Informatiebeveiliging

Adequate beheersing van informatiebeveiliging betekent optimale effectiviteit van de controls/beheersmaatregelen

Oktober 2024

In Audit

Inleiding

Wie ben ik?

Wat is informatiebeveiliging?

Beveiliging ten behoeve van:
Beschikbaarheid, Integriteit en Vertrouwelijkheid van data = **BIV**

Op basis van de classificatie op deze onderdelen wordt de beveiliging ingericht, denk aan:
Vertrouwelijkheid: 0 = openbaar/publiek, 1= intern . 2 = vertrouwelijk 3= zeer vertrouwelijk 4 = geheim

Framework: IS0 27001, COBIT, NIST etc. Deze frameworks helpen organisaties bij het beschermen van hun informatie en het naleven van wet– en regelgeving en het verbeteren van hun algehele beveiligingshouding

Vandaag nemen we de Good Practice van DNB als uitgangspunt, waarin DNB voor de financiële sector uiteen heeft gezet wat zij verwachten en beschouwen als Good Practice. Daarnaast zal ik de rol van het bestuur van een organisatie als uitgangspunt nemen.

In Audit

Inleiding

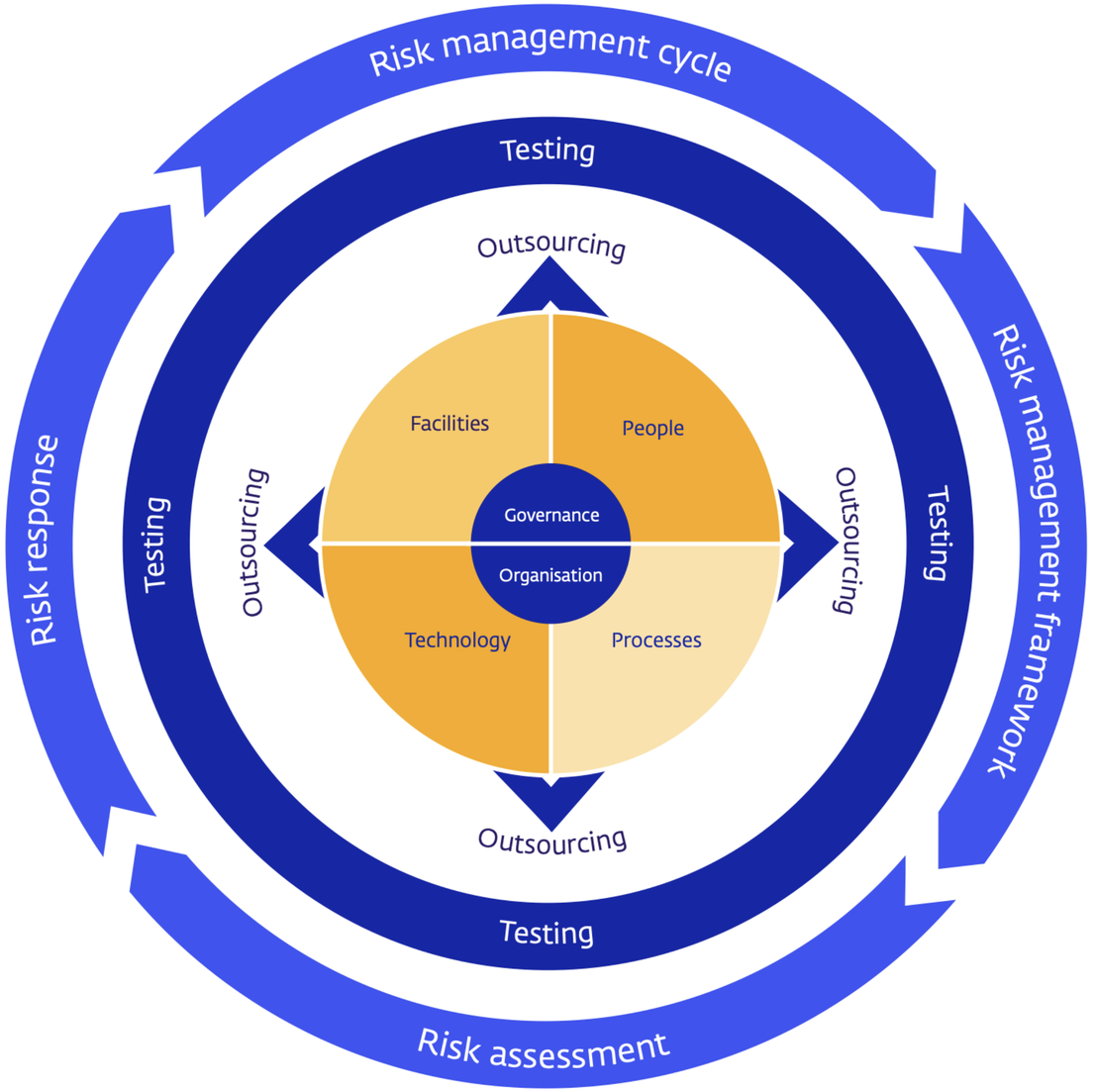
Risico gebaseerd
Een adequate beheersing van informatiebeveiliging betekent optimale effectiviteit van de controls/beheersmaatregelen die een instelling toepast. Een risico-gebaseerde aanpak per control/beheersmaatregel biedt de instelling de mogelijkheid om steeds verdergaand maatwerk ten aanzien van haar informatiebeveiliging toe te passen alsmede een proportionele benadering te hanteren.

