Begeleidende informatie

Deze stroomdiagrammen geven de gewenste (happy) flows weer voor de implementatie van de GRC-tool TrustBound.
De scope van deze implementatie omvat een onderwijsinstelling onder de vlag van SURF. Binnen deze organisaties vindt de tool toepassing op het gebied van privacy en informatiebeveiliging.
Deze manier van implementeren is niet de enige manier, maar wel de manier die SURF adviseert en die je organisatie naar het eindpunt brengt. Deze flow met beschrijving blijft een hulpmiddel. Afwijken is een beslissing die organisaties zelf moeten maken.
Deze implementatie gaat uit van één organisatie(onderdeel) bij technische oplevering.

De implementatie begint bij het verwerkingsregister, vanwege de wettelijke verplichting en het gebruik als masterdata voor het koppelen van andere modules zoals incidenten (datalekken), bedrijfsmiddelen, externe partijen en risico-assessments.

Meer informatie over het gebruik van de modules en details staan in de TrustBound Community (https://community.trustbound.com) de op SURF discussiefora (https://sec.surf.nl en https://pec.surf.nl).

Module: Governance (Verwerkingsregister/Processes/Externe Organisaties/Bedrijfsmiddelen)
Het instapniveau vormt het startpunt voor organisaties die met TrustBound werken aan informatiebeveiliging en privacy. Aan het begin van het stroomdiagram gelden slechts twee voorwaarden: TrustBound functioneert en iemand beschikt over de juiste rechten voor inrichting. In deze fase draait het om een werkend verwerkingsregister met één gebruiker (de privacy officer) die alles configureert en hier verantwoordelijk voor is. Het eindpunt van dit niveau wordt doorgaans binnen een jaar bereikt.

Na afronding volgt het groeilevel. In deze fase breidt het gebruik van TrustBound zich uit naar meerdere gebruikers, elk met eigen verantwoordelijkheden. Hiervoor is een meer volwassen organisatie nodig met een basis van governance en processen rond GRC. De verantwoordelijkheid verschuift van de privacy officer naar de lijnorganisatie. Tijdens deze periode wordt TrustBound gevuld met processen, externe organisaties en IBP-overeenkomsten (informatiebeveiligingsaddenda, verwerkersovereenkomsten en overeenkomsten conform artikel 26). De focus ligt op een volledig verwerkingsregister, een werkend processenregister en een register met externe organisaties en overeenkomsten. Ook de masterdata wordt steeds completer. Op dit niveau kan de FG eventueel al betrokken worden. Het bereiken van het eindpunt duurt gemiddeld twee tot drie jaar na afronding van het instapniveau.

Het geavanceerde niveau vormt de laatste stap. Veel organisaties blijven bij het groeilevel, maar wie verdergaat legt hier de nadruk op volledige koppeling tussen processen, verwerkingen, bedrijfsmiddelen, externe partijen en overeenkomstenmodules. Het eindpunt van dit niveau wordt doorgaans bereikt binnen een jaar na afronding van de groeifase.

Module: Risk (Risicobeheer, Analyses, Beheersmaatregelen, Taken)
Het instapniveau geeft organisaties de mogelijkheid om risico's te registreren en ad-hoc te wegen. Daarnaast kunnen security- en privacy officers analyses uitvoeren, zoals Data Protection Impact Assessments (DPIA) en Security Risk Assessments (SRA). Aan het begin van het stroomdiagram gelden drie voorwaarden: TrustBound functioneert, iemand heeft de juiste rechten voor inrichting en een DPIA en SRA zijn ingeladen. Het eindpunt van dit niveau wordt doorgaans bereikt binnen een jaar na de start.

Na afronding volgt het groeilevel. Hierbij breidt het gebruik van de tool zich uit naar meerdere gebruikers met eigen verantwoordelijkheden. Dit vraagt om een meer volwassen organisatie met een basis van governance en processen voor het beheer van GRC. De verantwoordelijkheid verschuift van de officers naar de lijnorganisatie. Tijdens deze fase ontstaat meer structuur in het uitvoeren van analyses en het opvolgen van risico's. Ook integreert de riskmodule zich met de governancemodule, waardoor een totaaloverzicht ontstaat. Dit register bevat gewogen risico's, inclusief vervolgacties zoals behandelplannen. Het bereiken van het eindpunt duurt gemiddeld één tot twee jaar na afronding van het instapniveau.

