**Afbeelding met Lettertype, Graphics, schermopname, tekst

Automatisch gegenereerde beschrijving**

**Risk Management**

Security Nederland

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 0.1 | Concept | 5-9-2023 | Ludo Cuijpers  Leo Jaarsma  Henk Links  Sebastiaan van Trigt | Basisdocument |
|  |  |  |  |  |

**Vastgesteld door Security Nederland:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 1.0 |  |  | College van Bestuur |

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en MBO Raad geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.



Creative commons

MBO Raad 4.0 Nederland

(CC BY 4.0) **Copyright**

De gebruiker mag:

Het werk kopiëren, verspreiden en doorgeven

Remixen – afgeleide werken maken

Onder de volgende voorwaarde:

Naamsvermelding – De gebruiker dient bij het werk de naam van MBO Raad te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

[1. Inleiding 3](#_Toc144896463)

[1.1. Aanleiding 3](#_Toc144896464)

[1.2. Gemaakte afspraken 4](#_Toc144896465)

[1.3. Risico beoordeling 4](#_Toc144896466)

[1.4. Risico cyclus 4](#_Toc144896467)

[2. Risico inventarisatie op basis van Cyberdreigingsbeeld 5](#_Toc144896468)

[2.1. Samenvatting 5](#_Toc144896469)

[Dreigingen en kwetsbaarheden permanent aanwezig 5](#_Toc144896470)

[Weerbaarheid blijft aandachtspunt 5](#_Toc144896471)

[Incidenten beter gedetecteerd maar nog niet altijd gedeeld 5](#_Toc144896472)

[Risicobeheer nog in de kinderschoenen 5](#_Toc144896473)

[2.2. Dashboard sectoraal beeld 2022 6](#_Toc144896474)

[Risicobeeld 2022 6](#_Toc144896475)

[Incidentbeeld in 2022 7](#_Toc144896476)

[2.3. Risicobeheer 7](#_Toc144896477)

[2.4. Ketenafhankelijkheid 7](#_Toc144896478)

[2.5. Capaciteitstekort 8](#_Toc144896479)

[2.6. Onveilig gedrag en gebrek aan awareness 8](#_Toc144896480)

[2.7. DPIA’s van verschillende applicaties 9](#_Toc144896481)

[2.8. Te mitigeren risico’s vanaf 2023 9](#_Toc144896482)

[Bijlage 1: Risico’s plotten op NBA statements 10](#_Toc144896483)

[Bijlage 2: Geplotte statements per cyberdreiging 13](#_Toc144896484)

[Bijlage 1: Gehanteerde classificatiemethodiek 21](#_Toc144896485)

[2.9. Risico beoordeling 22](#_Toc144896486)

# Inleiding

## Aanleiding

Het onderwerp Informatiebeveiliging en Privacy (afgekort tot IBP) staat prominent op de agenda van Security Nederland. In het onderwijs worden steeds meer gegevens bijgehouden en Security Nederland realiseert zich hoe belangrijk het is om op een goede en veilige manier met deze informatie om te gaan. Dit geldt zeker voor alle persoonsgegevens die Security Nederland beheert.

Ondernemen is risico’s nemen. Een organisatie en dus ook een onderwijsinstelling dient daarom een gezonde, verstandige afweging te maken tussen risico’s, maatregelen en bedrijfsbelang. Dit geldt ook als het gaat om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Om deze aspecten van informatie en de ondersteunende processen, systemen en netwerken te kunnen waarborgen, dienen organisaties diverse maatregelen te treffen. Aan het treffen van deze maatregelen gaat een risicoanalyse vooraf. Hierdoor kunnen risico’s die van invloed zijn op genoemde aspecten op een evenwichtige wijze worden geïnventariseerd, beheerst en gereduceerd tot een voor de organisatie aanvaardbaar niveau. De onderwijsinstelling maakt gebruik van een Informatie risicomanagement framework om de risico’s in kaart te brengen.

|  |  |
| --- | --- |
| **Internal audits**  (proceseigenaren) | * **Informatiebeveiliging NBA (=toetsingskader SURF)**   Afspraak om vóór 31-12-2023 alle statements scoren gemiddeld op volwassenheidsniveau 3. |
| **Cyberdreigingsbeeld SURF** | Risico’s zijn tot stand gekomen op basis van overleg met alle deelnemende HO en mbo instellingen.  Risico’s worden overgenomen door onderwijsinstelling. |
| **DPIA’s kernapplicaties**  (applicatie-eigenaren)  *Voorbeeld onderwijsinstelling ->* | *1 Studenten Informatiesysteem: Eduarte*  *2 HRM systeem: AFAS*  *3 Financieel systeem: AFAS*  *4 Kantoorautomatiseringssysteem: Office 365*  *5 Identiteitsbeheersysteem (IAM): eigen* |
| **Decentrale assessments**  (leidinggevenden – first line) | Toetsing op:   * Scholing leidinggevenden * Scholing medewerkers * Governance/compliance acceptatie * Toegekende autorisaties (SOLL autorisatie matrix) * Ondertekende verwerkersovereenkomsten (decentrale applicaties)   Ophalen niet benoemde risico’s |
| **Overige assessments**  (proceseigenaren) | * Privacy (SURF) * Digitaal ondertekenen (optioneel) |

## Gemaakte afspraken

* risico-eigenaarschap (Accountable) College van Bestuur
* risicoproces Risico set wordt geplot op de 69 NBA statements en op de RACI
* risicobeoordeling Kans x impact conform SURF (Cyberdreigingsbeeld)
* risicomitigatie Risico’s worden geplot op het NBA kader. De statements die betrekking hebben op het risico worden (versneld) naar

het noodzakelijke niveau gebracht, zodat het risico verkleind wordt.

