GIDS

De complete gids voor security audits & assessments

Van quickscan tot compliance-audit: wat het kost, hoe het werkt en waar je op moet letten.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De belangrijkste cijfers over security audits, compliance en het Nederlandse dreigingslandschap.

EUR 270K
Gemiddelde schade per cyberincident voor MKB in Nederland
Apex Security [1]

~10.000
Nederlandse organisaties die onder de Cyberbeveiligingswet (NIS2) vallen
Digitale Overheid [2]

86%
van Nederlandse bedrijven gebruikt antivirussoftware -- maar hoeveel heeft een audit gedaan?
CBS Cybersecuritymonitor 2024 [3]

EUR 10M
maximale boete onder NIS2 voor essentieel entiteiten (of 2% wereldwijde jaaromzet)
Digitale Overheid [2]

121+
unieke ransomware-incidenten in Nederland in 2024
NCSC Cybersecuritybeeld 2025 [4]

88%
van MKB-datalekken bevat ransomware
Verizon DBIR 2025 [5]

EUR 2.500
RVO subsidie beschikbaar voor cybersecurity bij MKB
RVO / TTTP [6]

34%
stijging in exploitatie van kwetsbaarheden als initial access vector
Verizon DBIR 2025 [5]

1. Wat is een security audit & assessment?

Een security audit is een systematische evaluatie van de cybersecurity-status van je organisatie, met als doel risico's in kaart te brengen en een concreet verbeterplan op te stellen.

Een security audit beoordeelt de technische maatregelen, het beveiligingsbeleid, de processen en de naleving van relevante wet- en regelgeving van je organisatie. Het is een foto van je huidige beveiligingssituatie, inclusief concrete aanbevelingen voor verbetering.

Er bestaan verschillende typen assessments, van een snelle quickscan (halve dag) tot een uitgebreide compliance-audit (meerdere weken). Het juiste type hangt af van je doelstelling: wil je een globaal beeld, wil je certificeringsklaar worden, of moet je voldoen aan specifieke regelgeving?

TYPEN SECURITY ASSESSMENTS

TYPE	DOEL	DOORLOOPTIJD	KOSTEN MKB
Quickscan/nulmeting	Globaal beeld van beveiligingsstatus	1-2 weken	EUR 1.500 - 5.000 [7]
Gap analysis	Vergelijking met norm (ISO 27001, NIS2)	2-4 weken	EUR 5.000 - 15.000 [8]
Volledige security audit	Diepgaande beoordeling van alle aspecten	4-8 weken	EUR 10.000 - 30.000 [8]
Compliance audit (NIS2)	Toetsing aan specifieke regelgeving	3-6 weken	EUR 8.000 - 25.000 [9]
Configuration review	Beoordeling technische configuraties	1-3 weken	EUR 2.500 - 8.000

2. Waarom is het belangrijk?

Zonder audit weet je niet wat je niet weet. En wat je niet weet, kan je organisatie ernstig schaden.

De gemiddelde kosten van een cyberincident voor een MKB-organisatie in Nederland bedragen EUR 270.000 [1]. Een security audit kost een fractie daarvan en brengt de kwetsbaarheden in kaart voordat aanvallers ze vinden. Het is het verschil tussen een brandoefening en een echte brand.

Met de komst van de Cyberbeveiligingswet (NIS2) worden onafhankelijke audits voor essentieel entiteiten verplicht [2]. Maar ook zonder wettelijke verplichting is een periodieke audit een best practice die door verzekeraars, klanten en ketenpartners steeds vaker wordt verwacht.

DE COMPLIANCE-DRUK NEEMT TOE

- **NIS2/Cyberbeveiligingswet:** onafhankelijke audits verplicht voor essentieel entiteiten, boetes tot EUR 10 miljoen [2]
- **AVG:** boetes tot EUR 20 miljoen of 4% wereldwijde jaaromzet [10]
- **ISO 27001:2022 transitie:** organisaties moeten opnieuw geaudit worden
- **Cyberverzekeraars:** eisen steeds vaker een security assessment als acceptatievoorwaarde
- **Ketenpartners:** vragen om aantoonbare beveiliging (SOC 2, ISO 27001)

3. Hoe werkt het?

Het auditproces van intake tot oplevering.

1 Intake en scopebepaling

1-2 DAGEN

De auditor inventariseert je organisatie, IT-omgeving en doelstellingen. Samen bepaal je de scope: welke systemen, processen en normen worden getoetst.

2 Documentatie-review

3-5 DAGEN

Bestaand beleid, procedures, risicoanalyses en technische documentatie worden beoordeeld op volledigheid en actualiteit.

