****

**Eigenaarschap**

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).

# RACI

## Inleiding

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.

## Terugblik op de vorige documenten

De visie is inmiddels vastgesteld en het daarvan afgeleide IBP beleid gecommuniceerd en wellicht al vastgesteld. De rollen binnen de 1ste lijn verantwoordelijken zijn door het College van Bestuur benoemd. Een van de rollen zijn de proceseigenaren. In het architectuur document zijn alle processen benoemd.

## Aanpak eigenaarschap

In dit document gaan we in 2 stappen de processen toewijzen aan de proceseigenaren.

Stap 1: Eigenaarschap, rollen, verantwoording en verantwoordelijkheid (statement 6)

Stap 2: Functiescheiding (statement 7)

**Stap 1: Eigenaarschap, rollen, verantwoording en verantwoordelijkheid (statement 6)**

Binnen het statement 6 wordt op het volwassenheidsniveau 4b verwezen naar de RACI matrix. Dit document hanteert om die reden de RACI matrix.

|  |  |
| --- | --- |
| **4** | 1. Eigenaarschap, verantwoordelijkheid en aansprakelijkheid voor IT-gerelateerde risico's zijn in de organisatie op senior management niveau ingebed. 2. Bijkomende verantwoordelijkheden voor (Information) Security Management kunnen op een systeemspecifiek niveau worden toegewezen (het juiste niveau kan worden bepaald met bijvoorbeeld een RACI matrix). 3. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid worden periodiek geëvalueerd. |

Voordelen van gebruik van een RACI-tabel:

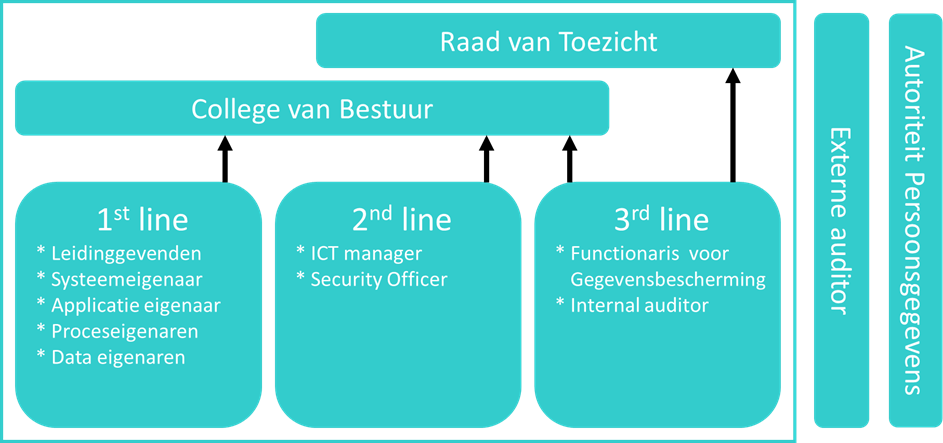
* Het levert afstemming en verheldering van de rol(len) en verantwoordelijkheden van de betrokkenen op door de afstemming wordt het draagvlak vergroot.
* Teamwerk wordt aangemoedigd, en dubbelingen in werk worden voorkomen.

De letters staan voor de volgende termen:

* **R (Responsible, NL: Verantwoordelijk)**

Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is.

* **A (Accountable, NL: Eindverantwoordelijk)**

Degene die (eind)verantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat. Als het erom gaat, moet hij/zij het eindoordeel kunnen vellen, vetorecht hebben. Er is slechts één persoon Accountable.

**Dit is altijd een leidinggevende uit de eerste lijn, die tevens proceseigenaar is, of het College van Bestuur.**

* **C (Consulted, NL: Geraadpleegd)**

Deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd. Dit is tweerichtingscommunicatie.

* **I (Informed, NL: Geïnformeerd)**

Iemand die geïnformeerd wordt over de beslissingen, over de voortgang, bereikte resultaten enz. Dit is eenrichtingscommunicatie.

In het voorbeeld op de volgende pagina’s is het RACI model uitgebreid met de kolom uitvoerder.

**Stap 2: Functiescheiding (statement 7)**

Het is niet wenselijk om de 1ste en 2de lijn rollen te combineren. De ICT directeur kan geen CISO of ISO zijn. Dit om de onafhankelijkheid te kunnen garanderen.

De rol van IBP coördinator en FG is ook niet te combineren. De FG is immers toezichthoudend.

De rollen FG en IT auditor zijn wel te combineren.

In document 7 (Assurance) wordt dit verder uitgewerkt.