* risicoacceptatie College van Bestuur

## Risico beoordeling

De risicoanalyse levert informatie op, waarmee het College van Bestuur in staat wordt gesteld te beslissen welke risico’s (of combinatie van risico’s) een te groot potentiële schade vormen en met welke maatregelen deze risico’s verkleind kunnen worden. Op hoofdlijnen zijn er vier reacties mogelijk op elk risico:

1. Risico vermijden (avoid)

2. Risico verkleinen (mitigation)

3. Risico accepteren (accept)

4. Risico elders beleggen (transfer)

## Risico cyclus

Start voor de aanzet van het risico actieplan is het Cyberdreigingsbeeld van SURF.

Jaarlijks vindt ook de beperkte audit plaats van de organisatorische eenheden.

Aanbevelingen van DPIA’s worden meegenomen.

Het niet realiseren van het volwassenheidsniveau 3 van het NBA kader wordt ook als een risico geïnterpreteerd.

# Risico inventarisatie op basis van Cyberdreigingsbeeld[[1]](#footnote-2)

## **Samenvatting**

Dreigingen en kwetsbaarheden permanent aanwezig

De laatste jaren verandert het beeld over dreigingen en kwetsbaarheden weinig. Ze worden vooral veroorzaakt door statelijke actoren, cybercriminelen, (h)acktivisten en mensen binnen organisaties die onbedoeld incidenten veroorzaken. Het aantal incidenten blijft nog steeds stijgen. Ook worden er steeds meer kwetsbaarheden gevonden in systemen en applicaties en blijven DDoS-aanvallen, phishing-mails en ransomware-aanvallen aan de orde van de dag.

Weerbaarheid blijft aandachtspunt

De professionaliteit van kwaadwillenden ontwikkelt zich vaak sneller dan de snelheid waarmee instellingen hun weerbaarheid kunnen verbeteren. De snelheid waarmee nieuwe aanvalstechnieken worden ontwikkeld is aanzienlijk en zorgt voor permanente uitdaging om bij te blijven. De metingen die SURF uitvoert op procesvolwassenheid, internetveiligheid en awareness, laten zien dat weerbaarheid een aandachtspunt blijft. Het besef groeit dat niet alleen de interne processen en systemen op orde moeten zijn, maar dat ook het menselijk handelen en processen voor samenwerkingsverbanden, ketenpartners en leveranciers aan passende richtlijnen moeten voldoen.

Incidenten beter gedetecteerd maar nog niet altijd gedeeld

Instellingen worden beter in het detecteren van incidenten, zeker nu steeds meer instellingen monitoring en detectie inrichten of uitbesteden. Toch nemen instellingen tijdens een incident niet altijd contact op met SURFcert. Niet alleen kan SURFcert ondersteuning bieden, maar kunnen zij ook de (technische) informatie over het incident delen om andere instellingen voor eenzelfde lot te behoeden.

Risicobeheer nog in de kinderschoenen

Er zijn nog maar weinig instellingen die risico gebaseerd werken. Risico eigenaarschap is nog beperkt ingebed bij het hogere management. Functionarissen die risico-eigenaren moeten ondersteunen zijn vaak nog niet goed in positie gebracht en worden gehinderd door capaciteitsproblemen. Toch zien we dat bestuurders steeds meer betrokken zijn en in de hele sector worden verbeterprogramma’s uitgevoerd.

## Dashboard sectoraal beeld 2022

Risicobeeld 2022

Ten opzichte van het vorige dreigingsbeeld valt op dat dit jaar geen van de risicocategorieën als ‘zeer hoog’ wordt ingeschat. Daarnaast zijn er twee nieuwe categorieën toegevoegd: Onveilig gedrag en gebrek aan awareness en Capaciteitstekort.

Afbeelding met tekst, schermopname, nummer, Lettertype

Automatisch gegenereerde beschrijving

Incidentbeeld in 2022

In 2022 hebben er incidenten plaatsgevonden in alle risicocategorieën uit het Cyberdreigingsbeeld van 2021-2022

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

## Risicobeheer

Het algemene beeld voor heel Nederland is helder in de Nederlandse Cybersecurity Strategie: ‘Risicomanagement staat nog in de kinderschoenen’. Risicobeheer blijkt vaak organisatorisch complex te zijn, ook in onze sector. We zien dit terug in de SURFaudit benchmark, het instrument waarmee de compliance wordt gemeten tegen het SURFaudit toetsingskader informatiebeveiliging. De benchmark scores laten zien dat het volwassenheidsniveau van risicobeheer en governance bij de deelnemende leden nog niet op het geambieerde volwassenheidsniveau 3 is. Het volwassenheidsniveau van het domein risicobeheer is al twee metingen op rij de laagste van alle vijftien deelgebieden van het toetsingskader. Instellingen die bij risicobeheer op niveau 2 zijn, hebben wel beleid en processen voor (informatiebeveiliging)risicobeheer, maar gebruiken die voornamelijk bij grote projecten of als reactie op problemen. Informatie- en privacy risicobeoordeling op basis van organisatiedoelstellingen gebeurt op beperkte schaal. Daarbij is het eigenaarschap van risico’s slechts gedeeltelijk toegewezen aan senior managers.