3 Technische beoordeling

3-10 DAGEN

De auditor beoordeelt de configuratie van systemen, netwerken en applicaties. Dit kan handmatig en/of geautomatiseerd gebeuren.

4 Interviews en observaties

2-5 DAGEN

Gesprekken met medewerkers, management en IT om te toetsen of beleid ook in de praktijk wordt gevolgd.

5 Rapportage en verbeterplan

3-5 DAGEN

Je ontvangt een rapport met bevindingen, risicoclassificatie en een geprioriteerd verbeterplan met concrete aanbevelingen.

4. Wat kost het?

Tarieven voor security audits in Nederland.

KOSTENPOST	TARIEF
Security consultant (per uur)	EUR 120 - 160 [8]
Senior auditor (per dag)	EUR 1.200 - 1.500 [8]
Halve dag audit	EUR 600 - 750 [8]

PRIJSINDICATIE PER TYPE ASSESSMENT

TYPE	KLEIN MKB (10–50 MDW)	GROOT MKB (50–250 MDW)
Quickscan	EUR 1.500 - 3.000	EUR 3.000 - 5.000
Gap analysis (NIS2)	EUR 5.000 - 8.000	EUR 8.000 - 15.000
Volledige audit	EUR 8.000 - 15.000	EUR 15.000 - 30.000
Jaarlijkse heraudit	EUR 3.000 - 5.000	EUR 5.000 - 10.000

TIP

De RVO biedt een subsidie van tot EUR 2.500 voor cybersecurity-maatregelen bij MKB-bedrijven. Een quickscan kan hiermee (deels) worden gefinancierd [6].

5. Waar moet je op letten?

Selectiecriteria bij het kiezen van een auditpartner.

- **Certificeringen van de auditor** -- CISSP, CISA, RE (Register EDP-auditor), ISO 27001 Lead Auditor
- **Ervaring in jouw sector** -- Een auditor die je branche kent, begrijpt de context en risico's
- **Onafhankelijkheid** -- De auditor mag geen belang hebben bij het verkopen van oplossingen
- **Methodologie** -- Welk framework wordt gebruikt? (ISO 27001, NIST CSF, NIS2, CIS Controls)
- **Rapportage-kwaliteit** -- Zijn de aanbevelingen concreet en geprioriteerd?

10 VRAGEN VOOR JE AANBIEDER

1. Welke certificeringen hebben jullie auditors?
2. Hoeveel security audits voeren jullie jaarlijks uit?
3. Hebben jullie ervaring in mijn sector?
4. Welk framework/norm gebruiken jullie als referentie?
5. Wat is de doorlooptijd van intake tot rapport?
6. Hoe ziet het rapport eruit? Kan ik een voorbeeld zien?
7. Bieden jullie ook ondersteuning bij het opvolgen van bevindingen?
8. Hoe gaan jullie om met gevoelige informatie die tijdens de audit wordt gevonden?
9. Zijn jullie onafhankelijk van security-leveranciers?
10. Wat zijn de kosten en wat is inbegrepen?

6. Veelgemaakte fouten

Fout 1: Audit als eenmalige actie zien

Een security audit is een momentopname. Je IT-omgeving verandert continu: nieuwe systemen, nieuwe medewerkers, nieuwe dreigingen. Plan minimaal jaarlijks een heraudit of continue assessment om je beveiligingsstatus actueel te houden.

Fout 2: Audit alleen voor compliance doen

Een audit die puur op papieren compliance is gericht, levert een vinkjeslijst op maar geen echte beveiliging. Zorg dat de audit ook daadwerkelijk je risico's in kaart brengt en niet alleen toetst aan formele eisen.

Fout 3: Bevindingen niet opvolgen

Het rapport ligt op de plank, maar er verandert niets. Zonder opvolging is de audit weggegooid geld. Maak een concreet actieplan met eigenaren, deadlines en budget.

Fout 4: Scope te breed of te smal

Een audit van alles kost veel en levert oppervlakkige resultaten. Een audit van alleen je firewall mist de rest. Bepaal vooraf welke risico's prioriteit hebben en stem de scope daarop af.

Fout 5: Management niet betrekken

Zonder management-commitment worden bevindingen niet opgepakt. Betrek het management vanaf het begin bij de scopebepaling en presenteer bevindingen in business-taal, niet in technisch jargon.

7. NIS2 en regelgeving

De Cyberbeveiligingswet (NIS2) gaat naar verwachting in Q2 2026 in werking [2]. De wet vereist dat essentieel entiteiten onafhankelijke audits laten uitvoeren. Boetes voor niet-naleving kunnen oplopen tot EUR 10 miljoen of 2% van de wereldwijde jaaromzet [2].