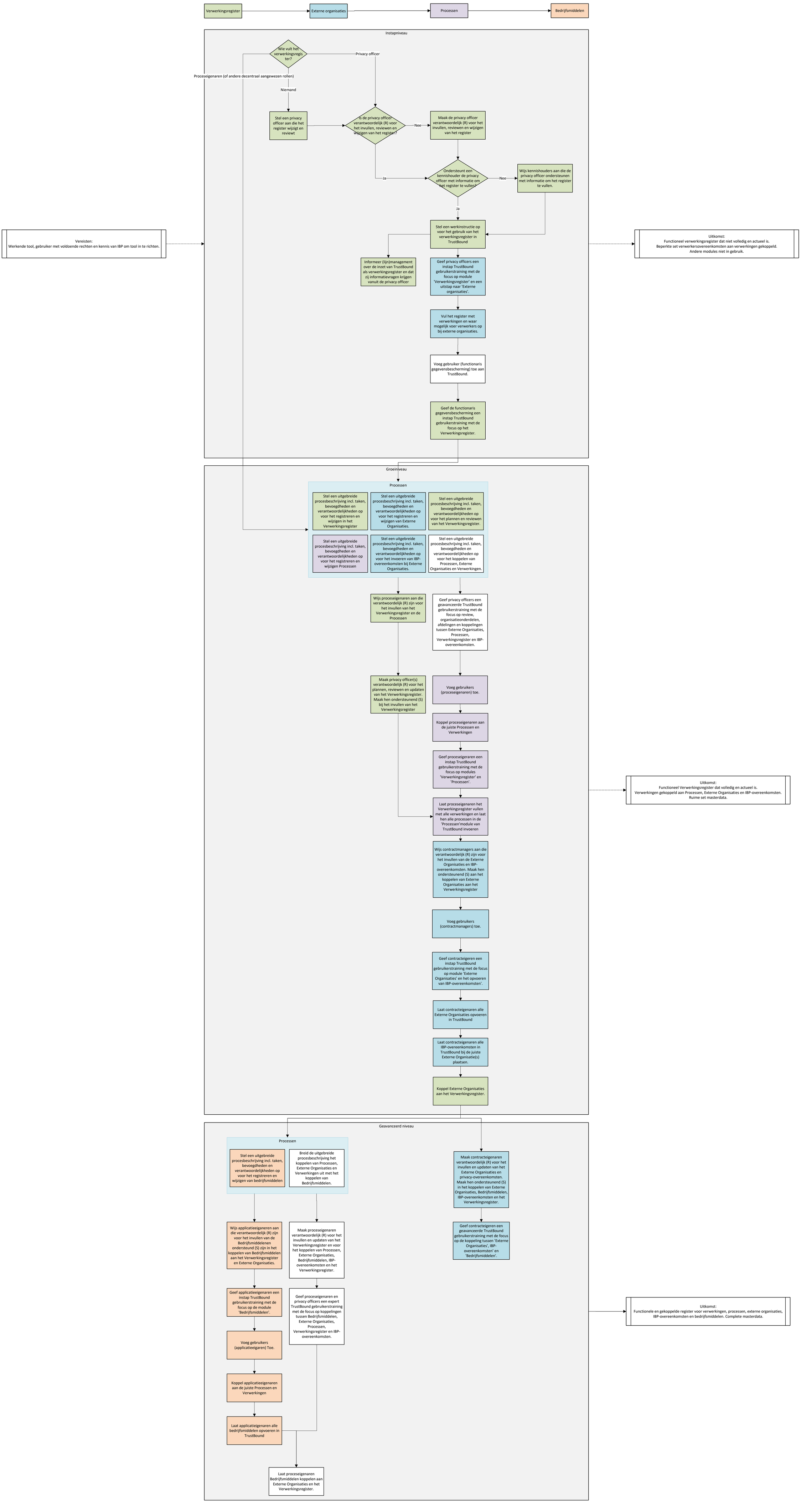
Het geavanceerde niveau vormt de laatste stap. Veel organisaties kiezen ervoor om bij het groeilevel te blijven, maar dit niveau legt de nadruk op leveranciersbeoordelingen en verdergaande detaillering van risico's met standaarddreigingen (MAPGOOD). Het eindpunt van dit niveau wordt doorgaans bereikt binnen een jaar na afronding van de groeifase.

