|  |
| --- |
| Template Toetsing[Ondertitel] |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |
|  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (piramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Beleid in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | GO.05; |
| ISO27001 |  |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc150775042)[1 Inleiding 5](#_Toc150775043)[2 Hoofdlijnen 6](#_Toc150775044)[2.1 Drie lijnen 6](#_Toc150775045)[2.2 Toewijzing 6](#_Toc150775046)[2.3 Audit door audits 7](#_Toc150775047)[3 Audit-proces 8](#_Toc150775048)[3.1 Auditjaarplanning 8](#_Toc150775049)[3.2 Auditplanning 8](#_Toc150775050)[3.3 Auditwerkzaamheden 8](#_Toc150775051)[3.4 Afronding van een audit 9](#_Toc150775052)[3.5 Rapportage 9](#_Toc150775053)[4 Resultaten 10](#_Toc150775054)[Vaststelling 11](#_Toc150775055) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

[INSTELLING] hanteert drie lagen van toetsing over de beheersing van onder andere informatiebeveiliging.

De eerste laag is de zelftoetsing die in de eerste lijn plaatsvindt, door medewerkers zelf en hun managers.

De tweede laag van toetsing bestaat uit toetsing en toezicht dat door de tweede lijn wordt uitgevoerd op de eerste en tweede lijn. Voor informatiebeveiliging is hiervoor de [CISO] aangewezen.

[INSTELLING] wenst op de derde laag onafhankelijk te worden getoetst over de algehele status van interne beheersing in de organisatie. Hiertoe heeft zij een Audit-functie (Internal Audit of een interne, relatief-onafhankelijke functie, al of niet ondersteund door externe auditors) met taken en bevoegd­heden als vastgelegd in het Audit Charter. Tevens maakt [INSTELLING] gebruik van externe auditdiensten, onder andere ten behoeve van de controle op de jaarrekening van [INSTELLING].

Dit document beschrijft deze drie lagen, waaronder hoe medewerkers en andere betrokkenen van [INSTELLING] in hun werk met betrekking tot informatiebeveiliging interacteren met de Audit-functie. Tevens staat hierin genoemd hoe de Audit-functie kan worden verwacht op te treden voor, tijdens en na audits, zodat auditees in de samenwerking of de uitkomsten niet voor verrassingen komen te staan.

# Hoofdlijnen intern toezicht en toetsing

## Drie lijnen

[INSTELLING] heeft voor de uitvoering van organisatiebreed risicomanagement het ‘3 Lines’-model geadopteerd; zie het document [GOVERNANCE/ORGANISATIE].

## Eerstelijns zelftoetsing en toezicht

In de eerste lijn houden medewerkers zichzelf en elkaar scherp op afwijkingen van overeenge­komen procedures en regels. Tevens houden managers, hoofden van afdelingen en dergelijke, toezicht op de juiste naleving van procedures en regels conform de Plan-Do-Check-Act-cyclus van [INSTELLING].

## Tweedelijns toezicht

[INSTELLING] heeft toetsing en toezicht op de uitvoering van informatiebeveiligingstaken in de eerste en tweede lijn neergelegd bij de [CISO], conform de Plan-Do-Check-Act-cyclus van [INSTELLING].

## Derdelijns toezicht

[INSTELLING] heeft voor het toezicht in de derde lijn op de eerste en tweede lijn een Audit-functie, (Internal Audit of een interne, relatief-onafhankelijke functie, al of niet ondersteund door externe auditors) met taken en bevoegd­heden als vastgelegd in het Audit Charter; hierna aangeduid als Interne Audit. Tevens maakt [INSTELLING] gebruik van externe auditdiensten, onder andere ten behoeve van de controle op de jaarrekening van [INSTELLING].

# Hoofdlijnen Audit

## Drie lijnen

[INSTELLING] heeft voor de uitvoering van organisatie-breed risicomanagement het ‘3 Lines’-model geadopteerd.