Functiescheiding binnen de volgende afdelingen zijn doorgaans goed geregeld:

Afdeling Financiën

Afdeling HRM

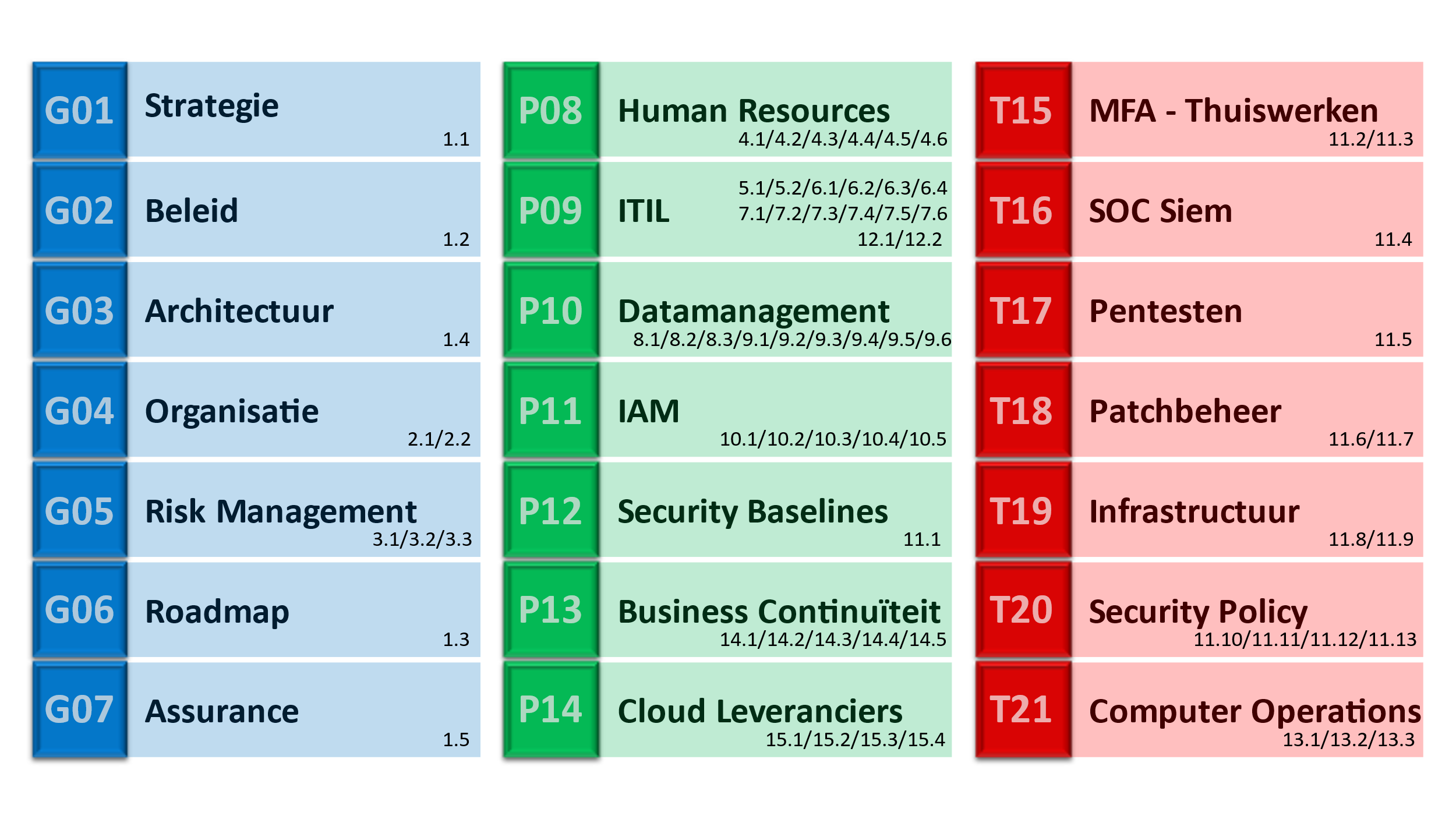
Examinering

## Van domeinen naar thema’s

De 69 NBA statements zijn ondergebracht in 15 domeinen. In onze aanpak worden de 69 statements verdeeld over 21 thema’s.

Deze 21 thema’s worden samengevoegd in 3 aandachtsgebieden.

1. **Governance** (**G**01 t/m **G**07)
2. **Processen** (**P**08 t/m **P**14)
3. **Technische weerbaarheid** (**T**15 t/m **T**21)

De processen die benoemd zijn in de MORA / HORA zij ook toepasbaar voor deze thematische aanpak.