Module: Compliance (Incidenten, Verzoeken, Audits, Bevindingen)
Het instapniveau stelt organisaties in staat om informatiebeveiligingsincidenten, datalekken en verzoeken van betrokkenen te registreren en beheren.

Na afronding volgt het groeilevel. In deze fase breidt het gebruik van de tool zich uit naar meerdere gebruikers met eigen verantwoordelijkheden. Dit vraagt om een meer volwassen organisatie met een basis van governance en processen voor het beheer van GRC. De verantwoordelijkheid verschuift van de officers naar de lijnorganisatie. Daarnaast biedt het groeilevel mogelijkheden voor het uitvoeren van audits en het opvolgen van bevindingen.
Het groeilevel van de compliance-module hangt sterk samen met de voortgang van de governance-module. Compliance bouwt voort op de decentrale rollen en de masterdata die binnen de governance-module ontstaan. Het eindpunt van deze fase wordt doorgaans bereikt binnen een jaar na afronding van het instapniveau.

Deze module kent geen geavanceerd niveau.

Governance


Verwerkingsregister
Externe organisaties
Processen
Bedrijfsmiddelen
Instapniveau
Wie vult het verwerkingsregister?
Privacy officer
Proceseigenaren (of andere decentraal aangewezen rollen)
Niemand
Stel een privacy officer aan die het register wijzigt en reviewt
Is de privacy officer verantwoordelijk (R) voor het invullen, reviewen en wijzigen van het register?
Nee
Maak de privacy officer verantwoordelijk (R) voor het invullen, reviewen en wijzigen van het register
Ja
Ondersteunt een kennishouder de privacy officer met informatie om het register te vullen?
Nee
Wijs kennishouders aan die de privacy officer ondersteunen met informatie om het register te vullen.
Ja
Stel een werkinstructie op voor het gebruik van het verwerkingsregister in TrustBound
Informeer (lijn)management over de inzet van TrustBound als verwerkingsregister en dat zij informatievragen krijgen vanuit de privacy officer
Geef privacy officers een instap TrustBound gebruikerstraining met de focus op module 'Verwerkingsregister' en een uitstap naar 'Externe organisaties'.
Vul het register met verwerkingen en waar mogelijk voer verwerkers op bij externe organisaties.
Voeg gebruiker (functionaris gegevensbescherming) toe aan TrustBound.
Geef de functionaris gegevensbescherming een instap TrustBound gebruikerstraining met de focus op het Verwerkingsregister.
Vereisten:
Werkende tool, gebruiker met voldoende rechten en kennis van IBP om tool in te richten.
Uitkomst:
Functioneel verwerkingsregister dat niet volledig en actueel is.
Beperkte set verwerkersovereenkomsten aan verwerkingen gekoppeld.
Andere modules niet in gebruik.
Groeinlveau
Processen
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren en wijzigen in het Verwerkingsregister
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren en wijzigen van Externe Organisaties.
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het plannen en reviewen van het Verwerkingsregister.
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren en wijzigen Processen
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het invoeren van IBP-overeenkomsten bij Externe Organisaties.
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het koppelen van Processen, Externe Organisaties en Verwerkingen.
Wijs proceseigenaren aan die verantwoordelijk (R) zijn voor het invullen van het Verwerkingsregister en de Processen
Geef privacy officers een geavanceerde TrustBound gebruikerstraining met de focus op review, organisatieonderdelen, afdelingen en koppelingen tussen Externe Organisaties, Processen, Verwerkingsregister en IBP-overeenkomsten.
Maak privacy officer(s) verantwoordelijk (R) voor het plannen, reviewen en updaten van het Verwerkingsregister. Maak hen ondersteunend (S) bij het invullen van het Verwerkingsregister
Voeg gebruikers (proceseigenaren) toe.