Uit de survey blijkt dat bestuurders van de meeste instellingen met regelmaat rapportages over informatiebeveiliging en privacy ontvangen. Bij bijna de helft van de instellingen vindt daarbij elk kwartaal een dialoog plaats tussen het college van bestuur en de rapporterende functionaris. Er is weinig uniformiteit in de rapportagevormen: de respondenten van de survey rapporteren elk op hun eigen wijze aan verschillende gremia.

## **Ketenafhankelijkheid**

De categorie Ketenafhankelijkheid heette vorige jaar Afhankelijkheid van clouddiensten. We hebben de naam aangepast om een bredere lading te dekken. Respondenten gaven aan dat zij niet alleen met cloud-leveranciers, maar ook met andere leveranciers uitdagingen ervaren. Bovendien is het van belang om ook de risico’s bij samenwerkingen met partnerorganisaties te beheersen. Organisaties zijn digitaal verbonden en verweven, ook met samenwerkingspartners, leveranciers en overheden. Wanneer een van de partijen wordt getroffen door een incident, kan dat gevolgen hebben voor meerdere organisaties. En die gevolgen kunnen zich uitstrekken buiten informatiebeveiliging: toen in 2022 een leverancier van toegangspassen was getroffen door een incident, was dat niet alleen een datalek, maar was er ook een mogelijke impact op de fysieke beveiliging

## Capaciteitstekort

We hebben deze categorie dit jaar toegevoegd omdat het tekort aan mensen en kennis in de survey veelvuldig werd genoemd als een hoog tot zeer hoog urgent risico, dat ook andere risicocategorieën beïnvloedt: maar liefst 81% van de respondenten in de survey gaf aan dat hun instelling onvoldoende mensen heeft om informatiebeveiligings- en privacy taken uit te voeren. Tijdelijke inhuur van professionals lijkt dit probleem niet op te lossen omdat ook ict-dienstverleners kampen met personeelstekorten. Vacatures voor informatiebeveiliging en privacy zijn lastig te vervullen. Het probleem is niet beperkt tot informatieveiligheid, maar betreft de hele ict-sector. Door gebrek aan goed geschoolde en ervaren medewerkers kunnen instellingen niet groeien in weerbaarheid en cybervolwassenheid.

## **Onveilig gedrag en gebrek aan awareness**

De meerderheid van cyberincidenten vindt plaats als gevolg van onbedoeld onveilig handelen door mensen. Dit beeld is niet uniek voor onze sector. Voor veel mensen is het nog geen routine om basale cybersecuritymaatregelen toe te passen, of om daarbij hulp te vragen. Van medewerkers en studenten wordt verwacht dat zij weten hoe zij met ict moeten omgaan, terwijl niet iedereen daarin een basisniveau heeft. Bovendien kan hoge werkdruk leiden tot vergissingen. Uit de reacties van de respondenten bleek dat bepaalde soorten vergissingen binnen hun organisatie herhaaldelijk de oorzaak waren van incidenten:

• Fouten met het versturen van e-mails, waarbij persoonsgegevens bij de verkeerde ontvanger terecht komen.

• Klikken op linkjes in phishingmails en vervolgens accountgegevens invoeren op een malafide website.

• Een drive met documenten delen met personen die daartoe geen toegang nodig hebben.

• Het delen van inloggegevens.

• Onvoldoende kennis van autorisaties in een samenwerkingsomgeving.

• Vergissingen van ict-beheerders bij wijzigingen in systemen waardoor de autorisaties veranderen.

• Buiten de procedures om ict inkopen, waardoor de basismaatregelen voor privacy en informatiebeveiliging niet zijn geborgd.

De respondenten van de survey zijn het ermee eens dat structurele aandacht voor security en privacy onontbeerlijk is om een weerbare organisatie te zijn, en dat medewerkers hier een belangrijke rol in spelen. Een aantal respondenten geeft aan dat security en privacy nu te vrijblijvende thema’s zijn. Zij pleiten daarom voor het invoeren van bijvoorbeeld verplichte awareness trainingen en phishingtesten. De respondenten zien dit als een stok achter de deur; zij zijn zich ervan bewust dat collega's mogelijk minder gemotiveerd zijn door werkdruk, onduidelijke regels en gebrek aan interesse. Door awareness-activiteiten verplicht te maken, wordt voor de instelling ook duidelijk welke investering er van medewerkers verwacht wordt

## DPIA’s van verschillende applicaties

De bevindingen en aanbevelingen van de SIS (Studenten Informatie Systeem) en HR-applicaties geven aan de autorisatieprocedures niet op orde zijn. Deze aanbeveling sluit aan bij het 2e beschreven risico binnen het Cyberdreigingsbeeld (2. Identiteitsfraude).

