SECURANCE

Whitepaper

DigiD Assessment.

Inleiding

DigiD Assessment

In dit whitepaper bieden we inzicht in DigiD assessments en hoe organisaties kunnen voldoen aan de DigiD-normen zoals gedefinieerd door Logius. Dit document behandelt de DigiD-eisen, het proces van assessment en audit, en de voordelen van het uitvoeren van een DigiD-assessment oor uw organisatie.

Als professionele organisatie op het gebied van risicomanagement, governance en compliance ondersteunen wij organisaties bij het DigiD assessment proces. Wij beantwoorden graag alle vragen die u hierover heeft.

DigiD Assessment

Wat is een DigiD Assessment?

DigiD is een digitale identificatiemethode waarmee burgers veilig toegang krijgen tot online overheidsdiensten. Organisaties die DigiD gebruiken, moeten voldoen aan strikte beveiligingseisen die jaarlijks worden getoetst via een DigiD assessment.

Het assessment is verplicht voor alle organisaties die DigiD gebruiken in hun dienstverlening en omvat controles op informatiebeveiliging en compliance met de Baseline Informatiebeveiliging Overheid (BIO).

Fase 1. Scopebepaling

Hoe bepaal je de scope van een DigiD assessment?

De eerste fase bestaat uit het definiëren van de scope van het DigiD assessment. Dit is een cruciale stap die bepaalt welke systemen, processen en afdelingen binnen de organisatie worden beoordeeld. Een duidelijke scope zorgt ervoor dat het assessment efficiënt en effectief wordt uitgevoerd.

De belangrijkste onderdelen van de scopebepaling zijn:

- **Identificatie van de processen en systemen waarin DigiD wordt gebruikt:** Dit omvat het in kaart brengen van alle applicaties (en hun relevante versies), infrastructuren en systemen die met DigiD werken.

- **Bepaling van de interne controlemaatregelen op basis van de BIO:** De Baseline Informatiebeveiliging Overheid (BIO) stelt eisen aan informatiebeveiliging. Organisaties moeten bepalen welke maatregelen relevant zijn voor hun specifieke situatie.

- **Afstemming met stakeholders binnen de organisatie:** Het is essentieel om alle belanghebbenden (IT, compliance, management) te betrekken bij het definiëren van de scope, zodat alle risico's en afhankelijkheden goed worden meegenomen.

- **Opstellen van een gedetailleerde risicoanalyse:** Hierbij worden potentiële dreigingen en kwetsbaarheden in kaart gebracht en wordt beoordeeld hoe groot de impact van een incident kan zijn.

- **Overzicht van compliancevereisten en opstellen toetsingscriteria:** Dit omvat de wettelijke en contractuele verplichtingen waar de organisatie aan moet voldoen.

Daarnaast moet de organisatie beslissen of externe leveranciers en partners onderdeel zijn van de scope. Wanneer derde partijen betrokken zijn bij de verwerking van DigiD-gegevens, moeten hun beveiligingsmaatregelen ook worden beoordeeld.
Een goed gedefinieerde scope helpt niet alleen bij het stroomlijnen van het assessment, maar zorgt er ook voor dat alle relevante risico's en controlemaatregelen worden meegenomen. Dit draagt bij aan een succesvolle assessment en vermindert de kans op onverwachte problemen tijdens de auditfase.

Fase 2. Implementatie en voorbereiding

Beleidsmaatregelen en technische controles

In deze fase worden de nodige beleidsmaatregelen en technische controles geïmplementeerd. Dit proces omvat meerdere kritieke stappen om de beveiliging en compliance van DigiD-gebruik te waarborgen.

1. **Uitvoeren van een diepgaande risicoanalyse:**
    - Identificeren van de meest kwetsbare onderdelen binnen de organisatie.
    - Opstellen van een risicomatrix waarin de waarschijnlijkheid en impact van bedreigingen worden beoordeeld.

2. **Bepalen van beheersmaatregelen en security controls:**
    - Implementeren van technische beveiligingsmaatregelen zoals firewallconfiguraties, logging en monitoring.
    - Opstellen van toegangscontrolebeleid en autorisatieprocedures.