Koppel proceseigenaren aan de juiste Processen en Verwerkingen
Geef proceseigeraren een instap TrustBound gebruikerstraining met de focus op modules 'Verwerkingsregister' en 'Processen'.
Laat proceseigenaren het Verwerkingsregister vullen met alle verwerkingen en laat hen alle processen in de 'Processen'module van TrustBound invoeren
Wijs contractmanagers aan die verantwoordelijk (R) zijn voor het invullen van de Externe Organisaties en IBP-overeenkomsten. Maak hen ondersteunend (S) aan het koppelen van Externe Organisaties aan het Verwerkingsregister
Voeg gebruikers (contractmanagers) toe.
Geef contracteigeren een instap TrustBound gebruikerstraining met de focus op module 'Externe Organisaties' en het opvoeren van IBP-overeenkomsten'.
Laat contracteigenaren alle Externe Organisaties opvoeren in TrustBound
Laat contracteigenaren alle IBP-overeenkomsten in TrustBound bij de juiste Externe Organisatie(s) plaatsen.
Koppel Externe Organisaties aan het Verwerkingsregister.
Uitkomst:
Functioneel Verwerkingsregister dat volledig en actueel is.
Verwerkingen gekoppeld aan Processen, Externe Organisaties en IBP-overeenkomsten.
Ruime set masterdata.
Geavanceerd niveau
Processen
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren en wijzigen van bedrijfsmiddelen
Breid de uitgebreide procesbeschrijving het koppelen van Processen, Externe Organisaties en Verwerkingen uit met het koppelen van Bedrijfsmiddelen.
Maak contracteigenaren verantwoordelijk (R) voor het invullen en updaten van het Externe Organisaties en privacy-overeenkomsten. Maak hen ondersteunend (S) in het koppelen van Externe Organisaties, Bedrijfsmiddelen, IBP-overeenkomsten en het Verwerkingsregister.
Wijs applicatieeiganeren aan die verantwoordelijk (R) zijn voor het invullen van de Bedrijfsmiddelenen ondersteund (S) zijn in het koppelen van Bedrijfsmiddelen aan het Verwerkingsregister en Externe Organisaties.
Maak proceseigenaren verantwoordelijk (R) voor het invullen en updaten van het Verwerkingsregister en voor het koppelen van Processen, Externe Organisaties, Bedrijfsmiddelen, IBP-overeenkomsten en het Verwerkingsregister.
Geef contracteigeren een geavanceerde TrustBound gebruikerstraining met de focus op de koppeling tussen 'Externe Organisaties', IBP-overeenkomsten' en 'Bedrijfsmiddelen'.
Geef applicatieeigenaren een instap TrustBound gebruikerstraining met de focus op de module 'Bedrijfsmiddelen'.
Geef proceseigenaren en privacy officers een expert TrustBound gebruikerstraining met de focus op koppelingen tussen Bedrijfsmiddelen, Externe Organisaties, Processen, Verwerkingsregister en IBP-overeenkomsten.
Voeg gebruikers (applicatieeigaren) Toe.
Koppel applicatieeigenaren aan de juiste Processen en Verwerkingen
Laat applicatieigenaren alle bedrijfsmiddelen opvoeren in TrustBound
Laat proceseigenaren Bedrijfsmiddelen koppelen aan Externe Organisaties en het Verwerkingsregister.
Uitkomst:
Functionele en gekoppelde register voor verwerkingen, processen, externe organisaties, IBP-overeenkomsten en bedrijfsmiddelen. Complete masterdata.

Risk

Risicobeheer → Analyses → Beheersmaatregelen → Integratie

Vereisten:
Werkende tool, gebruiker met voldoende rechten en kennis van IBP om tool in te richten.
Ingeladen (D)PIA model en ingeladen SRA model.

Instapniveau

Wie doen analyses en risico's?

- Risico eigenaar of andere decentrale rol
- Privacy officer en security officer
- Niemand → Stel een privacy officer en een security officer aan die risico's registreren, dreigingen analyseren, SRA's en DPIA's uitvoeren.

Officers verantwoordelijk (R) voor Analyses en Risico's?

- Nee → Maak de officers verantwoordelijk (R) voor Risico's → Maak de officers verantwoordelijk (R) voor Analyses.
- Ja

Ondersteunt een kennishouder de officers met informatie bij Risico's en Analyses?

