

Prompt – Korte digitale weerbaarheidscheck

Ik wil een korte check doen van de digitale weerbaarheid van mijn organisatie.

Gebruik de onderwerpen uit ISO/IEC 27001:2022 Annex A als inhoudelijk kader, maar behandel dit niet als een formele ISO-audit.

Treed op als kritische interviewer. Stel steeds **één vraag tegelijk** en wacht op mijn antwoord. Gebruik begrijpelijke taal. Stel alleen vervolgvragen als dat echt nodig is.

Stap 1 – Begrijp eerst mijn organisatie

Stel maximaal **zes korte vragen**:

1. In welke sector werken we en wat doen we?
2. Hoeveel medewerkers en locaties hebben we?
3. Van welke digitale systemen of cloudapplicaties zijn we sterk afhankelijk?
4. Welke gevoelige gegevens verwerken we, zoals persoonsgegevens, financiële gegevens of klantinformatie?
5. Wordt IT vooral intern beheerd, uitbesteed of allebei?
6. Welke situaties zijn op ons van toepassing:
 - meerdere locaties;
 - veel thuiswerken;
 - leveranciers met toegang tot systemen of gegevens;
 - eigen servers;
 - veel cloudapplicaties;
 - eigen softwareontwikkeling;
 - productie-, IoT- of OT-apparatuur;
 - bezoekers of publiek op locatie.

Gebruik deze antwoorden om daarna alleen relevante vragen te stellen.

Stap 2 – Stel maximaal 12 hoofdvragen

Kies de vragen die het meest relevant zijn voor mijn organisatie.

Zorg dat in ieder geval deze onderwerpen worden meegenomen wanneer ze van toepassing zijn:

Organisatie en verantwoordelijkheid

- Is duidelijk wie verantwoordelijk is voor cybersecurity?
- Weet de directie welke digitale risico's de grootste impact kunnen hebben?

Medewerkers

- Krijgen medewerkers periodiek training of awareness over cyberrisico's?
- Weten medewerkers wat ze moeten doen bij phishing, een verdacht telefoontje of een mogelijk incident?
- Worden nieuwe medewerkers, waar passend en wettelijk toegestaan, gescreend voor functies met toegang tot gevoelige informatie of kritieke systemen?

Accounts en toegang

- Wordt multifactor-authenticatie gebruikt voor belangrijke accounts en systemen?
- Krijgen medewerkers alleen toegang tot wat zij voor hun werk nodig hebben?
- Worden accounts en rechten aangepast of ingetrokken bij functiewijziging of uitdiensttreding?

Systemen en netwerk

- Worden apparaten en software tijdig bijgewerkt en beschermd tegen bekende kwetsbaarheden?
- Zijn netwerk, wifi en externe toegang passend beveiligd?
- Worden verdachte activiteiten ergens gemonitord?

Data en privacy

- Is duidelijk welke gevoelige en persoonlijke gegevens worden bewaard en wie daar toegang toe heeft?
- Worden gegevens verwijderd of geanonimiseerd wanneer ze niet meer nodig zijn?
- Worden back-ups gemaakt én periodiek getest?

Leveranciers

Alleen stellen als externe leveranciers of clouddiensten relevant zijn:

- Welke leveranciers zijn kritisch voor de bedrijfsvoering?
- Is geregeld welke toegang zij hebben, hoe zij gegevens beschermen en wat er gebeurt bij een incident of uitval?

Continuïteit en incidenten

- Weet de organisatie wie wat doet wanneer een belangrijk systeem, internetverbinding of leverancier uitvalt?
- Is dit ooit geoefend of getest?

Fysieke beveiliging

Alleen stellen als eigen locaties of apparatuur relevant zijn:

- Is toegang tot apparatuur, technische ruimtes en gevoelige informatie voldoende beperkt?

Softwareontwikkeling

Alleen stellen als de organisatie software ontwikkelt of laat ontwikkelen:

- Worden beveiligingseisen en tests meegenomen voordat software in productie gaat?

Stap 3 – Houd de check kort

Hanteer deze regels:

- Stel maximaal **12 hoofdvragen** na de profielvragen.
- Sla onderwerpen over die niet relevant zijn.
- Vermijd dubbele vragen.
- Stel maximaal één verdiepende vraag als een antwoord te algemeen is.
- Vraag niet naar wachtwoorden, IP-adressen, firewallregels of andere gevoelige technische details.
- Baseer de beoordeling alleen op mijn antwoorden.

Vraag aan het einde:

"Is er nog relevante informatie over jullie digitale omgeving of bedrijfsvoering die niet aan bod is gekomen?"

Stap 4 – Geef een compacte uitslag

Maak daarna een korte samenvatting met:

Wat gaat al goed

Maximaal drie punten.

Waar zitten de belangrijkste aandachtspunten?

Maximaal drie punten.

Wat verdient nu prioriteit?

Selecteer de drie belangrijkste onderwerpen.

Wat kunnen we de komende 30 dagen doen?

Geef maximaal vijf concrete acties en vermeld wie daarbij betrokken moet zijn, bijvoorbeeld directie, IT, HR, privacy, facilitair of leverancier.

Sluit af met:

Deze check gebruikt onderwerpen uit ISO/IEC 27001 Annex A als referentiekader.

Het is een eerste inventarisatie van digitale weerbaarheid en geen ISO 27001-audit, certificeringsbeoordeling of professionele security-audit.