3. **Ontwikkelen en documenteren van beveiligingsbeleid:**
    - Opstellen van een gedetailleerd informatiebeveiligingsbeleid conform de BIO-richtlijnen.
    - Invoeren van richtlijnen voor gegevensverwerking en incidentmanagement.

4. **Opstellen van werkinstructies en procedures:**
    - Creëren van heldere procedures voor medewerkers die DigiD gebruiken.
    - Documenteren van protocollen voor het reageren op beveiligingsincidenten.

5. **Training en bewustwording van medewerkers:**
    - Organiseren van security awareness-trainingen om medewerkers bekend te maken met DigiD-veiligheidsvereisten.
    - Simuleren van phishingaanvallen en social engineering-testen om de weerbaarheid te verhogen.

6. **Implementatie van monitoringtools en continue naleving:**
    - Gebruik maken van Security Information and Event Management (SIEM) systemen om verdachte activiteiten te detecteren.
    - Regelmatige controle van logbestanden om afwijkingen en mogelijke inbreuken snel te signaleren.

Fase 3. Pre-audit en testfase

De stap voor de formele audit

De pre-audit en testfase is een essentiële stap om te zorgen dat de organisatie klaar is voor de formele audit. Tijdens deze fase wordt beoordeeld of de geïmplementeerde maatregelen effectief functioneren en of er nog tekortkomingen zijn die verholpen moeten worden.

1. **Beoordelen van de effectiviteit van de beheersmaatregelen:**
    - Controleren of alle beveiligingsmaatregelen correct zijn geïmplementeerd.
    - Vergelijken van de geïmplementeerde maatregelen met de BIO-eisen.

2. **Identificeren van zwakke plekken in het beveiligingsbeleid:**
    - Uitvoeren van kwetsbaarheidsanalyses en risico-evaluaties.
    - Simuleren van realistische aanvalsscenario's om de weerbaarheid te testen.

3. **Verzamelen van bewijsmateriaal voor de formele audit:**
    - Documenteren van alle testresultaten en analyses.
    - Opstellen van een rapportage over de status van de implementatie.

4. **Uitvoeren van simulaties en testscenario's:**
    - Organiseren van tabletop oefeningen en technische testen.
    - Evalueren hoe medewerkers reageren op beveiligingsincidenten.

5. **Evaluatie van incident response procedures:**
    - Testen van de effectiviteit van het incident response plan.
    - Controleren of alle medewerkers bekend zijn met hun rol tijdens een incident.

Door medewerkers bewust te maken van beveiligingsrisico's en hen de juiste middelen te geven, kan de organisatie beter inspelen op de DigiD-vereisten en de effectiviteit van haar beveiligingsmaatregelen vergroten.

Fase 4. Externe audit

De stap voor de formele audit

Tijdens deze fase wordt beoordeeld of de geïmplementeerde maatregelen effectief functioneren en of er nog tekortkomingen zijn die verholpen moeten worden.

Stappen in de externe audit en certificeringsfase:

1. **Selectie van een geaccrediteerde auditor:**
    - De organisatie schakelt een onafhankelijke IT-auditor in die ervaring heeft met DigiD-audits.
    - De auditor krijgt toegang tot relevante documentatie en systemen.

2. **Uitvoeren van een formele audit:**
    - De auditor beoordeelt de opgestelde documentatie en security policies.
    - Interviewrondes worden gehouden met sleutelfunctionarissen binnen de organisatie.
    - Technische controles en penetratietests worden uitgevoerd om de beveiligingsmaatregelen te verifiëren.

3. **Controle van operationele processen:**
    - De effectiviteit van interne procedures wordt beoordeeld.
    - Incidentrespons- en continuïteitsplannen worden getest en geëvalueerd.
    - Logging en monitoringmechanismen worden gecontroleerd op naleving en effectiviteit.

4. **Opstellen van het auditrapport:**
    - De auditor stelt een gedetailleerd rapport op waarin wordt aangegeven of de organisatie voldoet aan de DigiD-normen.
    - Eventuele tekortkomingen en verbeterpunten worden benoemd.
    - De organisatie krijgt de mogelijkheid om corrigerende maatregelen te nemen voordat het definitieve rapport wordt afgegeven.