Een ander risico, ook aangeven door de Onderwijsinspectie, zijn de bewaartermijnen.

Governance wordt meegenomen als 1e risico, immers een sluitende en werkbare governance is de voorwaarde om de overige risico’s te mitigeren. Nogmaals governance is de basis voor de mitigatie van de benoemde risico’s.

## Te mitigeren risico’s vanaf 2023

De volgende 5 risico’s zullen vanaf 2023 gemitigeerd worden:

De aanpak om te komen tot een laag risico wordt hieronder globaal beschreven. De bijlagen beschrijven de details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **R1**  **Governance** | **R2**  **Ransomware** | **R3**  **Ketenafhankelijkheid** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |
| 1 Strategie / Visie | **Governance** | **Governance** | **Governance** | **Governance** |
| 2 IBP Beleid | 1 Scholing | 1 Scholing | 1 Scholing | 1 Scholing |
| 3 Architectuur MORA/HORA | 2 Duidelijke afspraken met gebruikers | 2 Duidelijke afspraken met gebruikers | 2 Duidelijke afspraken met gebruikers | 2 Duidelijke afspraken met gebruikers |
| 4 Eigenaarschap | 3 Registreren van incidenten van gebruikers en SURFcert | 3 Inkoop als proceseigenaar benoemen | 3 Document voor Identity and Access Management (IAM) | 3 Veilig opslaan data |
| 5 Risk Management | 4 Implementeren van technische weerbaarheid (MFA, SOC SIEM, etc.) | 4 Uitvoeren van (pen-) testen en audits door SURF op kernapplicaties | 4 Toepassen van IAM door leidinggevenden en beheerders | 4 Classificatie van data |
| 6 Roadmap | 5 Implementeren en testen van Business Continuïteit (deelname OZON / NOZON) |  |  | 5 Verwijderen van data op basis van afspraken binnen de mbo sector (DSP) |