- Nee → Wijs kennishouders aan die de officers ondersteunen met informatie bij Risico's en Analyses.
- Ja

Stel een werkinstructie op voor het uitvoeren van DPIA's en SRA's, inclusief het opvoeren van risico's en dreigingsanalyses.

- Informeer (lijn)management over de inzet van TrustBound voor Risicobeheer en dat zij informatievragen krijgen vanuit de officers
- Geef officers een instap TrustBound gebruikerstraining met de focus op uitvoeren DPIA's en SRA's, inclusief het opvoeren van risico's en dreigingsanalyses.
- Informeer (lijn)management over de inzet van TrustBound voor Analyses en dat zij informatievragen krijgen vanuit de officers
- Geef FGs een instap TrustBound gebruikerstraining met de focus op Advies geven bij DPIA's.

Maak 2 type/soorten risico's aan: Security risico's en Privacy risico's.

Uitkomst:
Functioneel risicoregister dat niet volledig en actueel is.
Risico's hebben een weging op basis van een dreiginganalyses.
Mogelijkheid tot digitaal uitvoeren van DPIA's en SRA's.

Groeiniveau

Additionele vereisten:
Risicomanagementbeleid, risicomanagement procedure, eigen risicomatrix, Trustbound gevuld met processen, verwerkingen, bedrijfsmiddelen.
Eigen (Pre-)DPIA model, eigen PIA model, eigen Security Risk Assessment model.
Beleid omtrent uitvoeren (pre-)DPIA's en Security Risk Assessments.

Processen

- Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren, analyseren en updaten van Risico's.
- Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het maken en opvolgen van Behandelplannen.
- Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het plannen, uitvoeren en reviewen van SRA's.
- Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het koppelen van Risico's aan Processen, Verwerkingen, Bedrijfsmiddelen, Incidenten en Analyses.
- Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het plannen, uitvoeren en reviewen van Pre-DPIA's, PIA's en DPIA's.

- Wijs proceseigenaren aan die verantwoordelijk (R) zijn voor het uitvoeren van (Pre-)DPIA's, PIA's en Proces SRA's. Maak hen ondersteunend (S) bij het plannen van Analyses.
- Wijs applicatieeigenaren aan die verantwoordelijk (R) zijn voor het uitvoeren van Bedrijfsmiddel SRA's. Maak hen ondersteunend (S) bij uitvoeren van (Pre-)DPIA's en PIA's. Maak hen ondersteunend (S) bij het plannen van Analyses.
- Wijs risicoeigenaren aan die verantwoordelijk (R) zijn voor het maken van het behandelplannen. Maak hen ondersteunend (S) bij het maken van Dreigingsanalyses.
- Maak officers verantwoordelijk (R) voor het updaten van dreigingsanalyses en opvolgen Behandelplannen. Maak hen ondersteunend (S) bij het maken van Behandelplannen.
- Maak officers verantwoordelijk (R) voor het plannen en reviewen van Analyses. Maak hen ondersteunend (S) bij het uitvoeren van Analyses.
- Maak officers verantwoordelijk (R) voor het plannen en reviewen van Analyses, het opvolgen van Behandelplannen en het koppelen van Risico's aan Anayses. Maak hen ondersteunend (S) bij het uitvoeren van Analyses, Behandelplannen en Dreigingsanalyses

- Geef officers een TrustBound gebruikerstraining met de focus op Het toevoegen van Werkpakketten, Risico Matrices en Model Analyses én begeleiden van Behandelplannen.
- Voeg eigen organisatie Risico Matrix toe aan TrustBound.
- Voeg eigen organisatie Analysemodellen toe aan TrustBound. (Denk aan eigen PIA, (Pre-)DPIA en SRA)
- Voeg Werkpakket(ten) (normenkader(s)) toe aan TrustBound
- Geef officers een geavanceerde TrustBound gebruikerstraining met focus op reviewen en koppelen van Analyses aan Risico's en koppelen van Scope (Processen, Verwerkingen, Bedrijfsmiddelen) en Incidenten aan Risico's.
- Voeg gebruikers (risicoeigenaren) toe.

