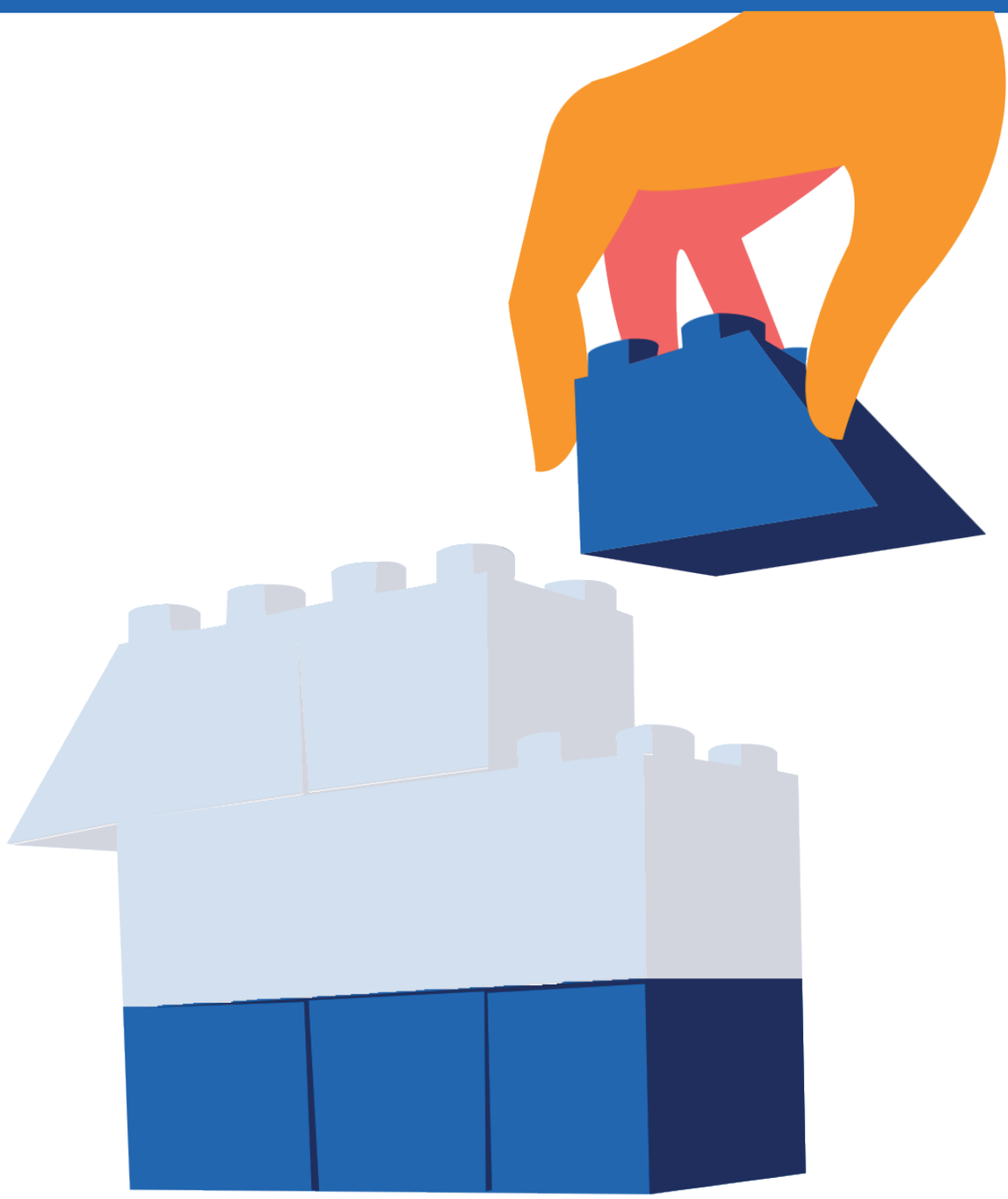
Audittrail
information security | privacy | quality | grc

BIC Building Blocks
Control & Audit



INFORMATIEBEVEILIGING MEETS AUDIT & CONTROLE

'Je weet nooit of u uw werk goed doet zonder een mate van controle'

De bovenstaande uitspraak geeft aan dat controle en audit niet per se vervelend of lastig hoeft te zijn. Niet alleen vinden veel collega's een controle eigenlijk best prettig, het is ook een noodzakelijk onderdeel van de PDCA. Plan, Do, Check, Act. Zonder checken is er geen bijsturing mogelijk en wordt informatiebeveiliging een ongeleid projectiel. We weten niet of iets werkt en of het überhaupt nut heeft wat we doen. Dus dat kan een duur grapje worden.

