SSC Audits

Wat is een SSC-Audit?

Een Shared Service Centrum IT audit is een manier om de organisatie, de governance, het applicatielandschap, de infrastructuur, en met name de kwaliteit van de beheersing van de IT van een SSC te beoordelen. Door de verdergaande digitalisering is continue monitoring essentieel. Daarom is een periodieke herhaling van een SSC-audit van groot belang: iets dat goed is, moet ook goed blijven.

Wat is het probleem?

Een SSC krijgt bij de oprichting mee dat het allemaal goedkoper moet: applicatiesanering, werken in de cloud, flexibel en mobiel werken, en met minder medewerkers is dan het verhaal. Het SSC moet simpelweg sneller, hoogwaardiger en tevens goedkoper werken dan de samenstellende IT-afdelingen daarvoor deden.

Aan de andere kant gaan de ontwikkelingen in de IT erg snel. Taken worden gedecentraliseerd, IT-functies worden samengevoegd, er wordt veel meer thuis en mobiel gewerkt en uitbesteding is aan de orde van de dag. Steeds meer processen worden stukje bij beetje verder gedigitaliseerd. Daarnaast nemen de bedreigingen sterk toe: hacks zijn aan de orde van dag en het regent ransomware aanvallen. Het SSC groeit organisch tot een steeds grotere organisatie, waarbij de IT alsmaar complexer wordt terwijl gebruikers in de praktijk steeds hogere eisen stellen. Steeds meer verschillende diensten worden toegevoegd. Steeds meer deelnemers sluiten zich aan en worden aan het bestaande netwerk toegevoegd.

Overzicht houden wordt steeds lastiger. Het gaat overal piepen en kraken. De koppelingsproblematiek wordt niet opgelost maar alsmaar ingewikkelder. Voormalige collega's zien het SSC als een leverancier en stellen zich anders op. Belangen van shared service centra en opdrachtgevers gaan onvermijdelijk uiteenlopen. Wat moet je als directie? Om je dienstverlening te kunnen beheersen moet je investeren in je mensen, in je bedrijfsmiddelen, je serverpark en je beheersinstrumentarium. Kortom de beheersing van de IT-processen komt steeds meer onder druk te staan. Dit heeft niet alleen gevolgen voor de performance, het personeel, de klanttevredenheid en de effectiviteit maar ook voor de informatiebeveiliging.

In de praktijk constateren we dan ook dat de performance onder druk staat door een niet adequaat ontworpen active directory die veel te veel bijgevoegde trusts kent en dat er veel schort aan het opleidingsniveau van o.a. de beheerders. *State of the art* tooling vereist *state of the art* medewerkers en niet alles valt op te lossen met inhuur. We zien dat fileshares en databases tussen deelnemers niet goed gescheiden zijn, dat het netwerk onvoldoende is gesegmenteerd waardoor ransomware vrij spel heeft, dat de OTAP-straat onvoldoende is doordacht, dat servers onveilig zijn geconfigureerd en dat de IT-infrastructuur slecht is gehardend. We zien dat contractmanagement niet op orde is omdat veel contracten bij de deelnemers achtergebleven zijn. Wachtwoordrestricties voor admins worden niet goed toegepast en systeem-/netwerkbeheerders moeten een veelheid aan admin accounts gebruiken. We zien dat programma's voor handige eindgebruikers te starten zijn waar dat niet de bedoeling is.

Het ergste is dat zich een "welles-nietes" spel tussen de directie van het SSC en het management van de deelnemers ontwikkelt over de kosten en kwaliteit van de dienstverlening, dat indgebruikers klagen over de gebrekkig geworden dienstverlening van het SSC en dat personeel van het SSC wegloopt vanwege de slechte sfeer waardoor de afhankelijkheid van inhuur soms tot extreme hoogte stijgt.

SSC Audits

Wat kunnen wij u bieden?

Wij kennen de markt, de situatie waarin u zich als deelnemer of als SSC bevindt, en weten waar u tegenaan loopt. Wij combineren kennis van uw bedrijfsprocessen met onze ervaring als IT-auditor. BKBO is aangesloten bij de Nederlandse Organisatie van Register EDP-auditors (NOREA) en wij hanteren de gedragsregels van de Register EDP-auditor (RE): NOREA Code of Ethics voor de IT-auditor.

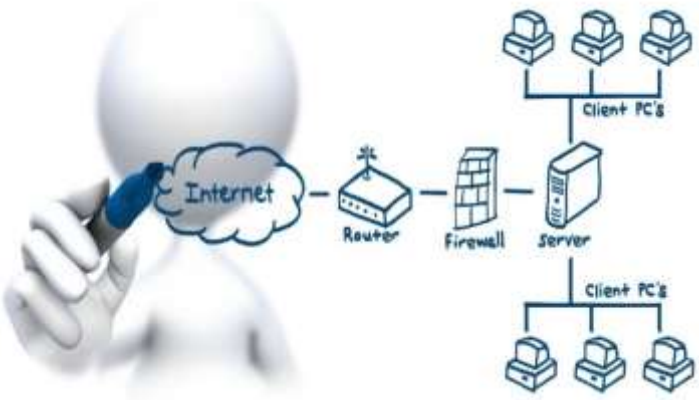
Met een SSC-audit krijgen het SSC en haar opdrachtgevers:

- Zicht op de technische en organisatorische kwetsbaarheden. Wij reiken u maatregelen aan om deze te beheersen;
- Betere dienstverlening door een analyse van de IT-processen in relatie tot de best practices van ITIL® waardoor de efficiency en de effectiviteit naar de deelnemers beter op orde kan worden gebracht;
- Betere kwaliteit van de geleverde diensten en gegevens doordat het netwerk, de infrastructuur en de databases kritisch worden geanalyseerd waardoor u maatregelen kunt nemen om de integriteit van gegevens te verbeteren;
- Een algeheel hoger niveau van informatiebeveiliging.

Hoe pakken wij dat aan?

We beginnen met een afbakeningsfase. Hierin worden afspraken gemaakt over doel, scope en diepgang van de audit. Ook stemmen we het te hanteren normenkader af, tenzij dit reeds is voorgeschreven.

Na de vaststelling van de scope leggen we onze werkzaamheden vast in een auditplan. U stelt als opdrachtgever een vaste contactpersoon aan bij wie de auditor voor de verdere voorbereiding en uitvoering kan aankloppen. Daarna leveren wij u een lijst aan met de benodigde bewijsstukken. Nadat deze stukken door u aan ons beschikbaar zijn gesteld, start de documentenstudie. Vervolgens vindt de audit plaats op locatie. We starten met een gezamenlijke kick-off.



Hierna volgen diepte-interviews voor de setting, de governance en de processen. Incident en problem management, access management, servicedesk en contractbeheer spelen daarbij een rol, maar ook security, configuratie, availability en release management. We nemen de gehele ITIL v3 bibliotheek door. Tegelijkertijd doen we netwerkscans op uw active directory en uw wifi, en vulnerabilityscans op uw complete infrastructuur en we onderzoeken de segmentering en de hardening en de scheiding op het niveau van fileshares, exchange en databases. Door onze jarenlange auditexpertise en actuele kennis hebben wij slechts twee à drie dagen nodig om samen met u de situatie te bekijken. Na de audit houden we een slotbijeenkomst om onze eerste bevindingen aan u kenbaar te maken.

We analyseren op kantoor de uitkomsten en formuleren de bevindingen en afwijkingen. Vervolgens stellen wij een conceptrapportage op. Deze leggen we aan u voor in een gezamenlijke eindbespreking. We nemen de risico's door en we lichten onze aanbevelingen toe. De resultaten van het eindgesprek worden vervolgens door ons verwerkt in een eindrapportage voor het SSC en de deelnemers.

We stellen feiten onweerlegbaar vast en leggen daarmee de vinger op de zere plek. We hebben er geen belang bij uw kwetsbaarheden of organisatieproblemen te vergroten om een adviesopdracht daarna zo groot mogelijk te maken. We hebben geen dubbele agenda. We stellen feiten vast en doen geen advieswerk. We staan voor de kwaliteit van onze bevindingen en onze rapportage en presenteren dezelfde feiten aan zowel SSC als

deelnemers., met gerichte aanbevelingen zodat de problemen kunnen worden aangepakt. Het jaar erop komen we graag weer terug om op basis van dezelfde normen objectief de voortgang te meten.

IV-audit

Omdat de prestaties van een SSC direct afhankelijk zijn van de volwassenheid van het opdrachtgeverschap van de deelnemers, ligt het voor de hand dat we de kwaliteit van de aansturing door de deelnemers gelijktijdig onderzoeken. Daarbij staan de kwaliteit van het demand management en het functioneel applicatiebeheer voorop. Naarmate deelnemers beter kunnen omschrijven welke ICT-dienstverlening men wanneer nodig heeft, kan het SSC projectmatig werken in plaats van "hap snap". Naarmate functioneel beheerders beter beheer doen, worden de mogelijkheden van bestaande informatiesystemen beter benut, beter getest en voorspelbaarder. En ook het onderlinge begrip stijgt over en weer.

Wat is uw investering?

Afhankelijk van wat u wilt dat onderzocht wordt, en de zekerheid die u daar als opdrachtgever aan wilt ontlenen, variëren de kosten. De keuze voor BKBO is een keuze voor kwaliteit. We doen u een voorstel waarbij we de SSC-audit elk jaar zullen herhalen om de voortgang objectief te kunnen meten. We combineren het SSC assurance onderzoek graag met infra- en netwerkscans en pentesten van onze partner Defenced.

Wilt u meer weten?

Als u meer wilt weten van dit product dan staan wij voor u klaar. Wij gaan graag met u in gesprek om tot een definitieve offerte te komen. U kunt direct bellen met BKBO op het telefoonnummer: 073 – 211 03 37.

U kunt ook direct een offerte aanvragen. Ga naar:
https://bkbo.nl/producten/overige-it-audits/

We komen graag met u hierover in contact.