Geef risicoeigenaren een instap TrustBound gebruikerstraining met de focus op het maken van Behandelplannen.

Geef Proces- en Applicatieeigenaren een instap TrustBound gebruikerstraining met de focus op het uitvoeren van DPIA's, PIA's en SRA's van Behandelplannen.

Maak 4 risico categorieen aan: Strategische security, Operationele security, Strategische privacy, Operationele privacy.

Uitkomst:
Meerdere mogelijkheden tot uitvoeren van Analyses. Risico's komende uit Analyses staan in het risicoregister.
Functioneel risicoregister dat volledig en actueel is.
Risico's hebben een actuele weging op basis van dreigingsanalyse.
Risico's hebben scope (gekoppeld aan processen, verwerkingen en/of Bedrijfsmiddelen)
Risico's zijn eventueel gekoppeld aan incidenten.
Risico's hebben een behandelplan op basis van beheersmaatregelen uit het SURF Normenkader.

Geavanceerd niveau

Additionele vereisten:
TrustBound gevuld met Externe Organisaties.

Processen

- Pas de uitgebreide procesbeschrijving voor het registreren, analyseren en updaten van Risico's aan met MAPGOOD dreigingen en de rol van risicomanagers.
- Pas de procesbeschrijving voor het maken en opvolgen van Behandelplannen met de rol van risicomanagers, incl. het toevoegen van Taken en koppelen aan MAPGOOD dregingen.
- Pas de uitgebreide procesbeschrijvingen het Uitvoeren, plannen en reviewen van Analyses aan met de rol van contracteigenaren.

- Wijs contractmanagers aan die verantwoordelijk (R) zijn voor het uitvoeren van Analyses op Externe Organisaties.
  Maak hen ondersteunend (S) bij het Dreigingsanalyses.
- Wijs risicomanagers aan die verantwoordelijk (R) zijn voor het maken en updaten van Dreigingsanalyses en het opvolgen van Behandelplannen. Maak hen ondersteunend (S) bij het maken van Behandelplannen.
- Maak officers ondersteunend (S) bij het maken van Dreigingsanalyses en Behandelplannen.

- Voeg eigen organisatie Externe Organisatie Analyses (leveranciersbeoordelingen) toe aan TrustBound.
- Geef security officers een specifieke TrustBound gebruikerstraining met focus op MAPGOOD dreigingen en risico's.
- Voeg MAPGOOD dreigingskader toe aan TrustBound.
- Voeg gebruikers (risicomanagers en contractmanagers) toe.

Geef risicomanagers een TrustBound gebruikerstraining met focus op het opvolgen van Behandelplannen.

Geef contracteigenaren een TrustBound gebruikerstraining met focus op het uitvoeren van Analyses en Dreigingsanalyses .

