Webinar

Information Security Management

Doel

Het delen van kennis, ervaring en best practices

Onderwerpen

- Wat houdt de ISO27001 in?
- Het stappenplan voor certificering
- Het verschil tussen ISO27001:2013 en ISO27001:2022
- Do's and dont's

INBISCO

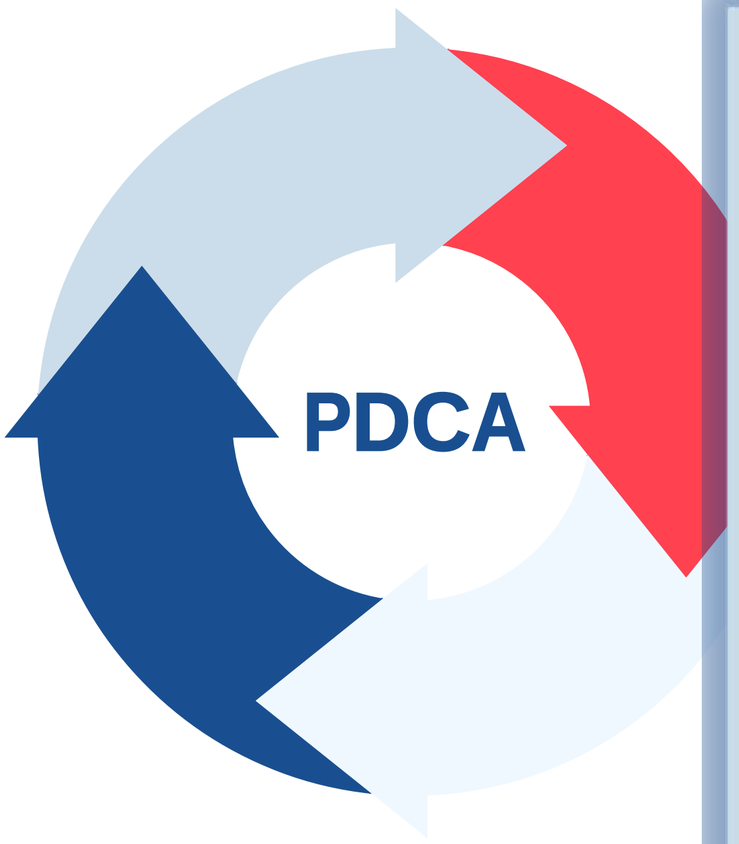
Uitleg van de norm

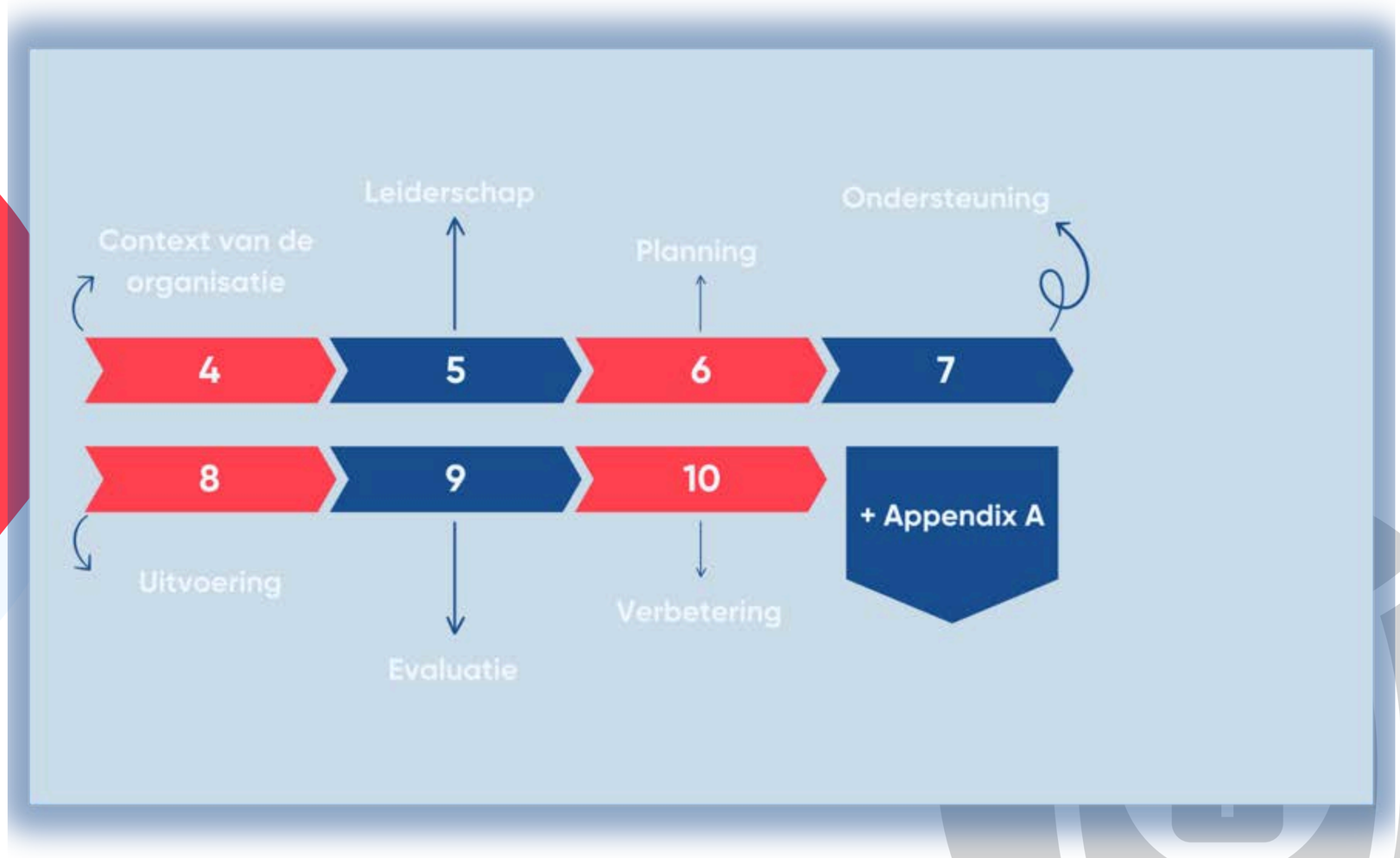
ISO27001:2022

- Waarom bestaat de ISO27001?
- Waaruit bestaat de ISO27001?
- Proces en risicomanagement als uitgangspunt van de ISO27001

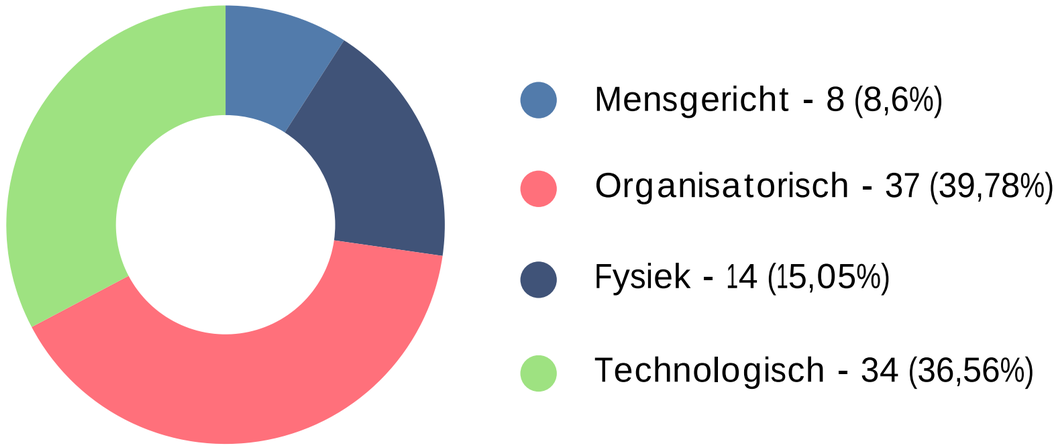
Het doel van de ISO 27001-certificering is het waarborgen van de informatiebeveiliging binnen een organisatie.

ISO27001:2022





ISO27002:2022 - Beheersmaatregelen



Annex A

- In de ISO27001 zijn 93 beheersmaatregelen gedefinieerd met richtlijnen hoe deze te implementeren.

Inbisco

INBISCO

Plan | Do | Check | Act

Vaststellen

- Implementatieplan en het doel bepalen
- Aanwijzen benodigde resources
- Context van de organisatie
- In kaart brengen van de processen van de organisatie

Implementeren en uitvoeren

