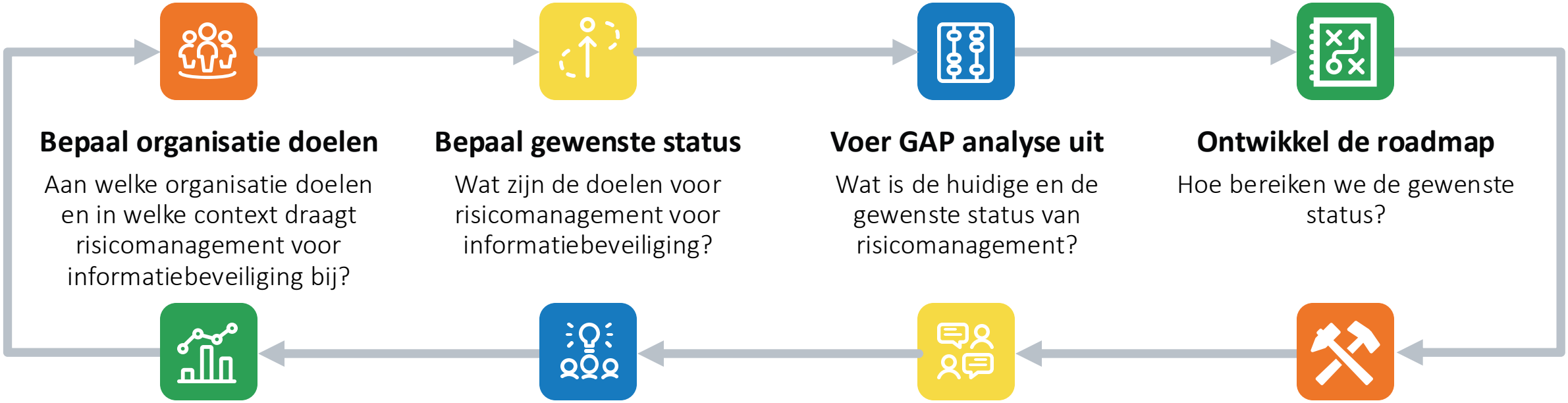
Risicomanagement voor informatiebeveiliging: Waar begin ik?

Versie 1.0 – 24-10-2024

Met een gestructureerde aanpak



Bepaal organisatie doelen

Aan welke organisatie doelen en in welke context draagt risicomanagement voor informatiebeveiliging bij?

Bepaal gewenste status

Wat zijn de doelen voor risicomanagement voor informatiebeveiliging?

Voer GAP analyse uit

Wat is de huidige en de gewenste status van risicomanagement?

Ontwikkel de roadmap

Hoe bereiken we de gewenste status?

Voer de roadmap uit

Hoe organiseren we de realisatie?

Houd iedereen betrokken

Hoe houden we iedereen betrokken en borgen we buy-in?

Versterk en verbeter

Hoe versterken en verbeteren we het programma?

Assess, audit en pas aan

Wat hebben we bereikt, wat is er veranderd en hoe passen we ons aan?

BEPAAL DE ORGANISATIE DOELEN

In welke context draagt risicomanagement voor Informatiebeveiliging bij aan de organisatie doelen?

Welk commitment en mandaat is er vanuit het bestuur?

STAPPEN

Inventariseer en analyseer:

- **Organisatie context**
- **Relevante wet- en regelgeving**
- **Organisatie missie, visie, strategie, doelen en beleid**

Borg commitment en mandaat vanuit bestuur.

BEPAAL DE GEWENSTE STATUS

Wat zijn voor nu en straks passende de nodige processen, methoden en technieken voor het gewenste volwassenheidsniveau?

Wat zijn de doelen en houding t.o.v. risicomanagement?

STAPPEN

Inventariseer en verzamel:

- **Risk appetite**
- **Stakeholders**
- **Reeds beschreven en –middelen**
- **Kennisniveau in organisatie**

Selecteer een standaard of framework

Definieer:

- **Doelen voor risicomanagement**
- **Rollen en verantwoordelijkheden**
- **-- Stem af met en betrek alle stakeholders -**

VOER EEN GAP ANALYSE UIT

Wat is de huidige en de gewenste status van risicomanagement voor informatiebeveiliging?

STAPPEN

Inventariseer de huidige status van:

- **systemen, processen, mensen, hulpmiddelen, technologieën, bewustzijn en interacties met derden.**

Bepaal IST en SOLL en voer een GAP analyse uit.

ONTWIKKEL DE ROADMAP

Hoe bereiken we de gewenste status?

Met welke activiteiten, prioriteiten en middelen?

STAPPEN

Ontwikkelen een strategie incl. roadmap

Stem af met stakeholders en verwerk hun feedback

Organiseer buy-in van bestuur incl. toewijzing van middelen, business case based

Ontwikkel en/of actualiseer het risicomanagementbeleid, -richtlijnen, -standaarden.

VOER DE ROADMAP UIT

Hoe organiseren we de realisatie?

STAPPEN

- **Ontwerp een programma- en/of projectstructuur en pas aan waar nodig.**
- **Integreer mogelijkheden, tools en technologieën.**
- **Adopteer best practices.**
- **Richt je op stakeholders waar goede energie zit**
- **Stel de rollen en verantwoordelijkheden van het (project) team vast.**
- **Identificeer stakeholders die verantwoordelijk zijn, geraadpleegd en geïnformeerd moeten worden (RASCI).**
- **Borg, ontwikkel of verwerf expertise en vaardigheden voor een succesvolle uitvoer.**
- **Pas kpi’s en mijlpalen toe om voortgang te bewaken en bij te sturen.**

HOUD IEDEREEN BETROKKEN

Hoe houden we iedereen betrokken en borgen we buy-in?

STAPPEN

Stel een communicatieplan op en voer die uit.

Rapporteer en communiceer over status, voortgang, mijlpalen en belemmeringen.

Communiceer over de al geleverde toegevoegde waarde van het programma, aan de organisatie en het bestuur (directie).

VERSTERK EN VERBETER

Hoe versterken en verbeteren we het programma?

Hoe borgen we het in de organisatie?

STAPPEN

- **Optimaliseer en borg de governance, verantwoordelijkheden en zekerheden.**
  - **Steun de lijnorganisatie met het inbedden van risicomanagement in hun processen**
- **Creëer een veilige omgeving en cultuur.**
- **Versterk bewustzijn met trainingen en campagnes**
- **Borg je monitoring en rapportage**
- **Leer van activiteiten die lastiger gingen**
- **Vier je successen**

ASSESS, AUDIT EN PAS AAN

Wat hebben we bereikt, wat is er veranderd en hoe passen we ons aan?

Klaar voor een volgende iteratie met aangescherpte scope en/of doelen!

STAPPEN

- **Organiseer en borg een proces van continu verbeteren**
- **Voer in- en externe (risk-) beoordelingen en audits uit**
- **Actualiseer de IST, SOLL en GAP-analyse en bepaal de volgende optimalisaties**
- **Pas kpi’s, mijlpalen en feedback toe om voortgang te bewaken, bij te sturen en om de effectiviteit van het programma te beoordelen en te verbeteren**