Hoe?
- Analyse op het eigen interne en externe dreigingsbeeld/ risico's.
- Bepaling welke beheersmaatregelen op welke wijze het meest effectief zijn.
- Bepalen van verantwoordelijkheden en opstellen van procedures
- Identificatie van relevante dienstverleners bij de monitoring en het uitwisselen van dreigingsinformatie en heeft daarvoor afspraken met deze partijen. Hierbij heeft de inzet op kwaliteit van beheersmaatregelen de voorkeur boven kwantiteit van beheersmaatregelen.

Three lines model
Een passende scheiding en onafhankelijkheid van IT-risicobeheer functies, controlefuncties en interne auditfuncties, volgens de regels van het 'three lines model' is een belangrijk uitgangspunt. Bij elke control is het van belang de taakverdeling en verantwoordelijkheid tussen de three lines te definiëren: *Hoe zijn per control de taken en verantwoordelijkheden tussen de eerste de tweede en derde lijn verdeeld?*

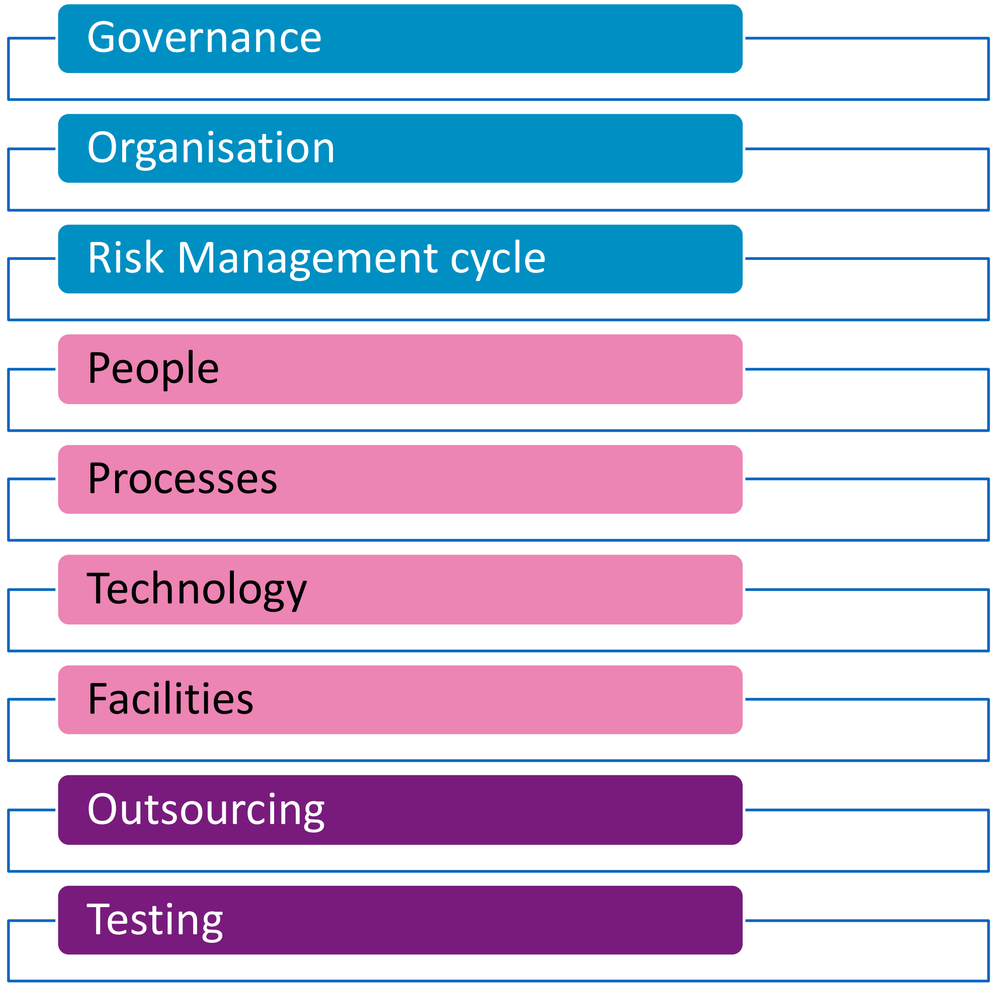
In Audit

De verschillende pijlers van Informatiebeveiliging



InAudit

De verschillende pijlers van Informatiebeveiliging



InAudit

De pijlers van Informatiebeveiliging samengevat (1/2):

De Basis:

Governance

- Information Security plan
- Information Security policies
- Security Architecture
- Data classification scheme
- Risks and opportunities of future trends and regulations
- Technology standards

Organisation

- Responsibility for risk, security and compliance and Information Security function
- Management of information security and tasks of the information Security function
- Data and system ownership