Korte toelichting:

Thema G01 Strategie is onderdeel van het aandachtsgebied Governance (**G**01) en is het eerste (1e) thema (G**01**). Het komt overeen met het NBA statement 1.1.

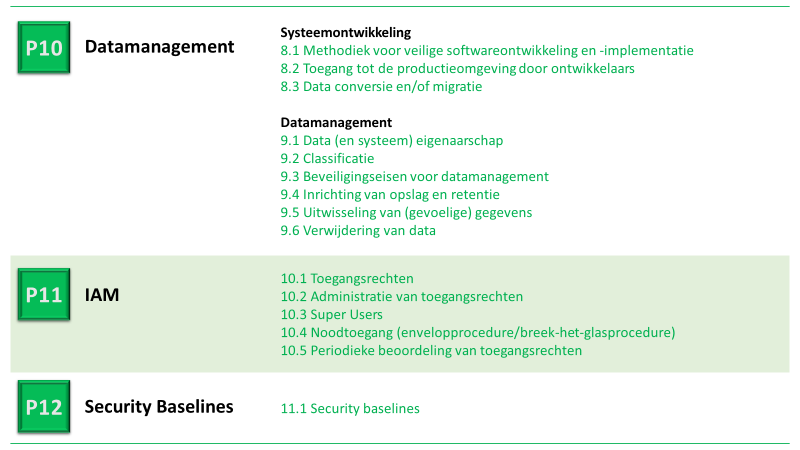
Thema P09 ITIL is onderdeel van het aandachtsgebied Processen (**P**09) en is het negende (9e) thema (P**09**). Het komt overeen met het NBA statements 5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 12.1 en 12.2.