# Bijlage 1: Risico’s plotten op NBA statements

Deze stap plot de NBA statements op de cyberdreigingsrisico’s. Bovendien wordt een volwasssenheidsniveau aangegeven. Voorbeeld statement 11.4, Logging, vermeldt SIEM op niveau 5, vandaar dat dit statement als mitigerende maatregel op volwassenheidsniveau 5 gerealiseerd moet worden.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF |
| **G01 Strategie** | 1.1 Strategie | **1** | **4** | **4** | **4** | **4** |  |
| **G02 Beleid** | 1.2 Beleid | **2** | **4** | **4** | **4** | **4** |  |
| **G03 Architectuur** | 1.4 Architectuur | **3** | **4** | **4** | **4** | **4** |  |
| **G04 Eigenaarschap** | 2.1 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid | **4** | **3** | **3** | **3** | **3** |  |
| 2.2 Functiescheiding | **5** | **3** | **3** | **3** | **3** |  |
| **G05 Risk Management** | 3.1 Informatie risicomanagementframework | **6** | **3** | **3** | **3** | **3** |  |
| 3.2 Risicobeoordeling | **7** | **3** | **3** | **3** | **3** |  |
| 3.3 Plan voor behandeling en beperking van risico's (incl. risicoacceptatie) | **8** | **3** | **3** | **3** | **3** |  |
| **G06 Roadmap** | 1.3 Planning / Roadmap | **9** | **4** | **4** | **4** | **4** |  |
| **G07 Assurance** | 1.5 Onafhankelijke toetsing | **10** | **4** | **4** | **4** | **4** |  |
| **P08 Human Resources** | 4.1 Werving | **11** |  |  |  |  |  |
| 4.2 Certificering, training en scholing | **12** |  |  |  |  |  |
| 4.3 Afhankelijkheid van individuen | **13** |  |  |  |  |  |
| 4.4 Verandering of beëindiging van functie | **14** |  |  |  |  |  |
| 4.5 Kennisdeling | **15** |  |  |  |  |  |
| 4.6 Veiligheidsbewustzijn | **16** | **4** | **4** | **4** | **4** | **20K** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF |
| **P09 ITIL** | 5.1 Identificatie en onderhoud van configuratie-items | **17** |  | **3** |  |  |  |
| 5.2 Configuratiedatabase en baseline | **18** | **3** | **3** |  |  |  |
| 6.1 Incident management | **19** | **3** |  |  |  |  |
| 6.2 Incident escalatie | **20** | **3** |  |  |  |  |
| 6.3 Incidentrespons op (cyber) beveiligingsincidenten | **21** | **3** |  |  |  |  |
| 6.4 Probleemmanagement | **22** |  |  |  |  |  |
| 7.1 Normen en procedures voor aanpassingen | **23** |  |  |  |  |  |
| 7.2 Impact assessment, prioriteren en autoriseren | **24** |  |  |  |  |  |
| 7.3 Noodaanpassingen | **25** |  |  |  |  |  |
| 7.4 Testomgeving | **26** |  |  |  |  |  |
| 7.5 Testen van aanpassingen | **27** |  |  |  |  |  |
| 7.6 Promotie naar productie | **28** |  |  |  |  |  |
| 12.1 Fysieke beveiligingsmaatregelen | **29** |  |  |  |  |  |
| 12.2 Beheer van fysieke toegangsrechten | **30** |  |  |  |  |  |
| **P10 Data Management** | 8.1 Methodiek voor veilige softwareontwikkeling en -implementatie | **31** |  |  |  |  |  |
| 8.2 Toegang tot de productieomgeving door ontwikkelaars | **32** |  |  |  |  |  |
| 8.3 Data conversie en/of migratie | **33** |  |  |  |  |  |
| 9.1 Data (en systeem) eigenaarschap | **34** |  |  |  | **3** |  |
| 9.2 Classificatie | **35** |  |  |  | **3** |  |
| 9.3 Beveiligingseisen voor gegevensbeheer | **36** |  |  |  | **3** |  |
| 9.4 Inrichting van opslag en retentie | **37** |  |  |  | **3** | **50K** |
| 9.5 Uitwisseling van (gevoelige) gegevens | **38** |  |  | **3** |  |  |
| 9.6 Verwijdering van data | **39** |  |  | **3** |  |  |
| **P11 IAM** | 10.1 Toegangsrechten | **40** |  |  | **3** |  |  |
| 10.2 Administratie van toegangsrechten | **41** |  |  | **3** |  |  |
| 10.3 Super Users | **42** |  |  | **3** |  |  |
| 10.4 Noodtoegang (envelopprocedure/breek-het-glasprocedure) | **43** |  |  | **3** |  |  |
| 10.5 Periodieke beoordeling van toegangsrechten | **44** |  |  | **3** |  |  |
| **P12 Security Baselines** | 11.1 Security baselines | **45** | **4** | **4** | **4** | **4** |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF |
| **P13 Business Continuity** | 14.1 Bedrijfscontinuïteitsplanning | **46** | **3** |  |  |  |  |
| 14.2 Testen van Disaster recovery | **47** | **3** |  |  |  |  |
| 14.3 Offsite back-upopslag | **48** | **3** |  |  |  |  |
| 14.4 Gegevensreplicatie | **49** | **3** |  |  |  |  |
| 14.5 Crisisbeheer | **50** | **3** |  |  |  |  |
| **P14 Cloud Leveranciers** | 15.1 Service level overeenkomst | **51** |  | **3** |  |  |  |
| 15.2 Service level beheer | **52** |  | **3** |  |  |  |
| 15.3 Risicobeheer van leveranciers | **53** |  | **3** |  |  |  |
| 15.4 Interne beheersing bij derden | **54** |  | **3** |  |  |  |
| **T15 MFA - Thuiswerken** | 11.2 Authenticatiemechanismes | **55** | **4** |  | **4** |  | **20K** |
| 11.3 Mobiele apparaten en telewerken | **56** | **3** |  |  |  |  |
| **T16 SOC SIEM** | 11.4 Logging | **57** | **5** |  |  |  | **40K** |
| **T17 Pentesten** | 11.5 Testen van, inspectie van en toezicht op beveiliging | **58** | **3** |  |  |  | **20K** |
| **T18 Patchbeheer** | 11.6 Patchbeheer | **59** | **3** |  |  |  | **20K** |
| 11.7 Beheer van bedreigingen en kwetsbaarheden | **60** | **3** |  |  |  |  |
| **T19 Infrastructuur** | 11.8 Beschikbaarheid en bescherming van infrastructuur | **61** |  |  |  |  |  |
| 11.9 Onderhoud van de infrastructuur | **62** |  |  |  |  |  |
| **T20 Security Policy** | 11.10 Beheer van cryptografische sleutels | **63** |  |  |  |  |  |
| 11.11 Network security | **64** |  |  |  |  |  |
| 11.12 Beheersing van malware-aanvallen | **65** |  |  |  |  |  |
| 11.13 Bescherming van beveiligingstechnologie | **66** |  |  |  |  |  |
| **T21 Computer Operations** | 13.1 Job processing | **67** | **3** | **3** |  |  |  |
| 13.2 Procedures voor back-up en herstel | **68** |  |  |  |  |  |
| 13.3 Capaciteits- en prestatiebeheer | **69** |  |  |  |  |  |
|  | **Gegeven risicoscore (Netto score)** |  | **R2**  **Ransomware** | **R3**  **Cloud** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |  |