- Segregation of duties

Risk Management cycle

- IT Risk Management framework
- Risk assessment
- Maintenance and monitoring of a risk action plan

De pijlers van Informatiebeveiliging samengevat (2/2):

De Uitvoering:

People & knowledge

- Personnel recruitment and retention
- Personnel competencies and culture
- Dependence upon individuals
- Personnel clearance procedures
- Job change and termination
- Knowledge transfer to end users
- Knowledge transfer to operations and support staff
- Employee awareness

Processes (1)

- Change standards and procedures
- Impact assessment, prioritisation and authorisation
- Test environment
- Testing of changes
- Promotion to Production
- Business impact analysis and IT Continuity plans
- Testing of the IT Continuity plan
- Immutable backup storage
- Restoration

Processes (2)

- Storage and retention arrangements
- Disposal
- Security requirements for data management
- Configuration repository and baseline

Processes (3)

- Security incident policy and definition
- Incident escalation Data and system ownership
- Monitoring of internal control framework
- Evaluation of compliance with external requirements
- Independent assurance
- Identity Management
- User account management

Technology

- Infrastructure resource protection and availability
- Infrastructure maintenance
- Cryptography and Cryptographic key management
- Network Security
- Exchange of sensitive data
- Malicious software prevention, detection and correction
- Vulnerability Management
- Application Maintenance
- Protection of security technology