De ‘derde’ lijn is de interne audit-functie die door middel van risico-gebaseerde audit(jaar)­planningen en audits, onafhankelijk verslag uitbrengt over het functioneren van de eerste twee lijnen in deze. Dit doet de auditfunctie door middel van rapporten met bevindingen en aanbevelingen. De derde lijn onderhoudt ook reguliere contacten met de Raad van Toezicht, en met externe auditors en inspectiediensten en dergelijke om dubbel werk en dubbele belasting van auditees te voorkomen;

## Toewijzing

Voor *informatie*-risicomanagement en informatiebeveiliging heeft [INSTELLING] afdeling Interne Audit aangewezen als verantwoordelijke voor uitvoering van de derde lijn. Deze adviseert ook het [COLLEGE VAN BESTUUR] bij bovengenoemde besluiten, vaststellingen en acceptaties voor zover deze raken aan informatiebeveiliging, en over besluiten inzake geconstateerde bevindingen en de afhandeling daarvan.

[INSTELLING] heeft het beheer over vooralsnog onafgehandelde bevindingen en aanbevelingen inzake informatiebeveiliging neergelegd bij de [CISO].

## Audit door audits

Audits, leidende tot rapporten met conclusies, bevindingen en aanbevelingen, zijn het primaire middel waarmee auditors verbeterpunten aandragen aan auditees, het [COLLEGE VAN BESTUUR] en de Raad van Toezicht. Deze audits worden door daartoe gekwalificeerde auditors uitgevoerd conform kwaliteits- en procesvereisten die de beroepsgroepen waar zij zijn geregistreerd, dwingend opleggen.

Interne en externe auditors hebben hun eigen audit-jaarplanningen waarin hun werkzaamheden zijn geagendeerd. Van auditors mag worden verwacht dat zij bij hun planning rekening houden met de door de organisatie onderkende risico’s, geaccepteerde tekorten in interne beheersing en in bevinding-oplossingsmogelijkheden, en de agenda’s van te betrekken afdelingen en functionarissen.

Interne en externe auditors hebben formeel recht op toegang tot alle door hen noodzakelijk geachte informatie en personen.

# Audit-proces

Auditen bestaat uit het toetsen van feitelijke situaties aan de relevante normen die de organisa­tie zichzelf heeft opgelegd.

Slechts bij gebreke daarvan kan een auditor voorstellen om normen van buiten te hanteren. Daarbij zal vooraf afstemming met en goedkeuring door de Raad van Toezicht en het [COLLEGE VAN BESTUUR] in samenspraak met de auditee(s) moeten plaatsvinden over het hanteren van die externe normen. De goedkeuring van het [COLLEGE VAN BESTUUR] wordt opgenomen bij het Statement of Applicability. Daarin staat per audit (externe) normen wel, en welke niet, van toepassing zijn op [INSTELLING]. Bevindingen zullen niet als tekorten in uitgevoerd werk van de auditees mogen worden beschouwd maar als mogelijke verbeterpunten waarover opvolgende besluitvorming door of namens de Raad van Toezicht en het [COLLEGE VAN BESTUUR] nodig zijn.

## Auditjaarplanning

Interne auditors hanteren een jaarplanning waarin, op basis van eigen risico-analyses en op verzoek van hoger management, auditobjecten en -aspecten worden ingeschaald op belang­rijkheid van goede interne beheersing en voor komend jaar keuzes worden gemaakt welke audits zullen worden uitgevoerd, gegeven beperkte auditcapaciteit. De auditor houdt bij de spreiding over het jaar van de audits rekening met de jaarkalenders van de auditors zelf en van de auditees zodat de primaire werkzaamheden van de auditees niet onredelijk hoeven worden gestoord. Deze auditjaarplannen worden door de Raad van Toezicht in consultatie met het [COLLEGE VAN BESTUUR] goedgekeurd.