# Bijlage 2: Geplotte statements per cyberdreiging

R1 Governance

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF | **Proceseigenaar**  **Accountable** |
| **G01 Strategie** | 1.1 Strategie | **1** | **4** | **4** | **4** | **4** |  | College van Bestuur |
| **G02 Beleid** | 1.2 Beleid | **2** | **4** | **4** | **4** | **4** |  | College van Bestuur |
| **G03 Architectuur** | 1.4 Architectuur | **3** | **4** | **4** | **4** | **4** |  | College van Bestuur |
| **G04 Eigenaarschap** | 2.1 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid | **4** | **3** | **3** | **3** | **3** |  | College van Bestuur |
| 2.2 Functiescheiding | **5** | **3** | **3** | **3** | **3** |  | College van Bestuur |
| **G05 Risk Management** | 3.1 Informatie risicomanagementframework | **6** | **3** | **3** | **3** | **3** |  | College van Bestuur |
| 3.2 Risicobeoordeling | **7** | **3** | **3** | **3** | **3** |  | College van Bestuur |
| 3.3 Plan voor behandeling en beperking van risico's (incl. risicoacceptatie) | **8** | **3** | **3** | **3** | **3** |  | College van Bestuur |
| **G06 Roadmap** | 1.3 Planning / Roadmap | **9** | **4** | **4** | **4** | **4** |  | College van Bestuur |
| **G07 Assurance** | 1.5 Onafhankelijke toetsing | **10** | **4** | **4** | **4** | **4** |  | College van Bestuur |
| **P08 Human Resources** | 4.6 Veiligheidsbewustzijn | **16** | **4** | **4** | **4** | **4** | **20K** | Hoofd HRM |

**Samenhang binnen Governance**

Het onderdeel governance bestaat uit 7 documenten.

De logische volgorde wijkt af van de indeling binnen het NBA kader (=SURF kader).

Binnen de deze documenten reeks wordt de onderstaande volgorde gehanteerd:

1. **Strategie (NBADOC01 Strategie)**

*Een strategie en visie op informatie- en cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.*

***Leidend****: Alle medewerkers en leidinggevenden zijn verantwoordelijk voor een optimaal functionerend privacy en security beleid.*

1. **Beleid (NBADOC02 Beleid)**

*De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld en beschreven en gecommuniceerd aan medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management*.

***Leidend****: De rol van de 1e lijn wordt verder uitgewerkt met het benoemen van een systeemeigenaar, applicatie eigenaren en proceseigenaren.*

1. **Architectuur (NBADOC03 Architectuur)**

*De onderwijsinstelling past de MORA/HORA architectuur toe. Dit model moet het mogelijk maken om effectief, veilig en op een robuuste manier informatie te creëren, gebruiken en te delen zoals wordt vereist door bedrijfsdoelstellingen en wettelijke voorschriften.*

***Leidend****: De processen zoals aangegeven binnen de MORA/HORA zijn leidend voor de onderwijsorganisatie.*

1. **Eigenaarschap (NBADOC04 Eigenaarschap)**

*Informatiebeveiliging wordt gemanaged op alle toepasselijke organisatieniveaus en Security (of Information Risk) Management wordt gemanaged in overeenstemming met business requirements/risico's. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn formeel toegewezen en ingebed in de organisatie.*

***Leidend****: De processen worden toegewezen aan de proceseigenaren (Accountable). Het RACI model wordt samen met de proceseigenaren ingevuld.*

1. **Risk Management (NBADOC05 Risk Management)**

*Er is een framework voor Information Risk Management opgesteld en afgestemd op de doelstellingen van de organisatie en het framework voor (enterprise) Risk Management. Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland om de benodigde mitigerende maatregelen te implementeren, inclusief het bepalen van kosten en baten en de verantwoordelijkheid voor de uitvoering. Goedkeuring wordt verkregen voor aanbevolen acties en acceptatie van restrisico's en er wordt voor gezorgd dat uitgevoerde acties onder verantwoordelijkheid van betrokken proceseigenaar(s) vallen. De uitvoering van plannen wordt bewaakt en eventuele afwijkingen worden gerapporteerd aan het senior management.*

*Leidend: Het SURF Cyberdreigingsbeeld en de door de onderwijsorganisatie uitgevoerde DPIA’s. De cyberdreigingsrisico’s en DPIA risico’s worden geplot op de statements van het NBA kader. Het NBA kader bestaat uit 15 domeinen, die binnen de MORA/HORA benoemd zijn als processen. De domeinen (processen) zijn toegewezen aan de proceseigenaren en dus ook de risico’s. Uiteindelijk leidt dit tot het Risico Actieplan.*

1. **Roadmap (NBADOC06 Roadmap)**

*Bedrijfsdoelstellingen, risico's en compliance eisen worden vertaald in een algemeen informatiebeveiligingsplan en/of cyber security plan, rekening houdend met de IT-infrastructuur en de veiligheidscultuur.*

***Leidend****: Het Risico Actieplan is de basis voor de Roadmap 2023-2025. De proceseigenaren zijn verantwoordelijk voor de planning om de maturity levels te kunnen realiseren.*

1. **Assurance (NBADOC07 Assurance)**

*Onafhankelijke assurance (intern of extern) wordt verkregen om te bepalen in hoeverre de informatievoorziening (inclusief IT) voldoet aan relevante wet- en regelgeving; het beleid van de organisatie, de normen en procedures van de organisatie; algemeen aanvaarde werkwijzen; en effectieve en efficiënte prestaties van IT.*

***Leidend****: Vanwege de hoge kosten voor het verkrijgen van een Assurance wordt door het College van Bestuur overwogen om te komen tot een (goedkopere) certificering. Besluitvorming betreffende dit onderwerp zal in de loop van 2023 plaatsvinden.*

