|  |
| --- |
| Template Risicobehandeling‘Naam’ risico |

|  |  |
| --- | --- |
| 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 |  |  |
| [BELEID RISICOBEHEER] | x |  |  |
| [PROCEDURE RISICOBEHEER] | x |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | RM.01, RM.02, RM.03 |
|  |  |

**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](#_Toc192752905)[1 Inleiding 5](#_Toc192752906)[1.1 Probleemstelling 5](#_Toc192752907)[1.2 Scope van het risico 5](#_Toc192752908)[2 Behandelplan… 6](#_Toc192752909)[2.1 Actieplan 6](#_Toc192752910)[2.1.1 Kop 3 6](#_Toc192752911)[2.2 Impact analyse 6](#_Toc192752912)[3 Beschrijving risico 7](#_Toc192752913)[4 Beoordeling risicobehandelplan 8](#_Toc192752914)[4.1 Beoordeling 8](#_Toc192752915)[Bijlage 1 Verklarende woordenlijst 9](#_Toc192752916) |

Samenvatting

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

|  |
| --- |
| SAMENVATTING |
| Referentienummer | RA.23-01 (voorbeeld) |
| Datum | DD MM YYYY |
| Systemen en/of processen | Betrokken systemen en processen |
| Korte beschrijving risico | Wat houdt het risico in? |
| Risico inschatting | Laag/Gemiddeld/Hoog/Zeer Hoog |
| SURF Control(s) | Referenites SURFaudit Toetsingskader Informatiebeveiliging |
| Eigenaar (‘accountable’) | Naam en Functie |
| Actiehouder (‘responsible’) | Naam en Functie |
| Huidig restrisico | Gemiddeld/Hoog/Zeer Hoog |
| Toekomstig restrisico  | Laag/Gemiddeld/Hoog |
| Einddatum  | DD MM YYYY |

# Inleiding

## Probleemstelling

[Voeg een beschrijving toe van wat op dit moment een verhoogd risico veroorzaakt]

## Scope van het risico

[Geef aan of dit een instellings-breed of een specifiek proces / faculteit / service betredft]

# Behandelplan…

## Actieplan

[Beschrijf de acties voor dit risico-behandelplan, inclusief voorbereiding, verloopdata en actiehouders}

### Kop 3

#### Kop 4

Tekst

## Impact analyse

[Beschrijf de impact van dit uit te voeren risico-behandelplan, op o.a. financiën en andere werkzaamheden]

# Beschrijving risico

[Beschrijf hier het risico]

Het risico wordt ingeschat als**:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans |  | Impact |  | Risico |
| [kans niveau] | X | [impact niveau] | = | risiconiveau |

Pas de tabel hieronder om het ingeschatte risico weer te geven (gebruik het template Risico-matrix voor de juiste termen en kleuren.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RISICO SCORE**(kans \* impact) | **Kans 1**Zeer klein | **Kans 2**Klein | **Kans 3**Gemiddeld | **Kans 4**Groot | **Kans 5**Zeer Groot |
| **Impact 1**Verwaarloosbare  |  |  |  |  |  |
| **Impact 2**Klein |  |  | **Gemiddeld** |  |  |
| **Impact 3**Gemiddeld |  |  |  |  |  |
| **Impact 4**Grote |  |  |  |  |  |

# Beoordeling risicobehandelplan

Alle behandelplannen moeten door […..] beoordeeld worden.

## Beoordeling

[Voeg hier de beoordeling toe]

1. Verklarende woordenlijst

|  |  |
| --- | --- |
| Begrip | Toelichting |
| **Risico-eigenaar** *(Risk owner)* | In dit veld staat de naam van de risico-eigenaar, die verantwoordelijk is voor het behandelen van het risico en dus voor het opstellen van het risicobehandelplan, het aanvragen van de relevante beoordelingen en goedkeuringen en uitvoeren van de plannen. |
| **Actiehouder** *(Action owner)* | De actiehouder kan door de risico-eigenaar aangewezen worden om het risicobehandelplan en de onderliggende acties uit te voeren. De risico-eigenaar blijft wel eindverantwoordelijk voor het risicobehandelplan.  |
| **Risico titel** *(Risk description)* | In dit veld staat een beknopte omschrijving van het risico, waarbij een oorzaak en consequentie benoemd worden. Bijvoorbeeld: “Ongeoorloofde toegang tot IT-systeem X verhoogt het risico op verlies van gevoelige data.”  |
| **Huidig rest-risico** *(Current residual risk)* | In dit veld staat de uitkomst van de meest recente risicoanalyse. Dit moet een score op basis van de risico-matrix uit het IB-Risicomanagement beleid zijn.  |
| **Toekomstig rest-risico** *(Target residual risk)* | In dit veld staat de beoogde risicoscore na het succesvol uitvoeren van de risico-behandeling. Wanneer het toekomstige rest-risico hoger dan ‘Laag’ is, moet er ook een risico-acceptatie aangevraagd worden. |
| **Probleemstelling (Problem statement)**  | In dit veld moet een beschrijving staan van de oorzaak van het verhoogde risico. Het identificeren van de hoofdoorzaak is belangrijk om een passende behandeling te definiëren. Bijvoorbeeld: “De synchronisatie tussen het HR-systeem en Microsoft Azure AD ligt al meerdere weken stil, waardoor een aantal werknemers te hoge privileges hebben.” |
| **Scope van het risico** *(Risk scope)* | In dit veld moet aangegeven worden of het risico van toepassing is op één systeem of proces, of dat het Radboud-breed is. |
| **Actieplan** *(Action plan)*  | In dit veld moeten de verschillende acties op een SMART-manier gedefinieerd worden, inclusief verloopdata en actiehouders.  |
| **Impact analyse** *(Impact analysis)* | In dit veld moet beschreven worden hoe het behandelplan impact heeft op andere aspecten binnen de Radboud Universiteit, zoals financiën en werkzaamheden. Denk aan de extra tijd en eventuele extra kosten die het uitvoeren van een behandelplan met zich meebrengt, of een nieuwe prioritering van werkzaamheden.  |