Een aantal redenen om te auditeren:

- Omdat u het wilt. De Informatiebeveiligings-maatregelen treft u omdat u een bepaald risico wilt verminderen. En u wilt wel zeker weten dat a. de IB-maatregelen het risico vermindert en b. de maatregel ook echt werkt. Zo niet, dan zal u moeten bijsturen om de maatregelen te laten werken of een nieuwe implementeren;
- Omdat je het wil. Sommige controles zijn alsnog handmatig (user controls) en een vier ogen principe is goed om de maatregel te laten werken. Denk hier bijvoorbeeld aan een controle op het toekennen en intrekken van autorisaties;
- Omdat uw management het wil. Ook zij willen weten of de getroffen maatregelen zin hebben en het geen weggegooid geld is. En erger: een gevoel van schijnveiligheid geven;
- Omdat het moet. De accountant baseert bijvoorbeeld het oordeel aangaande de jaarrekening voor een deel op basis van de juistheid, volledigheid, tijdigheid en rechtmatigheid van de financiële administratie. En daar zitten nogal wat onderwerpen in aangaande informatiebeveiliging. Zonder dat, geen goedgekeurde jaarrekening.

In deze whitepaper maken we onderscheid in controles en audits. De controles zullen veelal in de eerste lijn plaatsvinden en de audits veelal in de tweede of derde lijn.

Wie gaat auditeren of controleren?

Een audit is volgens de definitie: '*een onafhankelijk en objectief onderzoek over een specifiek onderdeel, proces of organisatie op basis van een norm, waarbij een oordeel gevormd wordt*'.

Hoe u een auditproces inricht valt buiten de scope van deze whitepaper. Het advies is om bij de auditcharter van de interne auditfunctie aan te sluiten.

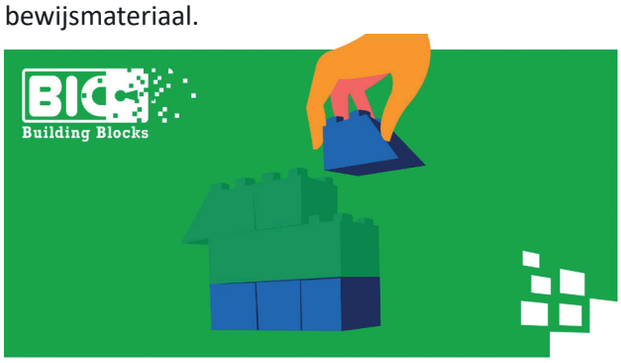
De 'three lines of defense' is een veel gebruikte systematiek in de corporatiesector. En daarmee ook het meest eenvoudig uit te leggen en toe te passen. Hierin heeft de medewerker een rol, de interne auditafdeling en de externe auditor. De laatste kan de accountant zijn, maar ook een andere, onafhankelijke en gespecialiseerde auditor.

Omdat u wilt zorgen dat u als organisatie ‘in control’ bent, wilt u de focus wel leggen op de interne audit (de eerste en tweede lijn). Veelal is deze functie al aanwezig binnen de organisatie. Deze moet dan wel in staat zijn, of worden gesteld om ook IT-audits en IB-audits uit te voeren. Let wel: natuurlijk kan de interne auditafdeling zich op bepaalde punten laten ondersteunen door een externe.

De controles zijn veelal operationeel van aard. Denk daarbij aan de check op het toekennen van autorisaties, het doorvoeren van wijzigingen op basis van de personeelslijst en de wekelijkse check op autorisatie incidenten. Deze controles zijn ook maatregelen op zichzelf.

Wat gaat u auditen, normenkader en aanpak

Idealiter audit u de complete BIC (de ‘norm’ in de definitie). Dat begint dus met een periodieke audit op uw beleid (voldoet het beleid, is het up-to-date, is het nog steeds ‘passend’) en het risicomanagement(proces) (zijn de risico’s op een juiste wijze geïnventariseerd, zijn deze nog steeds valide, zijn de risico’s recent nog beoordeeld?). Van daaruit gaat u naar de audit op de maatregelen, voor zover u deze maatregelen hebt geïmplementeerd. Kernvraag: heb je norm adequaat gegeven en heb je het risico daadwerkelijk verminderd. En hoe dan? Dit dient aangetoond te worden met voldoende bewijsmateriaal.



