Gecombineerde audit

Een efficiënte aanpak verlaagt uw auditdruk

Introductie

Zo, u heeft als security officer of information risk manager de organisatie net door een audit geloodst. Langdurige gesprekken met auditoren die moeilijke en belangrijke vragen stelden. Het zijn lange en intensieve dagen geweest. Gelukkig zit de ISAE 3402 audit of de SOC 2 audit er voor dit jaar weer op! Op naar de ISO 27001 audit. Deze staat namelijk voor volgende week gepland. Met veelal dezelfde onderwerpen, vragen en gelijksoortige documentatie.
Dat kan slimmer, toch?

Wij zien als auditoren van Grant Thornton en BSI dat er vaak overlap zit in de scope voor ISAE 3402/SOC 2 en ISO 27001 audits. Met het planmatig combineren van deze audits en het stroomlijnen van de scope voor wat betreft de ISAE 3402/SOC 2 en ISO-normen maken organisaties een efficiencyslag. Dit verlaagt de auditdruk. Daarnaast versterken de auditoren voor beide onderzoeken elkaar. Typisch een geval van één en één is meer dan twee!

Zo droeg de samenwerking tussen Grant Thornton en BSI al bij meerdere organisaties bij aan het versnellen en verbeteren van het audittraject.

Welke eigenschappen en voordelen biedt de gezamenlijke aanpak van Grant Thornton en BSI u? Wij geven u in dit whitepaper een helder overzicht van de overlap tussen de beide audits. Daarnaast neemt Jorg Voeten van CM.com u mee in zijn ervaring met de gecombineerde audit van Grant Thornton en BSI.

Wat zijn uw voordelen bij een gecombineerde audit?

Efficiency in het plannen van auditdagen
De gelijktijdige interviews leveren u tijdswinst op. Daarnaast verzamelt u eenmalig benodigde informatie en documentatie voor de gecombineerde auditdagen in plaats van verdeeld over verschillende momenten in het jaar.

Verminderde druk op de organisatie vanuit audits
Medewerkers uit uw organisatie zijn voorbereid op de gecombineerde auditdagen. Voor hun planning biedt dit zekerheid en rust. De auditoren komen op dezelfde momenten gezamenlijk over de vloer.

Gedeeld vertrekpunt van auditoren
De auditoren van Grant Thornton en BSI zijn op de hoogte van elkaars auditaanpak. Dit zorgt voor een efficiënter auditproces en een completer overzicht van uw organisatie als het gaat om informatiebeveiliging.

Implementatie ISAE 3402/SOC 2 & ISO 27001
Grant Thornton en BSI komen beiden met onafhankelijke eindrapportages. Doordat de auditoren van elkaar weten waar hun expertise ligt, profiteren zij van elkaars deskundigheid. Beide organisaties zullen u binnen hun vaktechnische ruimte voorzien van aanbevelingen voor het realiseren van verdere verbeteringen. De adviezen kunt u binnen uw organisatie implementeren. Daarvan heeft u in volgende auditcycli profijt.

Een gecombineerde eindpresentatie
De eindpresentatie van de gecombineerde bevindingen voedt uw verbeteragenda en helpt u organisatieprocessen nog beter in te richten. Dit zorgt voor consistent en duurzaam beheer van informatiemanagement.

Basics over ISAE 3402, SOC2 en ISO 27001

Wat bereikt u met ISAE 3402?
De International Standard on Assurance Engagements (ISAE 3402) richt zich op de kwaliteit van de dienstverlening en het beheersen van de risico's in processen die u namens uw opdrachtgevers uitvoert.

Met een ISAE 3402-rapport legt u als serviceorganisatie verantwoording af aan uw klanten over de beheersing van de processen die uitvoert, voor zover deze processen en diensten impact hebben op de financiële verslaggeving van uw klanten (de gebruikersorganisaties).

U toont als serviceorganisatie met een ISAE 3402-rapport aan hoe u de kwaliteit, risicobeheersing en compliance binnen de uitbestede processen waarborgt. De ISAE 3402-standaard biedt u de ruimte om op basis van uw eigen scopebepaling en ingeschatte risico's de inhoud van de verantwoording te bepalen.

Houd daarbij wel rekening met de informatie- en assurancebehoefte van uw gebruikers aan wie u de rapportage verstrekt.