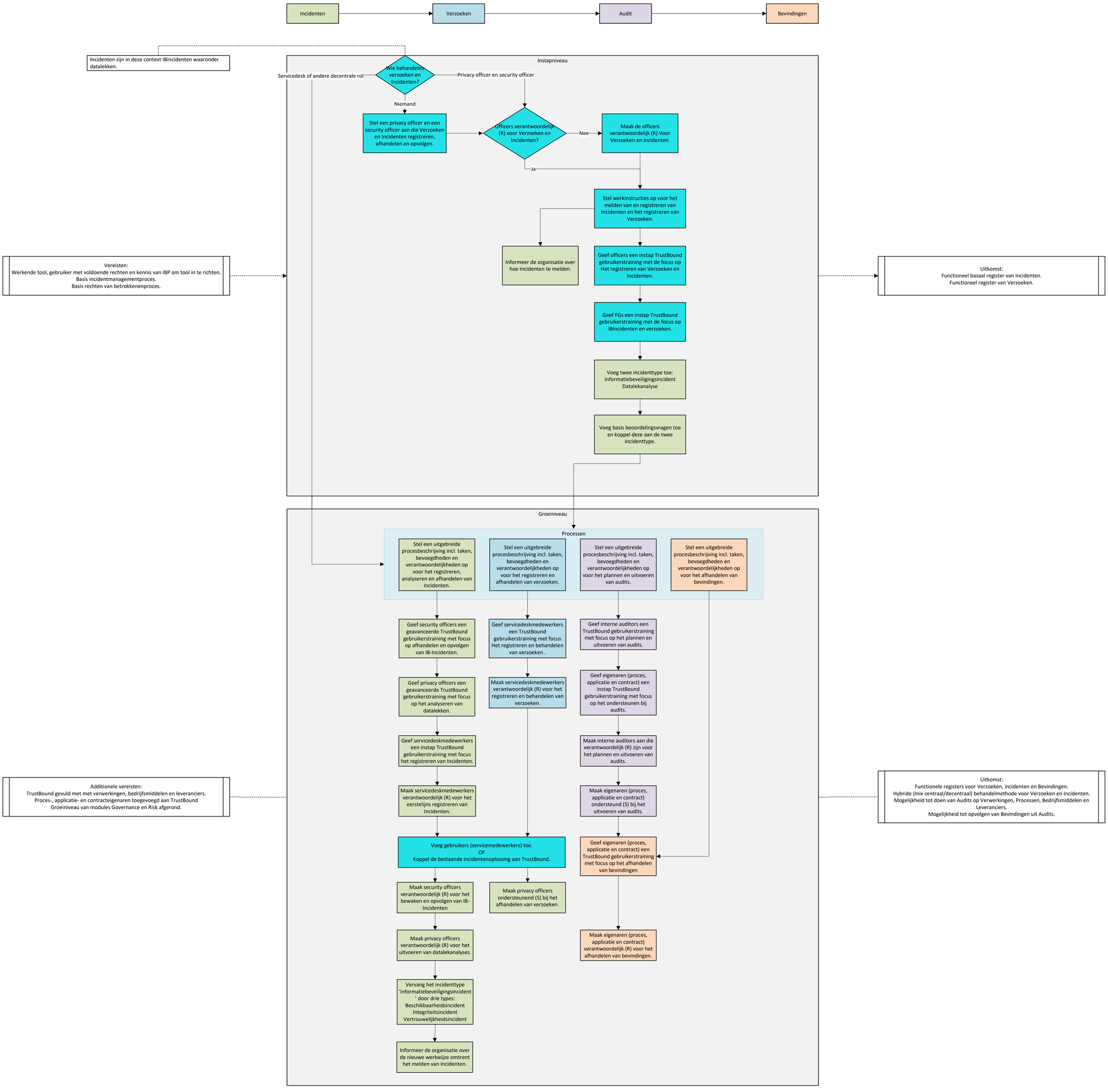
Voeg 2 risico Categorieen toe:
Privacy compliance.
Derde-partij.
Vervang 2 risico categorien: Strategisch privacy door Strategisch betrokkene.
Operationeel privacy door Operationeel betrokkene.

Voeg Classificaties (impact) toe.

Classificaties:
Beschikbaarheid
Integriteit
Vertrouwelijkheid
Financieen
Reputatie
Operationele verstoring
Lagere instroom studenten
Groter verloop personeel
Verscherpt toezicht
Identiteitsfraude
Financieel nadeel
Discriminatie, stigmatisering en/of uitsluiting
Psychisch leed, reputatieschade en/of sociale gevolgen
Beperking van rechten en vrijheden
Machtsmisbruik

Uitkomst:
Functioneel gedetailleerd risicoregister dat volledig en actueel is.
Risico's hebben een actuele weging op basis van dreigingsanalyse.
Security risico's hebben een dreiging op basis van MAPGOOD.
Risico's hebben scope (gekoppeld aan Processen, Verwerkingen, Externe Organisatie en/of Bedrijfsmiddelen)
Risico's zijn eventueel gekoppeld aan incidenten.
Risico's hebben een behandelplan op basis van beheersmaatregelen uit het SURF Normenkader.
Mogelijkheid tot uitvoeren van Analyses op Externe Organisaties (leveranciersbeoordelingen)