Facilities

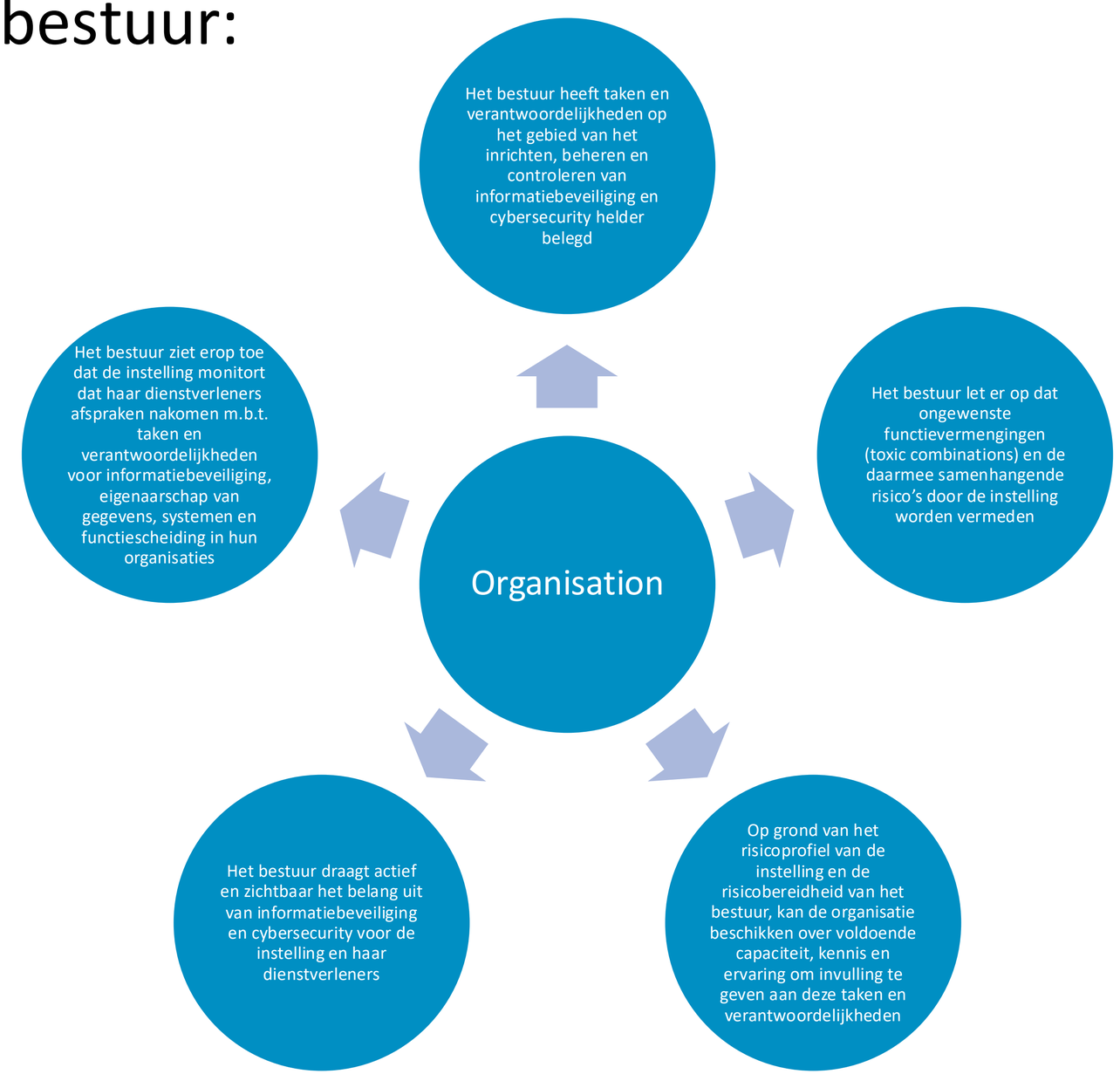
- Physical security measures
- Physical access

Outsourcing

- Third party and supplier services management
- Supplier risk management
- Internal control at third parties