Wat bereikt u met SOC 2?
De System and Organization Controls Reporting (SOC 2)-standaard van het American Institute of Certified Public Accountants, is een andere auditstandaard met een vergelijkbaar doel.

Deze standaard is gericht op het bieden van zekerheid door u als serviceorganisatie aan uw gebruikersorganisaties over de kwaliteit van dienstverlening en risicobeheersing voor de processen die namens opdrachtgevers uitvoert en die geen rechtstreekse impact hebben op de financiële verslaggeving bij uw gebruikers. Denk hierbij aan cloud services en andere IT-diensten van serviceproviders. Net als ISAE 3402 is SOC 2 een standaard voor het informeren van en verantwoorden aan uw externe stakeholders.

Het grootste verschil is dat de scope van een SOC 2-rapport betrekking heeft op informatiebeveiliging, privacy, beschikbaarheid, vertrouwelijkheid en integriteit van data en niet direct op de financiële aspecten.

Wat bereikt u met ISO 27001?
De internationaal norm voor informatiebeveiliging (ISO 27001) helpt organisaties met het procesmatig inrichten en beveiligen van informatie en data.

Door deze systematische aanpak wordt informatiebeveiligingsmanagement volledig geïntegreerd in uw organisatie. Informatiebeveiliging raakt elke afdeling van de organisatie, tot aan uw klantbestand en financiële data. Een datalek is voor bedrijven en hun stakeholders erg vervelend. Dankzij een gedegen informatiebeveiligingsbeleid (volgens ISO 27001) verkleint u de datarisico's en beschermt u de reputatie van uw organisatie. Tevens voldoet een ISO 27001 certificering aan de wet-en regelgeving op gebied van informatiebeveiliging.

Het informatiebeveiligingsbeleid kan per organisatie verschillen, zo legt uw informatie- en databeveiliging nog scherper vast met specifieke normen zoals dataprivacymanagement (ISO 27701) en informatiemanagement in de zorg (NEN 7510).

Ervaring uit de markt

Grant Thornton en BSI zijn al gestart met het aanbieden van de gecombineerde audit voor ISAE 3402/ SOC2 en ISO 27001. Zo wilde het beursgenoteerde CM.com de organisatie efficiënter laten auditen. CM.com is een internationale aanbieder van cloud software en commerciële communicatie, met deze service faciliteert CM.com een uitstekende klantervaring voor hun opdrachtgevers.

Na het vaststellen van de scope werd duidelijk dat een gecombineerde audit voor alle partijen mogelijk was. CM.com laat zich certificeren tegen drie ISO-schema's op het gebied van informatiebeveiliging:

- ISO 27001
- ISO 27017
- ISO 27018

Daarnaast verstrekt CM.com een ISAE 3402-rapport aan haar klanten voor de payments dienstverlening. In de aanloop naar de certificering werkten de professionals van Grant Thornton en BSI nauw samen met Robin Zegwaart, Risk Manager Payments en Jorg Voeten, Lead Risk & Compliance bij CM.com. Al snel bleek dat de constructieve en pragmatische insteek van de gecombineerde audit aansloot op de kwaliteitseisen van CM.com. Volgens Jorg Voeten is een van de voordelen de consistentie tussen de standaarden: "De normenkaders staan met elkaar in lijn, aangezien het normenkader voor de ISAE 3402 verklaring gebaseerd is op de ISO standaarden."

De gecombineerde audit biedt naast inhoudelijke voordelen op het gebied van informatiebeveiliging en kwaliteit, ook efficiëntie op organisatorisch vlak. "De uren van medewerkers zijn kostbaar. De gecombineerde audit zorgt ervoor dat deze uren efficiënter gepland worden en dat de dagelijkse werkzaamheden zo goed mogelijk doorliepen", aldus Jorg Voeten.

Lees de case study van CM.com en hun certificeringen bij BSI

Meer weten?
Wilt u meer weten over de gecombineerde audit van Grant Thornton en BSI? Neem contact op met BSI via +31 (0)20 346 0780 of Grant Thornton via +31 (0)88 676 9000.

Of lees hier meer over ISAE 3402 en SOC 2 en ISO 27001.

Hoe verloopt het gecombineerde traject?