**P08 Human Resources 4.6 Veiligheidsbewustzijn**

Veiligheidsbewustzijn is gebaseerd op een meetbare online training door alle medewerkers binnen de onderwijsinstelling. Fontys Hogeschool hanteert de volgende 15 gedragingen die behandeld worden in de online training. Deze gedragingen sluiten aan bij het Cyberdreigingsbeeld en DPIA’s en worden jaarlijks herzien op basis van nieuwe risico’s.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

R2 Ransomware

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF | **Proceseigenaar**  **Accountable** | |
| **P09 ITIL** | 5.2 Configuratiedatabase en baseline | **18** | **3** | **3** |  |  |  | Hoofd ICT | |
| 6.1 Incident management | **19** | **3** |  |  |  |  | Hoofd ICT | |
| 6.2 Incident escalatie | **20** | **3** |  |  |  |  | Hoofd ICT | |
| 6.3 Incidentrespons op (cyber) beveiligingsincidenten | **21** | **3** |  |  |  |  | Hoofd ICT | |
| **P12 Security Baselines** | 11.1 Security baselines | **45** | **4** | **4** | **4** | **4** |  | College van Bestuur | |
| **P13 Business Continuity** | 14.1 Bedrijfscontinuïteitsplanning | **46** | **3** |  |  |  |  | Hoofd Facilitair | |
| 14.2 Testen van Disaster recovery | **47** | **3** |  |  |  |  | Hoofd Facilitair | |
| 14.3 Offsite back-upopslag | **48** | **3** |  |  |  |  | Hoofd Facilitair | |
| 14.4 Gegevensreplicatie | **49** | **3** |  |  |  |  | Hoofd Facilitair | |
| 14.5 Crisisbeheer | **50** | **3** |  |  |  |  | Hoofd Facilitair | |
| **T15 MFA - Thuiswerken** | 11.2 Authenticatiemechanismes | **55** | **4** |  | **4** |  | **20K** | Hoofd ICT | |
| 11.3 Mobiele apparaten en telewerken | **56** | **3** |  |  |  |  | Hoofd ICT | |
| **T16 SOC SIEM** | 11.4 Logging | **57** | **5** |  |  |  | **150K** | Hoofd ICT | |
| **T17 Pentesten** | 11.5 Testen van, inspectie van en toezicht op beveiliging | **58** | **3** |  |  |  | **50K** | Hoofd ICT | |
| **T18 Patchbeheer** | 11.6 Patchbeheer | **59** | **3** |  |  |  | **30K** | Hoofd ICT | |
| 11.7 Beheer van bedreigingen en kwetsbaarheden | **60** | **3** |  |  |  |  | Hoofd ICT | |
| **T21 Computer Operations** | 13.2 Procedures voor back-up en herstel | **68** | **3** | **3** |  |  |  | Hoofd ICT | |
|  | **Gegeven risicoscore (Netto score)** |  | **R2**  **Ransomware** | **R3**  **Cloud** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |  |  |

***Leidend****: De Governance en training Veiligheidsbewustzijn is geregeld.*

*Documenten* **P09 ITIL**, **P12 Security Baselines** *en* **P13 Business Continuity.** *zijn* *in 2023 vastgesteld.*

**T15 MFA – Thuiswerken, T16 SOC SIEM**, **T17 Pentesten**, **T18 Patchbeheer** *en* **T21 Computer Operations** *zijn in 2023 vastgesteld.*

Om ransomware te voorkomen geeft het NCSC (Nationaal Cyber Security Centrum) een aantal tips, die een rol spelen in de verschillende fasen van een aanval.

1. Bescherm je organisatie tegen phishing
2. Organiseer vulnerability management, patchmanagement en netwerksegmentering
3. Beperk de mogelijkheden van code execution
4. Filter webbrowserverkeer
5. Beperk het gebruik van USB-sticks

R3 Cloud computing

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF | **Proceseigenaar**  **Accountable** | |
| **P09 ITIL** | 5.1 Identificatie en onderhoud van configuratie-items | **17** |  | **3** |  |  |  | Hoofd ICT | |
| 5.2 Configuratiedatabase en baseline | **18** | **3** | **3** |  |  |  | Hoofd ICT | |
| **P12 Security Baselines** | 11.1 Security baselines | **45** | **4** | **4** | **4** | **4** |  | College van Bestuur | |
| **P14 Cloud Leveranciers** | 15.1 Service level overeenkomst | **51** |  | **3** |  |  |  | Hoofd Inkoop | |
| 15.2 Service level beheer | **52** |  | **3** |  |  |  | Hoofd Inkoop | |
| 15.3 Risicobeheer van leveranciers | **53** |  | **3** |  |  |  | Hoofd Inkoop | |
| 15.4 Interne beheersing bij derden | **54** |  | **3** |  |  |  | Hoofd Inkoop | |
| **T21 Computer Operations** | 13.2 Procedures voor back-up en herstel | **68** | **3** | **3** |  |  |  | Hoofd ICT | |
|  | **Gegeven risicoscore (Netto score)** |  | **R2**  **Ransomware** | **R3**  **Cloud** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |  |  |

***Leidend****: 15.3 Risicobeheer van leveranciers en 15.4 Interne beheersing bij derden zijn belegd bij de SURF. De bevindingen en aanbevelingen van SURF kunnen dat vervolgens beoordeeld worden door de onderwijsinstelling.*