5. **Rapportbeslissing:**
    - Als de organisatie aan alle eisen voldoet, wordt een formeel certificaat afgegeven.
    - Indien er tekortkomingen zijn, moet de organisatie aanvullende verbetermaatregelen doorvoeren en een hertest laten uitvoeren.

6. **Indienen van het auditrapport bij Logius:**
    - Het auditrapport wordt ingediend bij Logius, de beheerder van DigiD.
    - Logius beoordeelt de resultaten en geeft definitieve goedkeuring voor het gebruik van DigiD.

De externe audit is een kritieke stap in het DigiD-certificeringsproces en vereist een grondige voorbereiding. Door proactief samen te werken met de auditor en open te staan voor verbeteringen, kan de organisatie de certificering succesvol afronden en de naleving van DigiD-vereisten borgen.

5. Verbeteracties en naleving

Verbetering en compliance

Na de audit is het van cruciaal belang dat de organisatie blijft werken aan het verbeteren en onderhouden van de beveiligingsmaatregelen om blijvende compliance met de DigiD-vereisten te waarborgen.

Stappen in de verbeteracties en continue naleving:

1. **Opstellen van een verbeterplan:**
   - Op basis van de auditbevindingen worden verbeterpunten geïdentificeerd.
   - Een gestructureerd verbeterplan wordt opgesteld met duidelijke actiepunten en verantwoordelijkheden.

2. **Implementatie van verbetermaatregelen:**
   - Corrigerende acties worden uitgevoerd om eventuele tekortkomingen te verhelpen.
   - Technische en organisatorische maatregelen worden aangescherpt om beveiligingsrisico's verder te minimaliseren.

3. **Doorlopende monitoring en rapportage:**
   - Beveiligingsmaatregelen worden continu gemonitord om afwijkingen tijdig te signaleren.
   - Regelmatige interne audits en evaluaties worden uitgevoerd om naleving te waarborgen.
   - Periodieke rapportages worden opgesteld voor management en toezichthouders.

4. **Training en bewustwording:**
   - Medewerkers worden regelmatig getraind om op de hoogte te blijven van de laatste beveiligingsrisico's en DigiD-compliancevereisten.
   - Security awareness-programma's worden geïntegreerd in de organisatiecultuur.

5. **Jaarlijkse herbeoordeling:**
   - De organisatie voert jaarlijks een herbeoordeling uit om ervoor te zorgen dat DigiD-compliance gehandhaafd blijft.
   - Nieuwe bedreigingen en wijzigingen in regelgeving worden geanalyseerd en waar nodig verwerkt in het beveiligingsbeleid.

Door deze stappen structureel te volgen, blijft de organisatie voldoen aan de DigiD-normen en voorkomt zij potentiële beveiligingsincidenten en sancties. Continue naleving is essentieel om de veiligheid en betrouwbaarheid van DigiD-diensten te garanderen.

Over Securance

Investeer in efficiëntie

- **Wij analyseren uw risico's**
- **Plannen uw projecten**
- **Helpen bij de implementatie**
- **Helpen u te voldoen aan de hoogste standaarden**

Securance komt voort uit een 'Big Four' auditkantoor en is opgericht in 2004. Het resultaat van onze achtergrond is dat we werken volgens de hoogste professionele standaarden en ervaring hebben in het werken met strakke deadlines. We leven naar onze professionele normen en leveren altijd de hoogste kwaliteit, terwijl we er voortdurend naar streven om aan de behoeften van onze klanten te voldoen.

Door onze vlakke structuur en efficiënte communicatie kunnen we snel reageren op uw behoeften. Kiezen voor Securance betekent kiezen voor een professionele organisatie, maar ook kiezen voor een persoonlijke benadering. Effectief projectmanagement, onze ervaring met het implementeren van risicomanagementraamwerken in uw branche en professionaliteit zijn volgens ons de basis voor uitstekende resultaten.

Als Securance geloven wij dat een goed begrip, heldere communicatie en kennis van de branche van onze klanten essentieel zijn voor het leveren van toegevoegde waarde aan u als klant. Op basis van deze aanpak informeren wij u over de relevante veranderingen in wet- en regelgeving en andere belangrijke ontwikkelingen.

SECURANCE
BE SURE

Onze tevreden klanten

Referenties

Securance BV

Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.securance.nl