VOORBEREIDING SOC2 AUDIT IN 10 STAPPEN

Je organisatie voorbereiden op een SOC2 audit kan een intensieve klus zijn. Onderstaande 10 stappen bieden houvast.

1 Bepaal de scope

De eerste stap is tweeledig: je bepaalt hier de scope van het ***systeem*** en de scope van de ***criteria*** (normen). Met het bepalen van de scope van het systeem definieer je zo goed mogelijk waar de SOC2 verklaring over moet gaan. Bepalend is de behoefte van de gebruiker van het rapport (de (potentiële) klant en zijn auditors). Over welk systeem willen zij zekerheid?

2 Doe kennis op van de criteria

Het is belangrijk te ***begrijpen*** wát er getoetst gaat worden. Lees de criteria aandachtig door en vraag je steeds af wat men wil bereiken met dit criterium. Op die manier kun je de juiste beheersmaatregelen koppelen aan de criteria en identificeren waar beheersmaatregelen tekort schieten, ontbreken of niet zijn beschreven. De IT-auditor kan je helpen bij het begrijpen van de criteria.

3 Schrijf wat je doet en doe wat je schrijft

Het is belangrijk dat de organisatie formele policies, procedures, plannen en richtlijnen vastlegt, zodat onder meer processen goed volgbaar zijn en formeel verantwoordelijkheden zijn belegd. ***Beschrijf*** dus het wat, hoe, wanneer en wie in de organisatie en maak de documenten waarin dit is vastgelegd beschikbaar.

4 Creëer bewustzijn

Wanneer de organisatie op alle niveaus zich ***bewust*** is van de noodzaak om veilig te werken, ontstaat pas een beheersbare omgeving. Het melden en beschrijven van security incidenten, het veilig omgaan met bedrijfsmiddelen en gegevensdragers, het on- en offboarding proces voor medewerkers; zo maar een greep uit beheersmaatregelen die sterk afhankelijk zijn van mensen in de organisatie.

5 Maak het controleerbaar

Wanneer ad hoc acties of overleggen plaatsvinden, ontbreekt soms vast-legging. Zorg bij overleggen daarom voor ***notulen*** of een ***verslag*** en bij acties voor tickets met een beschrijving. Zorg dat periodieke acties, zoals de controle van toegangsbeveiliging, uitgevoerd zijn en dat het duidelijk is hoe, wat, wanneer en door wie dit gedaan is. Kies voor een methode die bij je organisatie past zodat het weinig extra werk kost.

6 Maak een systeembeschrijving

Een essentieel onderdeel van het rapport is de ***beschrijving van het systeem***. De IT-auditor levert tijdens de nulmeting een format aan. Bij het beschrijven is de vuistregel dat het to the point moet zijn, maar niet te specifiek. Zo ontstaat een onderhoudsvriendelijke beschrijving zonder bedrijfsgeheimen prijs te geven. Het opnemen van details over processen, namen van leveranciers en specifieke merken van systeemonderdelen wordt dus afgeraden.

7 Doe zelf een interne audit

Een objectieve ***interne audit*** identificeert gaps en verbeterpunten. Bovendien laat het de organisatie en de mensen wennen aan het principe van een audit, wat het verloop van de audit sneller en gemakkelijker maakt.

8 Volg aanbevelingen uit eerdere audits op

Punten die in eerdere (interne) audits (zoals ISO of SOC2 type1) zijn geïdentificeerd, dienen te worden ***verzameld*** en te worden ***geëvalueerd***. De organisatie zal niet iedere aanbeveling kunnen of willen opvolgen. Dat is valide zolang maar duidelijk is dat hierin tijdens de evaluatie een gemotiveerde keuze is gemaakt.

9 Leg een dossier aan

Verzamel documentatie en voorbeelden van bestaan in een ***digitaal dossier***. Voorbeelden van bestaan komen meestal in de vorm van screenshots, tickets of andere zichtbaar uitgevoerde acties. De beste manier om deze documenten te ordenen is een verwijzing te maken naar het relevante criteriumnummer in de bestandsnaam of een mappenstructuur aan te leggen met mapnamen corresponderend aan de criteriannummers.

10 Zorg voor beschikbare kennis

De normen raken verschillende vakgebieden, team en afdelingen binnen een organisatie. De IT-Auditor zal daarom onder meer interviews willen houden met verantwoordelijken voor HR, directie, development en operations. Tijdens het plannen van de audit is het van belang dat deze verantwoordelijken beschikbaar zijn voor ***interviews*** en ***walkthroughs***. Overleg eventueel met de IT-auditor hoeveel tijd nodig is per vakgebied, zodat je een detailplanning kunt maken.