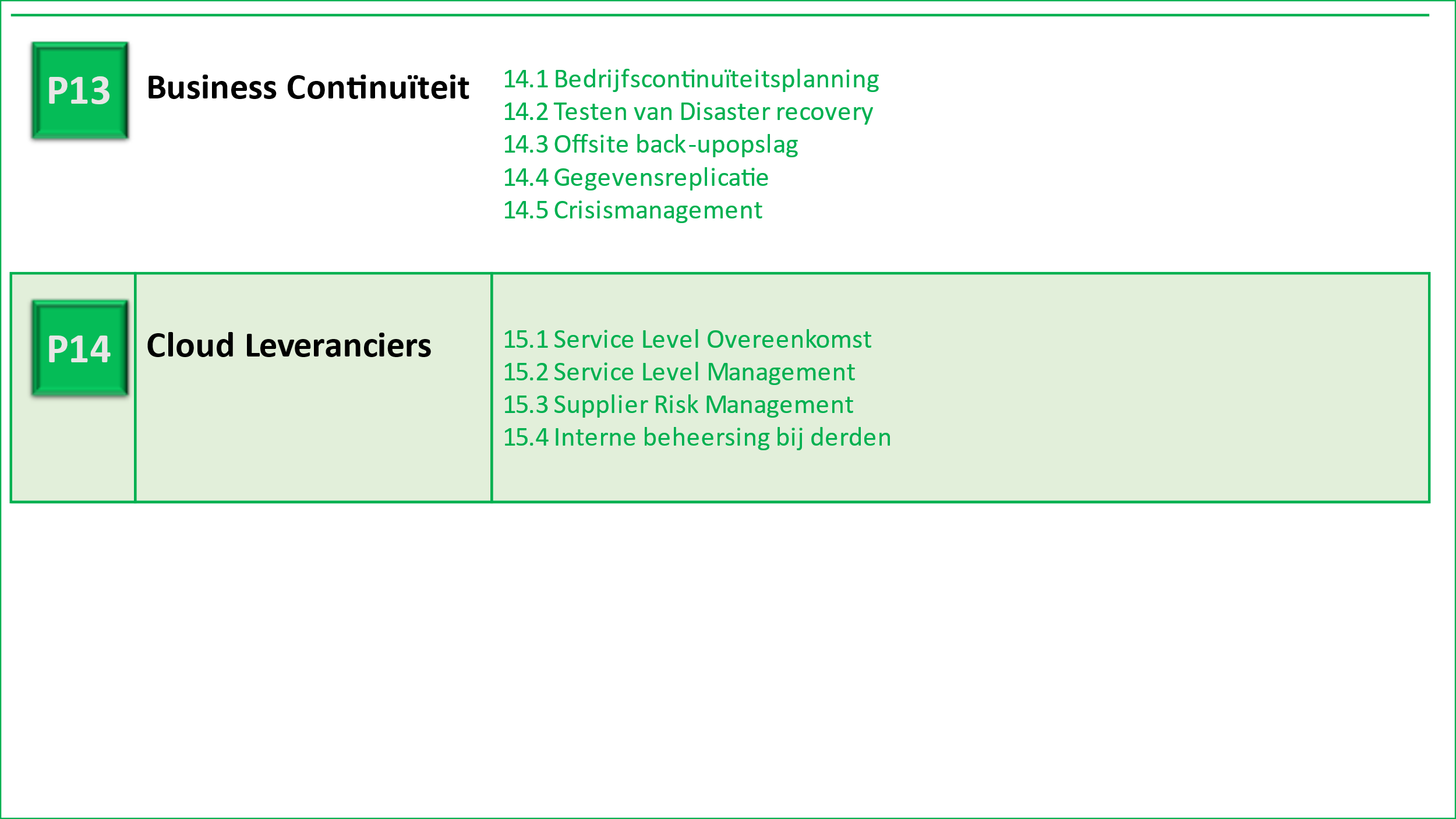
## Governance



## Processen







## Technische weerbaarheid



# Proceseigenaren (accountable) benoemd

|  |  |  |  |
| --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **Accountable**  **(eigenaar)** | **Responsible**  **(uitvoerder)** |
| **G01 Strategie** | 1.1 Strategie | College van Bestuur | Security officer |
| **G02 Beleid** | 1.2 Beleid | College van Bestuur | Security officer |
| **G03 Architectuur** | 1.4 Architectuur | College van Bestuur | Security officer |
| **G04 Eigenaarschap** | 2.1 Eigenaarschap, rollen, verantwoording en verantw. | College van Bestuur | Security officer |
| 2.2 Functiescheiding | College van Bestuur | Security officer |
| **G05 Risk Management** | 3.1 Informatie risicomanagementframework | College van Bestuur | Security officer |
| 3.2 Risicobeoordeling | College van Bestuur | Security officer |
| 3.3 Plan voor behandeling en beperking van risico's | College van Bestuur | Security officer |
| **G06 Roadmap** | 1.3 Planning / Roadmap | College van Bestuur | Security officer |
| **G07 Toetsing** | 1.5 Onafhankelijke toetsing | College van Bestuur | Internal IT auditor |
| **P08 Human Resources** | 4.1 Werving | Hoofd HRM | Medewerker HRM |
| 4.2 Certificering, training en scholing | Hoofd HRM | Hoofd ICT |
| 4.3 Afhankelijkheid van individuen | Hoofd HRM | Hoofd ICT |
| 4.4 Verandering of beëindiging van functie | Hoofd HRM | Medewerker HRM |
| 4.5 Kennisdeling | Hoofd HRM | Hoofd ICT |
| 4.6 Veiligheidsbewustzijn | Hoofd HRM | Medewerker HRM |

