheren van informatiebeveiliging in de ICT-keten 5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten 5.23 Informatiebeveiliging voor het gebruik van clouddiensten 5.31 Wettelijke, statutaire, regelgevende en contractuele eisen 5.32 Intellectuele-eigendomsrechten 5.37 Gedocumenteerde bedieningsprocedures 5.38 HLT Analyse en specificatie van informatiebeveiligingseisen 6.1 Screening 6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten 8.30 Uitbestede systeemontwikkeling

Key Take Away

- Verlies je niet in risico-assessments en te veel geloof in de uitkomsten daarvan.
- Er zijn per saldo 28 unieke technologierisico's te onderkennen (die voor elke organisatie vrijwel gelijk zijn).
- Er zijn per saldo ook 28 bekwaamheden nodig om de risico's af te dekken.
- Een goed gesprek in de bestuurskamer geeft inzicht in de effectiviteit van risicomitigatie op die bekwaamheden.
- Voorkom zoveel mogelijk dat meerdere normenkaders op verschillende wijze moeten worden verantwoord.
- Vertaal pas bij een externe audit dit met hulp van een mappingtabel naar de gevraagde standaard of norm.
- Een passende bestuursrapportage is simpel, op hoofdlijnen en toont verbeteracties (risk action plan).

Cenvio

Vragen?

Cenvio

Bedankt!

Contact:
Werner Zuurbier
+31 6 14279450
werner@zuurbier.nl
www.linkedin.com/in/zuurbier

Boek Cyber in the Board bestellen?
https://www.bravenewbooks.nl/wernerzuurbier

Cenvio