Audits zullen veelal door de tweede en derde lijn uitgevoerd worden. Daarmee zullen zij ook de eerste lijn controleren om zeker te zijn dat erop gesteund kan worden.

Om te komen tot een goed samenstel van audits en controles is een passende aanpak nodig. Deze kan u eenvoudigweg baseren op de normenkader (in dit geval de BIC).

Aandachtpunt is wel dat u ook kijkt naar normen waar u geen maatregelen voor hebt getroffen. Want wellicht is er wat gemist.

Omdat ‘de hele BIC’ nogal omvangrijk is, is het goed om de scope per onderzoek te beperken. Werk daarom met logische blokken die onderzocht worden, bijvoorbeeld de hoofdstukken van de BIC Building Blocks. Ook zal de audit een enorme doorlooptijd vergen als deze te omvangrijk is. Met als negatief bijeffect dat er minder adequaat kan worden bijgestuurd.

Niet ieder hoofdstuk van de BIC of ieder onderwerp hoeft even vaak geaudit te worden. Doe dit op basis van risico.

Audittrail
information security | privacy | quality | grc

AUDITPLANNING EN KALENDER

Het is raadzaam een goede auditplanning te maken. Zo zorgt u ervoor dat elk onderwerp de aandacht krijgt dat het verdiend en dat ‘minder belangrijke’onderwerpen niet vergeten worden. Voordelen van een goede auditplanning ofwel auditkalender:

- U mist geen onderwerpen;
- De onderwerpen komen naar gelang het risico vaker of minder vaak terug;
- De improvement over time (of decline) zijn beter meetbaar;
- Een planning geeft houvast voor alle stakeholders (auditor, auditee, auditcommissie, accountant).

Onderstaand model geeft aan op welke wijze u de planning kunt vormgeven. In de BIC Building Blocks sjablonen vindt u ook een voorbeeld werkwijze.

Auditplanning overzicht

Hoofdstuk	ISO Onderwerp	Per kwartaal	Jaarlijks	Tweejaarlijks	Bij wijzigingen	Laatst uitgevoerd	Uitgevoerd door	Eerstvolgende op	Verantwoordelijk
5	Informatiebeveiligingsbeleid		X			{Geef datum op}	{Geef aan}	{Geef datum op}	{Geef aan}
6	Organisatie van Informatiebeveiliging			X	X	{Geef datum op}	{Geef aan}	{Geef datum op}	{Geef aan}
7	Veilig personeel			X		{Geef datum op}	{Geef aan}	{Geef datum op}	{Geef aan}
8	Beheer van bedrijfsmiddelen	X	X			{Geef datum op}	{Geef aan}	{Geef datum op}	{Geef aan}

Afhankelijk van het risico zal u de planning opstellen.

De periodiciteit van de controles kunnen zijn:

- Dagelijks
- Wekelijks;
- Maandelijks;
- Per kwartaal;
- Per jaar;
- Per twee jaar;
- Bij wijzigingen.

Interne auditor versus externe

Zoals al eerdergenoemd, kunt u de taken verdelen. Onder intern verstaan we in deze whitepaper de interne medewerkers en de interne audit/control functie. Onder extern scharen we de verplichte accountants en toezichthouders. Voor de laatste is het duidelijk welke audits zij uitvoeren.

Natuurlijk is het mogelijk om een audit die onder de vlag van interne audit uitgevoerd wordt door een externe partij uit te laten voeren. Het is vooral goed om dat te doen als:

- De audit een hoge mate van expertise vergt die intern niet aanwezig is (zoals een pentest);
- Het goedkoper is om de audit uit te besteden (sneller werken);
- Er intern geen capaciteit aanwezig is om de audit uit te voeren;
- Een paar nieuwe ogen een verhelderend beeld kan geven.

De externe voert in dat geval een interne audit uit.

Veel succes met het auditprogramma en het uitvoeren van de controles en audits!

Audittrail
information security | privacy | quality | grc

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AE Leiderdorp

KantNoord
Winschoterdiep 50
9723 AB Groningen

071 - 747 71 71
BBB@audittrail.nl

Audittrail
information security | privacy | quality | grc