01

Voortraject
Past de werkwijze bij alle partijen? Dan maken we normenkaders passend voor uw organisatie. Voldoet het normenkader aan de kwaliteitswensen van uw organisatie, dan denken we na over de optimalisaties.

* Let op: dit gaat in op 'wat' we implementeren, niet op 'hoe'.
Een 0-meting of pre-assessment helpt om dit nog scherper te definiëren.

02

Planning
Gezamenlijke planning, inclusief momenten waarop auditoren op locatie zijn en wanneer relevante informatie beschikbaar is.

03

Uitwerking
We werken het documentatieverzoek uit. Ook al wordt er voorafgaand aan de ISO 27001 geen documentatie opgevraagd, maken we wel gebruik van documentatie en bewijsstukken voor een ISAE 3402 audit, voor het deel van de scope dat dekkend is voor de ISO 27001 audit.

04

Uitvoering
We nemen interviews af met de verschillende proceseigenaren, waarbij een ISO-auditor en ISAE 3402-/SOC 2-auditor deelnemen. Zo voeren deze proceseigenaren eenmalig gesprekken en lichten ze eenmalig de bewijsstukken toe. Dit scheelt hen veel tijd in de overvolle agenda's.

05

Rapportage
BSI stelt het ISO-certificaat op en Grant Thornton een ISAE 3402- of SOC 2-rapport.

06

Eindpresentatie
In de eindpresentatie kijken we samen met u naar potentiële verbeteringen die we hebben gesignaleerd tijdens de gecombineerde audit. Zo krijgen uw processen een optimalisatie-/efficiëntieslag.

Hoe helpt Grant Thornton u?

De professionals van Grant Thornton bieden u hoogwaardige dienstverlening op gebied van o.a. accountancy en financieel advies, audit en (third party) assurance, belastingadvies, sustainability & impact services en cyber risk services. Wij kijken pragmatisch en proactief naar uw uitdagingen en wisselen daarbij vaak kennis en expertise uit met andere leden uit ons onafhankelijke wereldwijde netwerk.

We voorzien u graag in en adviseren u graag bij uw ISAE 3402- en SOC 2-audits. We zien veel organisaties die zich op zowel ISAE 3402/SOC 2 als ISO 27001 laten auditen. Deze standaarden verschillen in aard, omvang en diepgang, maar er is veelal ook overlap binnen deze auditprogramma's. Daardoor onderzoeken we binnen de audittrajecten vaak dezelfde onderwerpen.

"De bewijslasten uit ISAE 3402-audits en ISO 27001-audits komen voor een (groot) overeen, terwijl auditoren op andere momenten deze informatie bij de organisatie opvragen. Het is voordeliger en efficiënter om die meetmomenten te combineren. Onze aanpak tijdens een audittraject blijft hetzelfde en het eindresultaat is een assurance rapportage., maar wij beperken de auditdruk op uw organisatie.'"
Jeffrey Martens en Christiaan Dommerholt, Grant Thornton

Hoe helpt BSI u?

De auditoren van BSI houden uw processen voor informatie- en databeveiliging constant tegen het licht. In welke sector uw organisatie zich ook bevindt, BSI heeft als wereldwijde certificeringsinstelling al sinds 1901 ervaring met het implementeren van standaarden in bijna alle sectoren en loopt voorop in en is betrokken bij het ontwikkelen van normen, zoals bij het ontstaan van ISO 27001, de norm voor informatiebeveiliging. Informatiebeveiliging en databeveiliging zijn voor het risicomanagement van uw organisatie belangrijker dan ooit. Onze auditoren ontdekten dat veel dienstverlenende organisaties naast ISO 27001 behoefte hebben aan ISAE 3402- of SOC 2-auditrapport. Omdat BSI zelf geen ISAE 3402 of SOC 2 dienstverlening aanbiedt, is het een logische stap om organisaties samen met Grant Thornton in deze behoefte te voorzien.

"Zowel qua tijd en geld als auditervaring is deze manier van werken het beste van twee werelden. U krijgt op hetzelfde moment twee professionals die uw bedrijfsprocessen onder de loep nemen. Dat is een geweldige efficiëntieslag. Dankzij de internationale oriëntatie van beide organisaties voeren we dit ook eenvoudig door bij uw andere Europese filialen."
Ismail Sarica, ISO 27001 auditor bij BSI

Neem contact met ons op
www.bsigroup.com
+31 (0)20 346 0780