|  |
| --- |
| Procedure Risicobeheer LeveranciersTemplate |

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

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Procedure 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 |  |  |
| [INKOOPBELEID] | x |  |  |
| [STANDAARD KETENBEHEER] | x |  |  |
| [PROCEDURES ‘KETENBEHEER’] |  | x |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001, ISO27002 en ISO28000**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | SC.01, SC.02, SC.03. SC.04 |
| ISO27001 | 4.3, 5.1, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 8.3, 9.1, 9.2, 9.3, 10.1, 10.2,12.6, 15.1, 15.3, 16.1, 17.1 en 18.2 |
| ISO27002 | 5.1, 6.1, 7.2, 7.3, 9.2, 13.2, 15.1, 15.2, 16.1, 17.1, 18.1 en 18.2 |
| ISO28000 | 4.1, 4.2, 4.3, 4.4, 4.5, 5.2, 5.3, 5.4, 6.2, 6.3, 6.4, 8.2, 8.3, 8.4, 8.5, 9.1, 9.2 en 9.3 |

**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

|  |
| --- |
| [1 Inleiding 4](#_Toc185341165)[2 Flowchart met taken en verantwoordelijkheden 5](#_Toc185341166)[3 Toelichting 6](#_Toc185341167) |

# Inleiding

Eventuele inleidende tekst

# Flowchart met taken en verantwoordelijkheden



# Toelichting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stap** | **Verantwoordelijke** | **Omschrijving** | **Document dat je nodig hebt tijdens het uitvoeren van deze processtap**  | **Plek waar je het resultaat van deze processtap archiveert** |
| 1. | CM | In de Levman Jaarkalender staat wanneer het tijd is voor de periodieke review van leverancier gerelateerde risico’s. Eén van de CMs van Levman is verantwoordelijk voor het coördineren van deze periodieke review, de zgn. ‘coördinerende CM’.In essentie beantwoordt de review deze twee vragen: Is de continuering van de dienstverlening of de informatieveiligheid mogelijk serieus/structureel in gevaar? Wat zijn mogelijke mitigaties?  | Levman Jaarkalender |  |
| 2. | CM | De coördinerende CM bepaalt op basis van de afspraken in het Levman Handboek welke leveranciers in deze review worden bekeken. Dit zijn de leveranciers met het hoogste afbreukrisico voor de organisatie. *Let op: Het kan zijn dat een collega CM een van deze hoog risico leveranciers onder zijn/haar hoede heeft. Dan wordt deze collega CM natuurlijk ook bij alle volgende stappen betrokken.* |  |  |
| 3. | CM | De CM die als CM verantwoordelijk is voor de betreffende hoog risico leverancier, vult samen met de Diensteigenaar en de SLM het Leverancier Risicoprofiel in. Ook de gewenste mitigatie acties worden bepaald. Indien nodig worden andere relevante stakeholders betrokken, zoals bijvoorbeeld de productmanager. De coördinerende CM zorgt ervoor dit voor elke in stap 2 geselecteerde leverancier gebeurt. | Template ‘Leverancier Risicoprofiel’  |  |
| 4. | CM | De coördinerende CM plant een meeting met het MT, en alle betrokken Diensteigenaren en CMs.  |  |  |
| 5. | MT | In deze review meeting wordt de status van de Leverancier Risicoprofielen gepresenteerd aan het MT, inclusief de voorgestelde mitigatie acties. Hierbij zijn de betrokken CMs en Diensteigenaren aanwezig. |  |  |
| 6. | MT | Het MT besluit tot het wel of niet nemen van mitigatie acties.Ja 🡪 7Nee 🡪 13 |  |  |
| 7. | CM | De CM zorgt voor een update van elk Leverancier Risicoprofiel n.a.v. de review meeting met het MT. Daarna zorgt hij/zij voor het opvolgen van alle afgesproken mitigatie acties door de relevante stakeholders. De coördinerende CM zorgt ervoor dit voor elke in stap 2 geselecteerde leverancier gebeurt. Hij/zij houdt overzicht over het totaal. |  |  |
| 8. | CM | De CM communiceert regelmatig status updates aan de Diensteigenaar, de SLM, en ook aan de in stap 7 betrokken stakeholders. De frequentie en de manier waarop wordt gezamenlijk bepaald naar eigen inzicht. |  |  |
| 9. | Diensteigenaar | De Diensteigenaar besluit in de loop van de tijd of een mitigatie actie is afgerond op basis van de ontvangen status updates. Ja 🡪 10Nee 🡪 7  |  |  |
| 10. | CM | Vanuit Contractmanagement wordt het eindresultaat van de afgeronde mitigatie acties teruggekoppeld aan het MT. De Diensteigenaren zijn hierbij betrokken. Hoe en door wie dit gebeurd is aan contractmanagement. Koppelt iedere CM apart de status terug aan het MT, of wordt er e.e.a. gebundeld door de coördinerende CM? Komt er een aparte meeting met het MT, of een jaarlijkse management rapportage? Dit bepaalt Contractmanagement naar eigen inzicht.  |  |  |
| 11. | MT | Het MT besluit of de mitigatie acties hiermee zijn afgerond.Ja 🡪 12Nee 🡪 7 |  |  |
| 12. | CM | De CM koppelt terug aan de Diensteigenaar en de SLM welke mitigatie acties definitief zijn afgerond.De coördinerende CM zorgt ervoor dit voor elke in stap 2 geselecteerde leverancier gebeurt. Hij/zij houdt overzicht over het totaal. |  |  |
| 13. | CM | De CM archiveert op SharePoint Levman:* Elk definitief ingevuld Leverancier Risicoprofiel zoals besproken in de review meeting met het MT.
* De afgesproken en afgesloten mitigatie acties, inclusief status updates.

De coördinerende CM zorgt ervoor dit voor elke in stap 2 geselecteerde leverancier gebeurt. Hij/zij houdt overzicht over het totaal. |  | Ingevuld Leverancier Risicoprofiel op SharePoint Levman |
| 14. |  | Einde proces |  |  |