## Auditplanning

Per uit te voeren audit conform de jaarplanning, stelt de auditor een planning van werkzaam­heden op. Hierbij betrekt de auditor de eigen capaciteit en deskundigheid, die van te betrekken collega’s (ook van en voor reeds bekende externe audits), de geeigendheid van de planning in samenhang met de planning en werkzaamheden van de auditees, de uit te voeren detailwerk­zaamheden, de te verzamelen informatie en de te hanteren normen.

De auditor bepaalt tevens op basis van een detail-risicoanalyse per norm welke informatie nodig is om een uitspraak te kunnen doen over de kwaliteit van de getoetste interne-beheersingsmaat­regelen, hoe diepgaand die informatie is, en op welke wijze de informatie dient te worden verkregen. Auditor kan daardoor per informatie-item nauwkeurig aangeven welke toetsnorm gediend is bij het hebben van dat informatie-item.

## Auditwerkzaamheden

De auditor verzamelt de gewenste informatie die deze nodig acht om een uitspraak te kunnen doen over de effectieve opzet, bestaan en/of werking van de getoetste interne-beheers­maatre­gelen. Als de auditor niet kan of wil vertrouwen op reeds in de gangbare processen opgeleverde informatie omtrent die beheersmaatregelen, zal de auditor zelf onderzoek doen.

Het gereedmaken van informatie alleen ten behoeve van de auditor is geen verplichting voor de auditee noch een recht van de auditor. Slechts indien het [COLLEGE VAN BESTUUR] directe opdracht heeft gegeven tot het vervaardigen van die informatie (ook wel PBCs genaamd, Prepared By Client), behoort dat tot het werk van betrokkene als arbeidsrechtelijk opgelegde taak waarvoor impliciet en formeel de benodigde werkuren ter beschikking worden gesteld naast de reguliere werkuren van betreffende betrokkene.

Overigens zal de auditor streven naar samenwerking met auditee(s) voor het verkrijgen van de benodigde informatie, in coördinatie met de [CISO].

Indien een auditor gedurende de audit bevindingen doet die een hoog risico inhouden voor bijvoorbeeld de informatieveiligheid, dan zullen deze onmiddellijk worden doorgegeven aan onder andere betreffende auditees om zo snel mogelijk risico-verminderende maatregelen te treffen.

## Afronding van een audit

De auditor zal bij en na afronding van de werkzaamheden de initiële bevindingen ter controle op juistheid afstemmen met de auditee(s), en opmerkingen en commentaar van auditees opnemen bij de bevinding. Tevens zal de auditor in deze afstemming de haalbaarheid van en beoogde tijd­spanne voor oplossing van de bevinding meenemen.

## Rapportage

De auditor levert een concept-rapport met conclusie(s), verslag van uitgevoerde werkzaam­heden en bevindingen aan de opdrachtgever (de Raad van Toezicht of het [COLLEGE VAN BESTUUR] of andere) en aan alle in het rapport genoemde verantwoordelijken voor oplossing van bevindingen. Eerst na bespreking met auditees en het [COLLEGE VAN BESTUUR] over de juistheid van de conclusie, bevindingen etc., levert de auditor aan bovenstaande een definitief rapport op.

# Resultaten

De [CISO of andere bevindingenregister-toegewezene] ontvangt de bevindingen inclusief aanbevelingen en beoogde oplossingstijden, en voegt deze toe aan het register van bevindingen.

De [CISO of andere bevindingenregister-toegewezene] bevraagt ten minste maandelijks de respectievelijk toegewezen verantwoordelijken voor de status van oplossing van de bevinding, en escaleert indien oplossing niet binnen de beoogde termijn dreigt te slagen. Alsdan zal na overleg [de naasthogere van de CISO / COLLEGE VAN BESTUUR] tot aanvullende oplossings­inspanning, aanpassing van de oplostermijn of acceptatie van het genoemde risico besluiten.

# Vaststelling

Dit beleid is aldus vastgesteld.

[PLAATS], [DATUM].

[HET COLLEGE / DE RAAD VAN BESTUUR].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]