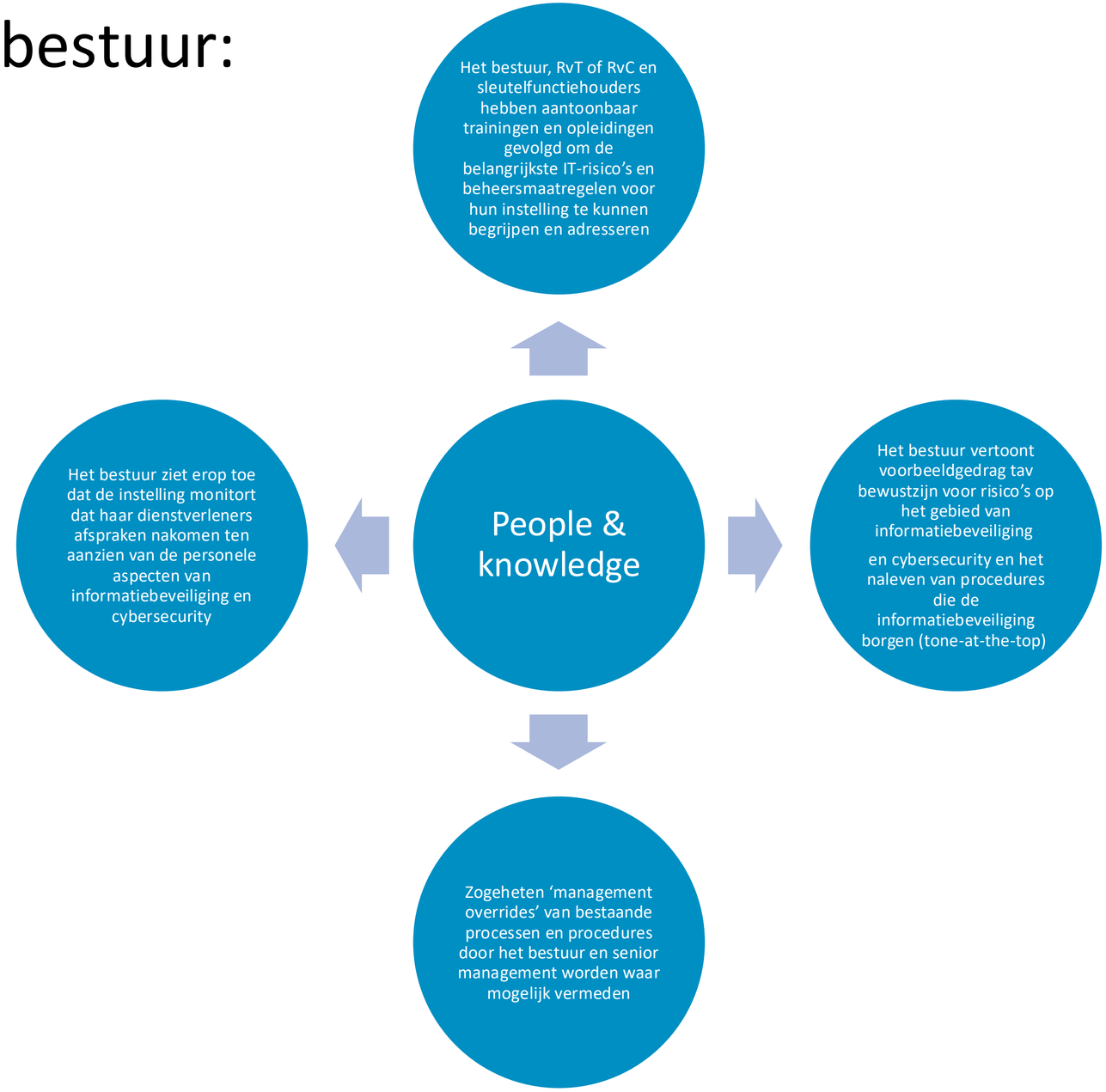
De rol van bestuur:

De rol van bestuur:



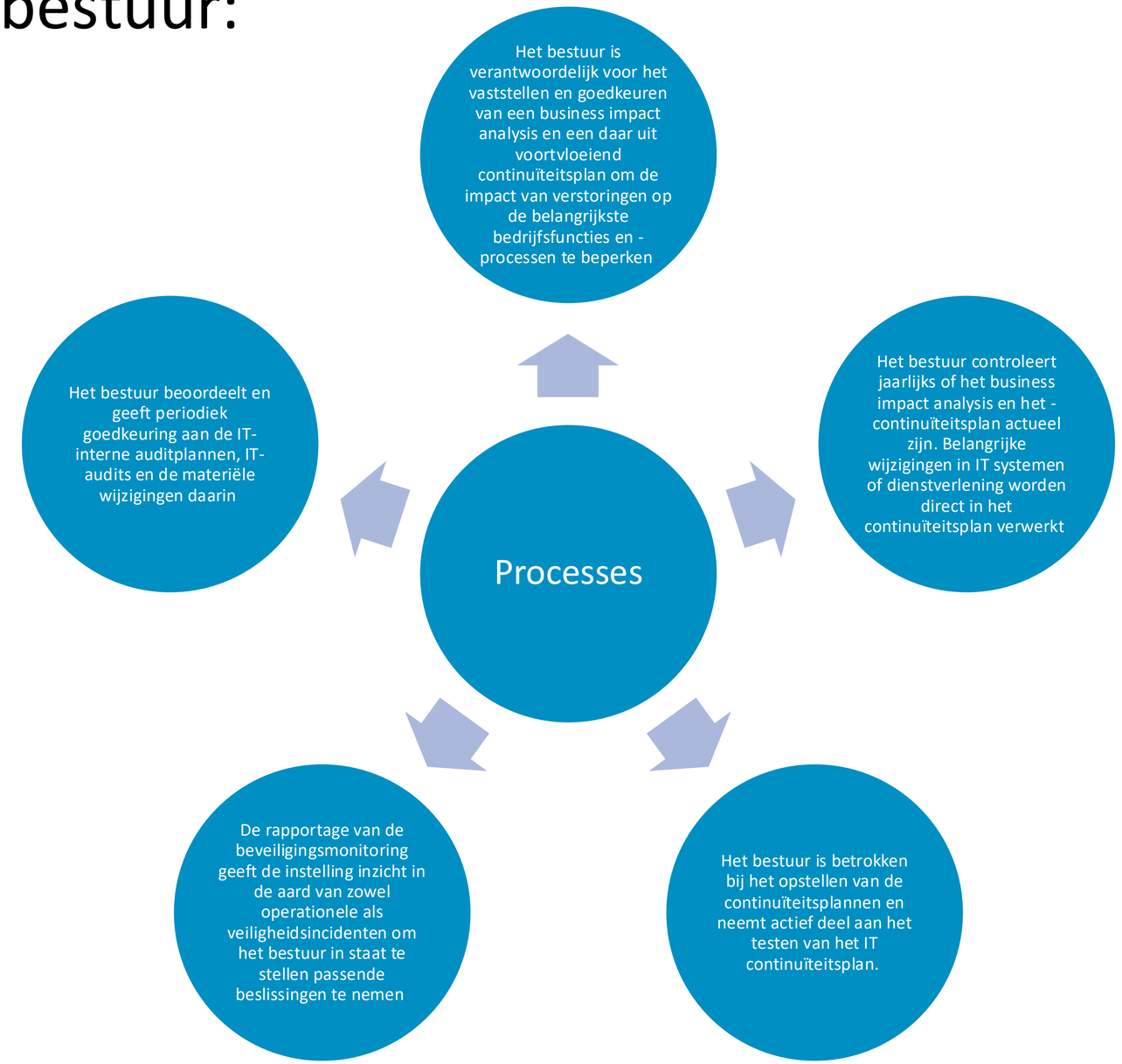
InAudit

De rol van bestuur:



InAudit

De rol van bestuur:



De rol van bestuur:

Technology

Het bestuur zorgt dat zij zich periodiek laat informeren over informatiebeveiligings-risico’s en over nieuwe technologische ontwikkelingen (die zowel kansen als risico’s met zich mee kunnen brengen op het gebied van informatiebeveiliging en cybersecurity)

