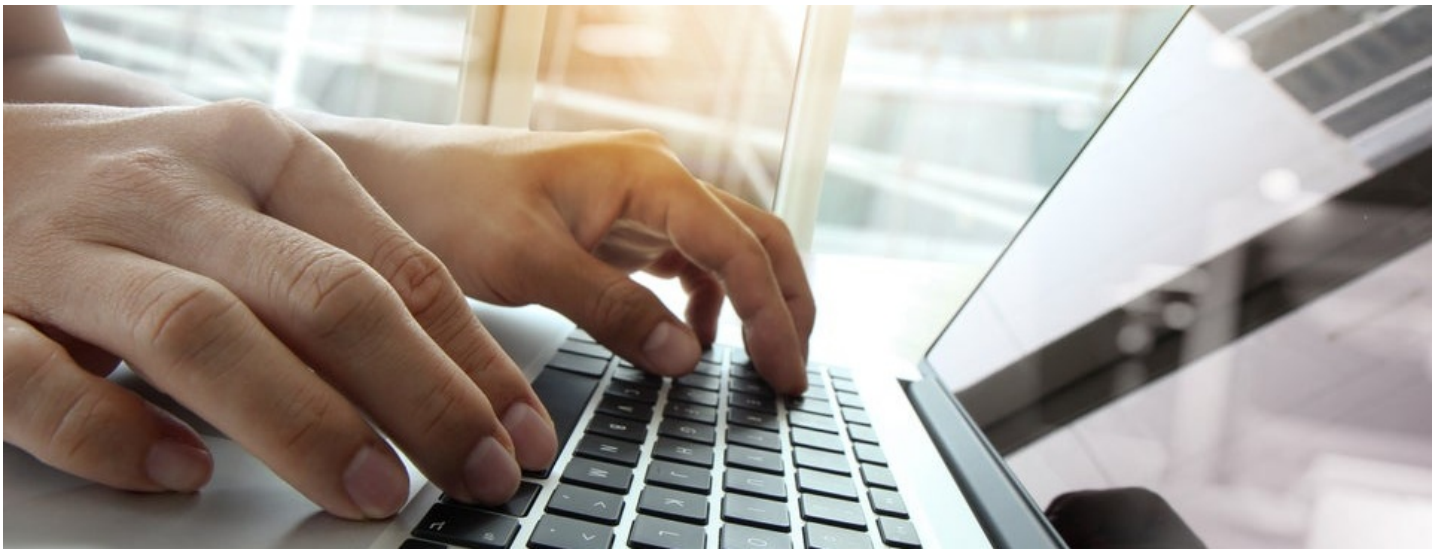
DigiD Audit



Via DigiD kunnen burgers steeds meer zaken regelen met de overheid. Het spreekt voor zich dat de beveiliging van systemen en informatie hierbij cruciaal is. Om organisaties die werken met DigiD te helpen om te voldoen aan de geldende overheidsrichtlijnen is er Kiwa's DigiD Audit.

Via DigiD wordt een breed aanbod e-overheidsdiensten ontsloten. Effectief en eenvoudig, maar onvoldoende aandacht voor de beveiliging van de systemen en informatie kan ongewilde risico's met zich meebrengen, met alle gevolgen van dien.
Alle organisaties die een DigiD-koppeling gebruiken, moeten daarom voldoen aan ICT-beveiligingsrichtlijnen die zijn vastgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Dit is een verplichting vanuit de overheid waarop een jaarlijkse toetsing plaatsvindt, uitgevoerd door een Register EDP-auditor.

Wat houdt de DigiD-audit in?

Bij de jaarlijkse toetsing van gebruikers van de DigiD-koppeling wordt getoetst of wordt voldaan aan richtlijnen rondom de beveiliging van webapplicaties. Hierbij wordt onder meer gekeken naar het beveiligingsbeleid, de webapplicatie zelf en het beheer van de webomgeving.
De norm bestaat uit de richtlijnen die de hoogste impact hebben op de veiligheid van DigiD. Het resultaat van deze audit is een rapport met hierin per maatregel de bevindingen. Dit rapport wordt gedeeld met Logius, de digitale dienstverlener van de Rijksoverheid.

Hoe kan Kiwa u bij de DigiD-audit helpen?

Kiwa kan u helpen de toetsing uit te voeren om vast te stellen of u voldoet aan de gestelde richtlijnen. Dat doen we via een vastomlijnd stappenplan.

- Nulmeting – De nulmeting betreft een interne beoordeling om vast te stellen waar de organisatie staat in relatie tot de

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 49 00

verplichte maatregelen en wat moet er nog moet gebeuren om klaar te zijn voor de DigiD audit. Kiwa kan u hierbij ondersteunen met een proefaudit. Die leidt tot een rapport met verbeterpunten.

- Penetratietest – Alvorens de DigiD audit uit te voeren is het belangrijk dat er een penetratietest wordt uitgevoerd op uw systeem. Hierbij wordt gekeken naar potentiële kwetsbaarheden waar kwaadwillenden misbruik van kunnen maken. De test wordt afgerond met een rapportage waarbij de bevindingen toegelicht zullen worden. Kiwa heeft partners die u kunnen helpen deze test uit te voeren.
- DigiD audit – Nadat de voorgaande stappen zijn doorlopen en de bevindingen zijn opgelost, kan het daadwerkelijke assessment op de DigiD omgeving plaatsvinden. Hierbij wordt gekeken of alle maatregelen getroffen zijn en ook werken. Dit onderzoek wordt voor u uitgevoerd door een Register EDP auditor.
- Rapportage – Na het onderzoek wordt er een rapportage opgesteld met hierin de feitelijke bevindingen. Per bevinding zal worden aangegeven of u voldoet of niet.

Kiwa - wereldwijde speler op het gebied van het uitvoeren van audits en certifcering - kan u helpen bij alle stappen van het proces en u begeleiden als partner for progress. Wilt u meer weten over onze diensten op het gebied van DigiD audits, neem dan contact op met ons Expert Center Information Security.

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 49 00