IT Audit Essentials™
Onmisbaar voor uw controle én dossier!

Belang van IT voor de controle
De IT-systemen van uw klanten zijn van invloed op uw controle. Bijvoorbeeld voor het bepalen van het (pre)auditrisk en de aanpak en uitvoering van de controle.

Om voldoende zekerheid te krijgen dat de jaarrekening geen afwijkingen van materieel belang bevat, is het in geautomatiseerde omgevingen, al snel noodzakelijk 'het informatiesysteem' te onderzoeken .

De praktijk
Ondanks deze noodzaak, blijkt in de praktijk, dat het onderzoeken van 'het informatiesysteem' maar beperkt of zelfs geen aandacht krijgt. Oorzaken zijn onder meer het ontbreken van kennis, ervaring en hulpmiddelen.

Het inschakelen van een IT-auditor past bovendien meestal niet in het budget. Zeker niet in de tijd waarin het controlebudget toch al onder zware druk staat. Toch wordt verwacht dat u, in relevante situaties, onderzoek verricht (NVCOS 315).

Onvoldoende aandacht brengt niet alleen risico's met zich mee maar u mist ook kansen om de dienstverlening aan uw klant te verbeteren.

IT Audit Essentials™
Om u hierin te ondersteunen is het webbased self-assessment IT Audit Essentials™ ontwikkeld.

In dit assessment zijn onze jarenlange ervaringen met en kennis van IT Audits in de controlepraktijk op een praktische en doeltreffende manier bij elkaar gebracht.

De uitkomsten van het assessment geven inzicht in de IT-omgeving en de beheersmaatregelen die zijn getroffen. Hiermee beschikt u over een gestructureerde basis om mogelijke risico's te bepalen en de aanpak van de controle hierop af te stemmen. Tevens beschikt u direct over noodzakelijke informatie voor uw dossier.

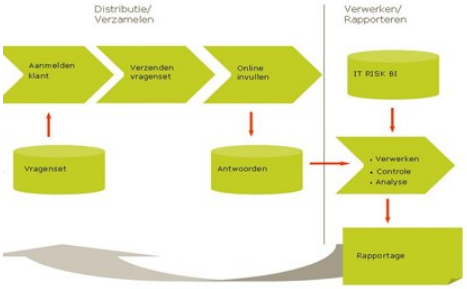
AVG
In het assessment IT Audit Essentials is ook een paragraaf opgenomen met vragen over de Algemene verordening gegevensbescherming (AVG). Immers het niet voldoen aan deze regelgeving kan mogelijk negatieve gevolgen hebben. Bijvoorbeeld financieel of reputatieschade.

Cyber security Healtcheck
Ook is de NBA Cybersecurity Check opgenomen. De check is een hulpmiddel om inzicht te krijgen in de staat van cyberbeveiliging bij de klanten van de accountant. De Health Check is op verzoek van de Cyber Security Raad ontwikkeld door vier grote accountantsorganisaties.

Volgens de NBA kunnen accountants een belangrijke bijdrage leveren aan de bewustwording van de klantorganisaties ten aanzien van digitale risico's. Voor de accountant biedt de Health check handvatten om het gesprek over cybersecurity aan te gaan. De accountant is immers wettelijk verplicht een oordeel te vellen over de betrouwbaarheid en de continuïteit van de ICT-systemen in een organisatie.

Door het assessment kunt u op een pragmatische manier invulling geven aan de oproep van de NBA om Cybersecurity onder de aandacht van uw klanten te brengen.

Hoe het werkt
Onderstaand schema toont globaal de werking.



Over de uitvoering van dit proces hoeft u zich geen zorgen te maken. Het proces wordt geheel door ons uitgevoerd. Het enige dat u hoeft aan te leveren zijn de contactgegevens en het email-adres van uw klant.

Uw klant ontvangt van ons een persoonlijke uitnodiging voor het invullen van het self-assessment via een beveiligde verbinding, wij bewaken de invulling en rapporteren de resultaten aan u, nadat de klant het invullen heeft afgerond.

Een voorbeeld van de rapportage vindt u op onze website.

De voordelen
Het assessment geeft invulling aan de behoefte om doeltreffend en doelmatig inzicht te krijgen in de kwaliteit van de IT-omgeving bij uw klanten, risico's te identificeren en daarmee rekening te houden met de aanpak van de controle.

Het assessment neemt de barrière weg tussen de noodzakelijke behoefte en de praktische belemmeringen. Voordelen zijn onder andere:
- Gestructureerd en gedocumenteerd inzicht in aandachtspunten en risico's;
- Betere afweging aanpak controle;
- Laagdrempelig en kosteneffectief;
- Geen kostbare inzet van eigen medewerkers nodig.

Aan het resultaat herkent u onze toegevoegde waarde!!
www. ITRiskControl.nl

De aanpak

Zet voorafgaand aan de interim het assessment in om een gestructureerd beeld te krijgen van de IT-omgeving, mogelijke aandachtspunten en risico's bij de controle. Aan de hand hiervan kunt u gericht vervolgstappen bepalen en doelgericht te werk gaan.

Een lage investering met een hoog rendement.
Alleen al het nadenken en intern bespreken over 'Wat te doen met de IT-omgeving van een klant?' kost al vele malen meer dan de kosten van een assessment.

En dan moet het werk nog worden gedaan!

Meer informatie

Wilt u ook op een praktische en doelmatige wijze voorzien in uw behoefte? Neem dan contact op met ons:

IT Risk Control b.v.
Gareelhoek 54
7546 MZ Enschede

Telefoon: + 31 (0) 6 53 94 84 79
Of mail naar info@itriskcontrol.nl