R4 Identiteitsfraude

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF | **Proceseigenaar**  **Accountable** | |
| **P10 Data Management** | 9.5 Uitwisseling van (gevoelige) gegevens | **38** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| 9.6 Verwijdering van data | **39** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| **P11 IAM** | 10.1 Toegangsrechten | **40** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| 10.2 Administratie van toegangsrechten | **41** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| 10.3 Super Users | **42** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| 10.4 Noodtoegang (envelopprocedure/breek-het-glasprocedure) | **43** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| 10.5 Periodieke beoordeling van toegangsrechten | **44** |  |  | **3** |  |  | Hoofd Studentenzaken | |
| **P12 Security Baselines** | 11.1 Security baselines | **45** | **4** | **4** | **4** | **4** |  | College van Bestuur | |
| **T15 MFA - Thuiswerken** | 11.2 Authenticatiemechanismes | **55** | **4** |  | **4** |  | **20K** | Hoofd ICT | |
|  | **Gegeven risicoscore (Netto score)** |  | **R2**  **Ransomware** | **R3**  **Cloud** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |  |  |

***Leidend****:* **P11 IAM**  *is in 2023 vastgesteld. Dit is een complex proces omdat het onderwijs, bedrijfsvoering en applicatie beheer een rol spelen.*

R5 Bewaartermijnen

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2**  **Ransomware** | **R3**  **Cloud computing** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** | Kosten INDICATIEF | **Proceseigenaar**  **Accountable** | |
| **P10 Data Management** | 9.1 Data (en systeem) eigenaarschap | **34** |  |  |  | **3** |  | Hoofd Studentenzaken | |
| 9.2 Classificatie | **35** |  |  |  | **3** |  | Hoofd Studentenzaken | |
| 9.3 Beveiligingseisen voor gegevensbeheer | **36** |  |  |  | **3** |  | Hoofd Studentenzaken | |
| 9.4 Inrichting van opslag en retentie | **37** |  |  |  | **3** | **50K** | Hoofd Studentenzaken | |
| **P12 Security Baselines** | 11.1 Security baselines | **45** | **4** | **4** | **4** | **4** |  | College van Bestuur | |
|  | **Gegeven risicoscore (Netto score)** |  | **R2**  **Ransomware** | **R3**  **Cloud** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |  |  |

***Leidend****: Service document of Document Structuur Plan.*

## Bijlage 1: Gehanteerde classificatiemethodiek [[2]](#footnote-3)

Classificatie van informatierisico's gebeurt op basis van een set van algemeen geldende karakteristieken vanuit het framework voor organisatiebreed Risk Management en getroffen maatregelen voor informatierisico's zijn gestandaardiseerd en geprioriteerd, waarbij rekening gehouden wordt met kans, impact en restrisico's.

**Risico = Kans x Impact**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Kans Laag**  **(1)** | **Kans Middel**  **(2)** | **Kans Hoog**  **(3)** |
| **Impact laag**  **(1)** | **Risico Laag**  **(1)** | **Risico Laag**  **(2)** | **Risico Medium**  **(3)** |
| **Impact Middel**  **(2)** | **Risico Laag**  **(2)** | **Risico Medium**  **(4)** | **Risico Hoog**  **(6)** |
| **Impact Hoog**  **(3)** | **Risico Medium**  **(3)** | **Risico Hoog**  **(6)** | **Risico Zeer Hoog**  **(9)** |

*Bron: SURF*

**Rood (Risico Zeer Hoog)**

• Er zijn ernstige ontwikkelingen die de dreiging acuut maken.

• OF Maatregelen hebben nauwelijks effect, zodat de dreiging ernstig blijft.

• OF Incidenten hebben zich meermaals voorgedaan in de sector.

**Oranje (Risico Hoog)**

• Er zijn duidelijke ontwikkelingen die de dreiging acuut maken.

• OF Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft.

• OF Incidenten hebben zich voorgedaan in de sector.

**Geel (Risico Medium)**

• Er worden nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat.

• OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen.

• OF Incidenten hebben zich voorgedaan buiten de sector.

**Blauw (Risico Laag)**

• Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat.

• OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen.

• OF Er hebben zich geen noemenswaardige incidenten van de dreiging voorgedaan in de sector.

## Risico beoordeling

De risicoanalyse levert informatie op, waarmee het College van Bestuur in staat wordt gesteld te beslissen welke risico’s (of combinatie van risico’s) een te groot potentiële schade vormen en met welke maatregelen deze risico’s verkleind kunnen worden. Op hoofdlijnen zijn er vier reacties mogelijk op elk risico:

1. Risico vermijden (avoid)

2. Risico verkleinen (mitigation)

3. Risico accepteren (accept)

4. Risico elders beleggen (transfer)

1. CYBERDREIGINGSBEELD 2023 ONDERWIJS EN ONDERZOEK, SURF Utrecht [↑](#footnote-ref-2)
2. CYBERDREIGINGSBEELD 2021-2022 ONDERWIJS EN ONDERZOEK, SURF Utrecht [↑](#footnote-ref-3)