



# DigiD-audits

# Scope

AuditConnect is expert op het gebied van DigiD-audits, IT-Audits en Security Scans. Onze medewerkers zijn allen gekwalificeerde IT-auditors en geregistreerd bij NOREA (Nederlandse Orde van Register EDP-Auditors). Hierdoor bent u verzekerd van de juiste kennis en kunde. Het ICT-Beveiligingsassessment DigiD is een jaarlijks terugkerend assessment dat alle Nederlandse gemeenten met een DigiD-koppeling moeten uitvoeren in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het assessment bestaat uit een audit en afhankelijk van de gemeentelijke ICT-infrastructuur uit één of meer penetratietesten. In deze White paper vindt u meer informatie over de norm, het toetsingsproces en op welke wijze AuditConnect u bij deze audit kan ondersteunen.



Kennis & kunde

## De DigiD norm

De DigiD norm is gebaseerd op de normen zoals die door het Nationaal Cybersecurity Center (NCSC) zijn geformuleerd voor web applicaties. De norm voor de DigiD audit bestaat uit de richtlijnen met de hoogste impact op de veiligheid van DigiD. Logius adviseert alle organisaties om buiten de maatregelen uit de norm ook de andere maatregelen uit de ICT-beveiligingsrichtlijnen voor web applicaties te adopteren.

Hoogste impact  
op veiligheid

# AuditConnect hanteert het volgende stappenplan

## **Stap 1** Zelf toetsen aan de hand van de richtlijnen

Door het uitvoeren van een interne beoordeling en vast te stellen in hoeverre de systemen aan de norm voldoen, krijgt u inzicht in maatregelen die in ieder geval moeten worden getroffen. AuditConnect kan u hierbij ondersteunen door het uitvoeren van een pre-audit.

## **Stap 2** Verbetermaatregelen implementeren

Op basis van de zelftoets of de pré-audit heeft u zicht op de zaken die nog moeten worden geïmplementeerd. In deze stap dient u de noodzakelijke maatregelen in te voeren.

## **Stap 3** Uitvoeren van een security scan en een penetratietest

Uitvoeren van een security scan (gericht op de interne ICT-omgeving) en een penetratietest (ook wel 'ethical hacking test') uitvoeren op uw systemen. AuditConnect kan dit voor u organiseren. Mocht u dit al hebben uitgevoerd dan beoordelen wij het pentestrapport met bevindingen om vast te stellen of wordt voldaan aan de eisen uit het normenkader.

## **Stap 4** Bevindingen oplossen

De uitkomsten van zowel de security scan als de penetratietest kunnen aanleiding zijn om verbeteringen door te voeren. Deze verbeteringen kunnen betrekking hebben op de interne organisatie maar mogelijk ook bij de externe leverancier (bij gebruik van oplossingen).

## **Stap 5** Audit uitvoeren

Als alle voorgaande activiteiten zijn afgerond wordt het feitelijke ICT-beveiligingsassessment uitgevoerd. Dit dient te gebeuren door een Register EDP-auditor (RE). AuditConnect beschikt over RE's en kan de audit voor u uitvoeren.

## **Stap 6** Bevindingen naar Logius sturen

De rapportage over het uitgevoerde ICT beveiligingsassessment DigiD dient verstuurd te worden naar Logius. De rapportage bevat een overzicht van de feitelijke bevindingen per maatregel. Per maatregel wordt aangegeven of deze voldoet: Ja, Nee of Niet van Toepassing.



## Overzicht

### Meer informatie?

Mocht u meer informatie willen over het ICT beveiligingsassessment DigiD of over de overige producten en diensten van AuditConnect, neem dan contact met ons op. Wij zijn te bereiken via:

Telefoon

**055-3010100**

E-mail

**[info@auditconnect.nl](mailto:info@auditconnect.nl)**

AuditConnect informeert u graag geheel vrijblijvend over de mogelijkheden en oplossingen.

- ✓ DigiD-audits
- ✓ IT-Audits
- ✓ Security Scans



**AuditConnect b.v.**

Bezoekadres:

Meester van Rhemenslaan 7

7316 AK Apeldoorn

Postadres:

Postbus 4355

7320 AJ Apeldoorn

Telefoon: 055 - 30 101 00

Fax: 055 - 30 100 11

[info@auditconnect.nl](mailto:info@auditconnect.nl)

[www.auditconnect.nl](http://www.auditconnect.nl)