De drie kernverplichtingen zijn: zorgplicht (passende maatregelen), meldplicht (incidenten binnen 24 uur melden) en registratieplicht. Een security audit helpt bij het aantonen van de zorgplicht en het identificeren van tekortkomingen.

8. Security audit vs pentest vs gap analysis

KENMERK	SECURITY AUDIT	PENETRATIETEST	GAP ANALYSIS
Focus	Breed: beleid, processen, techniek	Diep: technische kwetsbaarheden	Verschil huidige vs gewenste staat
Methode	Review, interviews, toetsing	Gecontroleerde aanvalssimulatie	Vergelijking met norm/ framework
Resultaat	Risico-overzicht + verbeterplan	Lijst kwetsbaarheden + bewijs	Roadmap naar compliance
Doorlooptijd	2-8 weken	1-4 weken	1-4 weken
Kosten MKB	EUR 5.000 - 30.000	EUR 3.000 - 25.000	EUR 5.000 - 15.000

Complementair, niet vervangend: Een pentest test technische kwetsbaarheden, een gap analysis vergelijkt met een norm, en een security audit beoordeelt het totaalplaatje. De meeste organisaties hebben alle drie nodig op verschillende momenten.

9. Trends 2025--2026

NIS2 compliance-audits

De verwachte inwerkingtreding van de Cyberbeveiligingswet in Q2 2026 zorgt voor een grote vraag naar NIS2 gap analyses en compliance assessments. Organisaties willen weten of ze eronder vallen en wat ze moeten doen [2].

Continuous security assessment

De trend verschuift van periodieke audits naar continue monitoring en beoordeling. Tools die continu je configuraties, kwetsbaarheden en compliance-status monitoren worden gangbaarder.

Supply chain audits

Met de verdubbeling van datalekken via derden [5] groeit de vraag naar supply chain security assessments. Organisaties willen zekerheid over de beveiliging van hun leveranciers.

10. Aan de slag

Klaar voor een security audit? Begin hier.

1. **Bepaal je doelstelling**
   Wil je een globaal beeld (quickscan), compliance aantonen (NIS2, ISO 27001) of een diepgaande risicobeoordeling?

2. **Verzamel basisinformatie**
   Maak een overzicht van je IT-omgeving, bestaand beleid en eerdere audits. Dit versnelt het intakeproces.

3. **Vergelijk aanbieders**
   Vraag offertes op bij minimaal 3 partijen. Let op certificeringen, ervaring en onafhankelijkheid.

Bronnenlijst

[1] **Apex Security** -- SIEM voor het MKB -- apexsecurity.nl/en/siem-voor-het-mkb-professionele-beveiliging-zonder-enterpriseprijskaartje/

[2] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2) -- digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[3] **CBS** -- Cybersecuritymonitor 2024 -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[4] **NCSC** -- Cybersecuritybeeld Nederland 2025 -- ncsc.nl/actueel/nieuws/2025/11/26/cybersecuritybeeld-2025

[5] **Verizon** -- 2025 Data Breach Investigations Report -- verizon.com/business/resources/reports/dbir/

[6] **The Trusted Third Party** -- MKB subsidie cybersecurity -- thetrustedthirdparty.nl/blogs/cyber-security/ga-nu-direct-werken-aan-jouw-cyber-security-met-subsidie-van-de-overheid/

[7] **NTNT** -- Wat kost goede cybersecurity voor een MKB? -- ntnt.nl/wat-kost-goede-cybersecurity-voor-een-mkb/

[8] **Innvolve** -- Wat kost cybersecurity? -- innvolve.nl/blog/wat-kost-cybersecurity/

[9] **Copla** -- NIS2 Audit Requirements -- copla.com/blog/compliance-regulations/nis2-audit-requirements-checklist-and-how-to-prepare-for-it/

[10] **DataGuard** -- NIS2 Requirements -- dataguard.com/nis2/requirements/

[11] **IBM** -- Cost of a Data Breach Report 2025 -- ibm.com/reports/data-breach

[12] **NOREA** -- Cyber Security Assessment -- norea.nl/uploads/bfile/e863236b-8e4e-4632-ad63-b62c0ac33bc3

[13] **CCV** -- Keurmerk Digitale Basisveiligheid MKB -- hetccv.nl/keurmerken/cybersecurity/keurmerk-digitale-basisveiligheid-mkb/

[14] **Securable** -- Tarieven -- securable.nl/tarieven/

[15] **CrowdStrike** -- 2026 Global Threat Report -- crowdstrike.com/en-us/global-threat-report/