Compliance


Incidenten
Verzoeken
Audit
Bevindingen
Incidenten zijn in deze context IBincidenten waaronder datalekken.
Instapniveau
Wie behandelen verzoeken en Incidenten?
Servicedesk of andere decentrale rol
Privacy officer en security officer
Niemand
Stel een privacy officer en een security officer aan die Verzoeken en Incidenten registreren, afhandelen en opvolgen.
Officers verantwoordelijk (R) voor Verzoeken en Incidenten?
Nee
Maak de officers verantwoordelijk (R) Voor Verzoeken en Incidenten.
Ja
Stel werkinstructies op voor het melden van en registreren van Incidenten en het registreren van Verzoeken.
Informeer de organisatie over hoe Incidenten te melden.
Geef officers een instap TrustBound gebruikerstraining met de focus op Het registreren van Verzoeken en Incidenten.
Geef FGs een instap TrustBound gebruikerstraining met de focus op IBincidenten en verzoeken.
Voeg twee incidenttype toe:
Informatiebeveiligingsincident
Datalekanalyse
Voeg basis beoordelingsvragen toe en koppel deze aan de twee incidenttype.
Vereisten:
Werkende tool, gebruiker met voldoende rechten en kennis van IBP om tool in te richten.
Basis incidentmanagementproces.
Basis rechten van betrokkenenproces.
Uitkomst:
Functioneel basaal register van Incidenten.
Functioneel register van Verzoeken.
Groeiniveau
Processen
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren, analyseren en afhandelen van Incidenten.
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het registreren en afhandelen van verzoeken.
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het plannen en uitvoeren van audits.
Stel een uitgebreide procesbeschrijving incl. taken, bevoegdheden en verantwoordelijkheden op voor het afhandelen van bevindingen.
Geef security officers een geavanceerde TrustBound gebruikerstraining met focus op afhandelen en opvolgen van IB-Incidenten.
Geef servicedeskmedewerkers een TrustBound gebruikerstraining met focus Het registreren en behandelen van verzoeken .
Geef interne auditors een TrustBound gebruikerstraining met focus op het plannen en uitvoeren van audits.
Geef privacy officers een geavanceerde TrustBound gebruikerstraining met focus op het analyseren van datalekken.
Maak servicedeskmedewerkers verantwoordelijk (R) voor het registreren en behandelen van verzoeken.
Geef eigenaren (proces, applicatie en contract) een instap TrustBound gebruikerstraining met focus op het ondersteunen bij audits.
Geef servicedeskmedewerkers een instap TrustBound gebruikerstraining met focus het registreren van Incidenten.
Maak interne auditors aan die verantwoordelijk (R) zijn voor het plannen en uitvoeren van audits.
Maak servicedeskmedewerkers verantwoordelijk (R) voor het eerstelijns registreren van Incidenten.
Maak eigenaren (proces, applicatie en contract) ondersteund (S) bij het uitvoeren van audits.
Voeg gebruikers (servicemedewerkers) toe.
OF
Koppel de bestaande incidentenoplossing aan TrustBound.
Geef eigenaren (proces, applicatie en contract) een TrustBound gebruikerstraining met focus op het afhandelen van bevindingen
Maak security officers verantwoordelijk (R) voor het bewaken en opvolgen van IB-Incidenten
Maak privacy officers ondersteunend (S) bij het afhandelen van verzoeken.
Maak privacy officers verantwoordelijk (R) voor het uitvoeren van datalekanalyses.
Maak eigenaren (proces, applicatie en contract) verantwoordelijk (R) voor het afhandelen van bevindingen.
Vervang het incidenttype ‘informatiebeveiligingsincident ’ door drie types:
Beschikbaarheidsincident
Integriteitsincident
Vertrouwelijkheidsincident
Informeer de organisatie over de nieuwe werkwijze omtrent het melden van Incidenten.
Additionele vereisten:
TrustBound gevuld met met verwerkingen, bedrijfsmiddelen en leveranciers.
Proces-, applicatie- en contracteigenaren toegevoegd aan TrustBound
Groeiniveau van modules Governance en Risk afgerond.
Uitkomst:
Functionele registers voor Verzoeken, incidenten en Bevindingen.
Hybride (mix centraal/decentraal) behandelmethode voor Verzoeken en Incidenten.
Mogelijkheid tot doen van Audits op Verwerkingen, Processen, Bedrijfsmiddelen en Leveranciers.
Mogelijkheid tot opvolgen van Bevindingen uit Audits.