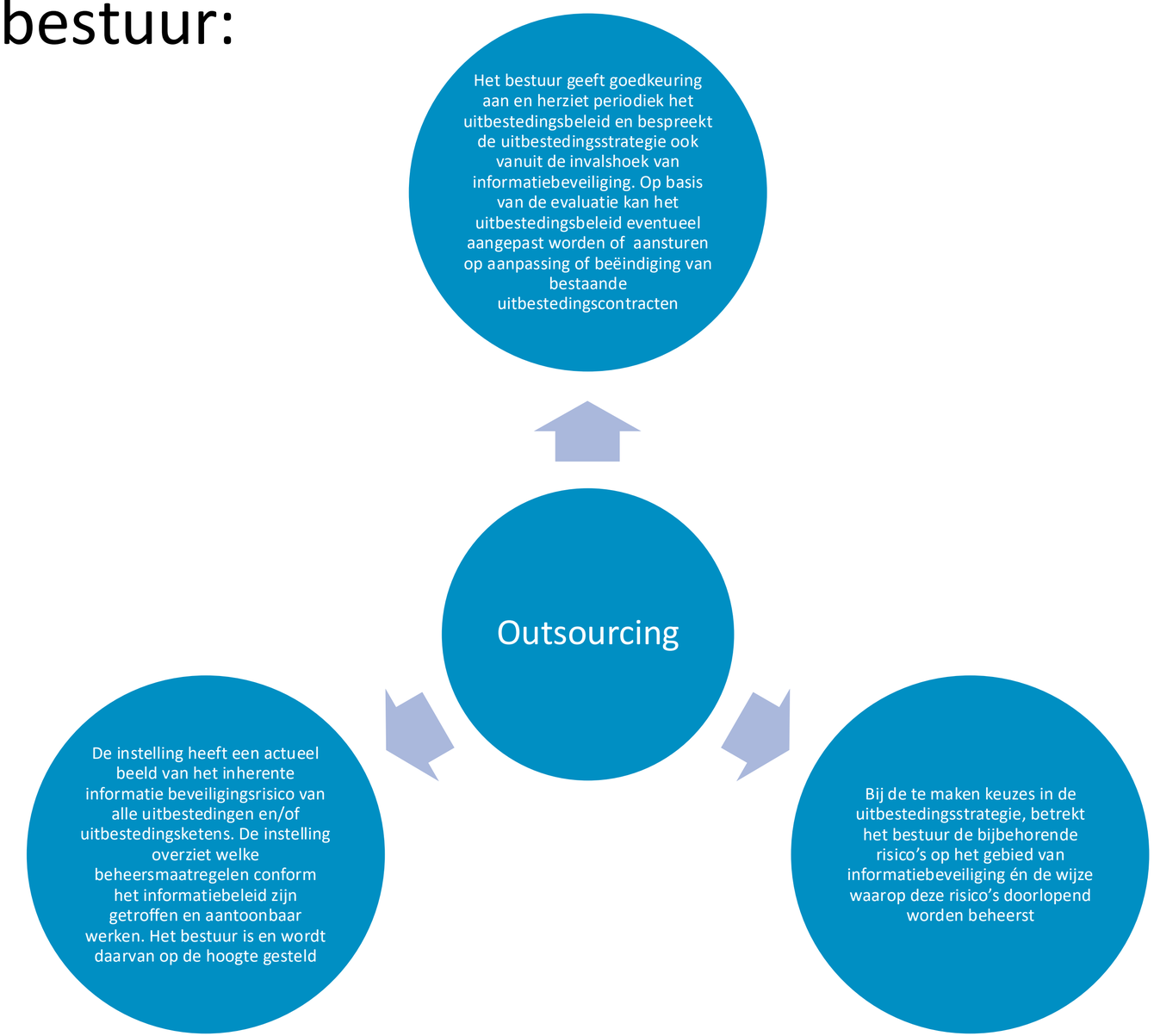
De informatiebeveiligings-risico’s kunt u als bestuurder meewegen binnen de Riskmanagement Cycle zie daartoe ook het betreffende element in het model

InAudit

De rol van bestuur:

In Audit

De rol van bestuur:



De rol van bestuur:

Conclusies

- Informatiebeveiliging is van wezenlijk belang
- Compliant te zijn met het vereiste beheersingsniveau en richtlijnen van de DNB is een uitdaging
- Kost veel capaciteit, maar maakt de organisatie robuuster tegen cybercriminaliteit

In Audit

Meer weten?

Wij kunnen u ondersteunen met onze diensten/ producten die wij in het kader van Informatiebeveiliging aanbieden.

1. Uitvoeren van een audit Informatiebeveiliging conform de standaarden van DNB
2. Tool om zelf een gap-analyse Informatiebeveiliging uit te kunnen voeren
3. Ondersteuning bij het implementeren van de geïdentificeerde gaps naar aanleiding van de door ons of door u uitgevoerde gap-analyse DORA

Laat het ons vooral weten als u meer informatie wilt ontvangen.

We zijn er om u te helpen!

In Audit

Contact

Offerte aanvragen?

- **InAudit BV**
  Spankerenseweg 16a
  6974 BC Leuvenheim (NL)
  T 055 – 303 2597
  W www.inaudit.nl
  E info@inaudit.nl

- **Ricardo Henriques**
  Directeur Audit Services
  InAudit Audit Services BV
  T 06 – 21 37 33 66
  E ricardo.henriques@inaudit.nl

Ricardo Henriques

Wessel Westerveld

Sam Althoff

Yorick Harmsen