**Consulted: FG en Security officer**

**Informed: Information Board**

|  |  |  |  |
| --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **Accountable (eigenaar)** | **Responsible (uitvoerder)** |
| **P09 ITIL** | 5.1 Identificatie en onderhoud van configuratie-items | Hoofd ICT | Medewerder ITIL processen |
| 5.2 Configuratiedatabase en baseline | Hoofd ICT | Medewerder ITIL processen |
| 6.1 Incident management | Hoofd ICT | Medewerder ITIL processen |
| 6.2 Incident escalatie | Hoofd ICT | Medewerder ITIL processen |
| 6.3 Incidentrespons op (cyber) beveiligingsincidenten | Hoofd ICT | Medewerder ITIL processen |
| 6.4 Probleemmanagement | Hoofd ICT | Medewerder ITIL processen |
| 7.1 Normen en procedures voor aanpassingen | Hoofd ICT | Medewerder ITIL processen |
| 7.2 Impact assessment, prioriteren en autoriseren | Hoofd ICT | Medewerder ITIL processen |
| 7.3 Noodaanpassingen | Hoofd ICT | Medewerder ITIL processen |
| 7.4 Testomgeving | Hoofd ICT | Medewerder ITIL processen |
| 7.5 Testen van aanpassingen | Hoofd ICT | Medewerder ITIL processen |
| 7.6 Promotie naar productie | Hoofd ICT | Medewerder ITIL processen |
| 12.1 Fysieke beveiligingsmaatregelen | Hoofd ICT | Hoofd Facilitair |
| 12.2 Beheer van fysieke toegangsrechten | Hoofd ICT | Hoofd Facilitair |
| **P10 Data Management** | 8.1 Methodiek voor veilige softwareontwikkeling/implem. | Hoofd HRM | Security officer |
| 8.2 Toegang tot productieomgeving door ontwikkelaars | Hoofd HRM | Security officer |
| 8.3 Data conversie en/of migratie | Hoofd HRM | Externe projectleider |
| 9.1 Data (en systeem) eigenaarschap | Hoofd HRM | Security officer |
| 9.2 Classificatie | Hoofd HRM | Security officer |
| 9.3 Beveiligingseisen voor gegevensbeheer | Hoofd HRM | Security officer |
| 9.4 Inrichting van opslag en retentie | Hoofd HRM | Applicatiebeheerder HRM |
| 9.5 Uitwisseling van (gevoelige) gegevens | Hoofd HRM | Security officer |
| 9.6 Verwijdering van data | Hoofd HRM | Hoofd ICT |
| **P11 IAM** | 10.1 Toegangsrechten | Hoofd Studentzaken | Applicatiebeheerder Osiris |
| 10.2 Administratie van toegangsrechten | Hoofd Studentzaken | Applicatiebeheerder Osiris |
| 10.3 Super Users | Hoofd Studentzaken | Security officer |
| 10.4 Noodtoegang (breek-het-glasprocedure) | Hoofd Studentzaken | Security officer |
| 10.5 Periodieke beoordeling van toegangsrechten | Hoofd Studentzaken | Security officer |
| **P12 Security Baselines** | 11.1 Security baselines | College van Bestuur | Security officer |
| **P13 Business Continuity** | 14.1 Bedrijfscontinuïteitsplanning | Hoofd Facilitair | Hoofd ICT |
| 14.2 Testen van Disaster recovery | Hoofd Facilitair | Hoofd ICT |
| 14.3 Offsite back-upopslag | Hoofd Facilitair | Hoofd ICT |
| 14.4 Gegevensreplicatie | Hoofd Facilitair | Hoofd ICT |
| 14.5 Crisisbeheer | Hoofd Facilitair | Hoofd ICT |
| **P14 Cloud Leveranciers** | 15.1 Service level overeenkomst | Hoofd Inkoop | Security officer |
| 15.2 Service level beheer | Hoofd Inkoop | Security officer |
| 15.3 Risicobeheer van leveranciers | Hoofd Inkoop | Security officer |
| 15.4 Interne beheersing bij derden | Hoofd Inkoop | Security officer |

**Consulted: FG en Security officer**

**Informed: Information Board**

|  |  |  |  |
| --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **Accountable**  **(eigenaar)** | **Responsible**  **(uitvoerder)** |
| **T15 MFA - Thuiswerken** | 11.2 Authenticatiemechanismes | Hoofd ICT | Medewerker ICT |
| 11.3 Mobiele apparaten en telewerken | Hoofd ICT | Medewerker ICT |
| **T16 SOC SIEM** | 11.4 Logging | Hoofd ICT | Medewerker ICT |
| **T17 Pentesten** | 11.5 Testen van, inspectie van en toezicht op beveiliging | Hoofd ICT | Medewerker ICT |
| **T18 Patchbeheer** | 11.6 Patchbeheer | Hoofd ICT | Medewerker ICT |
| 11.7 Beheer van bedreigingen en kwetsbaarheden | Hoofd ICT | Medewerker ICT |
| **T19 Infrastructuur** | 11.8 Beschikbaarheid en bescherming van infrastructuur | Hoofd ICT | Medewerker ICT |
| 11.9 Onderhoud van de infrastructuur | Hoofd ICT | Medewerker ICT |
| **T20 Security Policy** | 11.10 Beheer van cryptografische sleutels | Hoofd ICT | Medewerker ICT |
| 11.11 Network security | Hoofd ICT | Medewerker ICT |
| 11.12 Beheersing van malware-aanvallen | Hoofd ICT | Medewerker ICT |
| 11.13 Bescherming van beveiligingstechnologie | Hoofd ICT | Security officer |
| **T21 Computer Operations** | 13.1 Job processing | Hoofd ICT | Medewerker ICT |
| 13.2 Procedures voor back-up en herstel | Hoofd ICT | Medewerker ICT |
| 13.3 Capaciteits- en prestatiebeheer | Hoofd ICT | Medewerker ICT |

**Consulted: FG en Security officer**

**Informed: Information Board**