- Uitvoeren risico-assessment
- Beoordeling te implementeren beheersmaatregelen
- Processen en bijbehorende beleidstukken uitwerken

Bewaken en beoordelen

- Maatregelen uitvoeren
- Audits
- Incidenten registratie
- Management of change
- Monitoren en meten
- Directiebeoordeling
- Jaarplan (verbeterplan) opstellen
- Awareness

Bijhouden en verbeteren

- Uitvoeren Jaarplan (verbeterplan)
- Communiceren verbeteracties
- Evalueren verbeteracties
- Awareness

INBISCO

Uitleg van de norm

ISO27001:2022

- Hoofdstuk 4 - Context van de organisatie
- Hoofdstuk 5 - Leiderschap
- Hoofdstuk 6 - Planning
- Hoofdstuk 7 - Ondersteuning
- Hoofdstuk 8 - Uitvoering
- Hoofdstuk 9 - Evaluatie
- Hoofdstuk 10 - Continu verbeteren

INBISCO

Uitleg van de norm

ISO27001:2022

Hoofdstuk 4 - Context van de organisatie

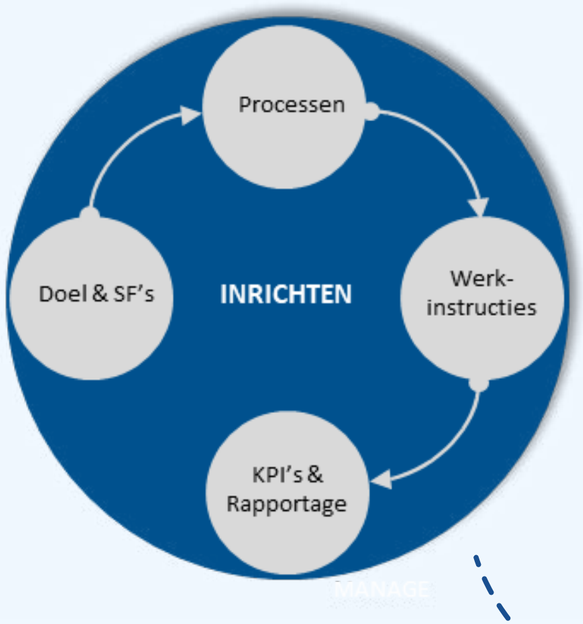
- Inzicht in de organisatie en haar context
- Inzicht in de behoeften en verwachtingen van belanghebbenden
- Het toepassingsgebied van het managementsysteem voor informatiebeveiliging
- Het managementsysteem van informatiebeveiliging

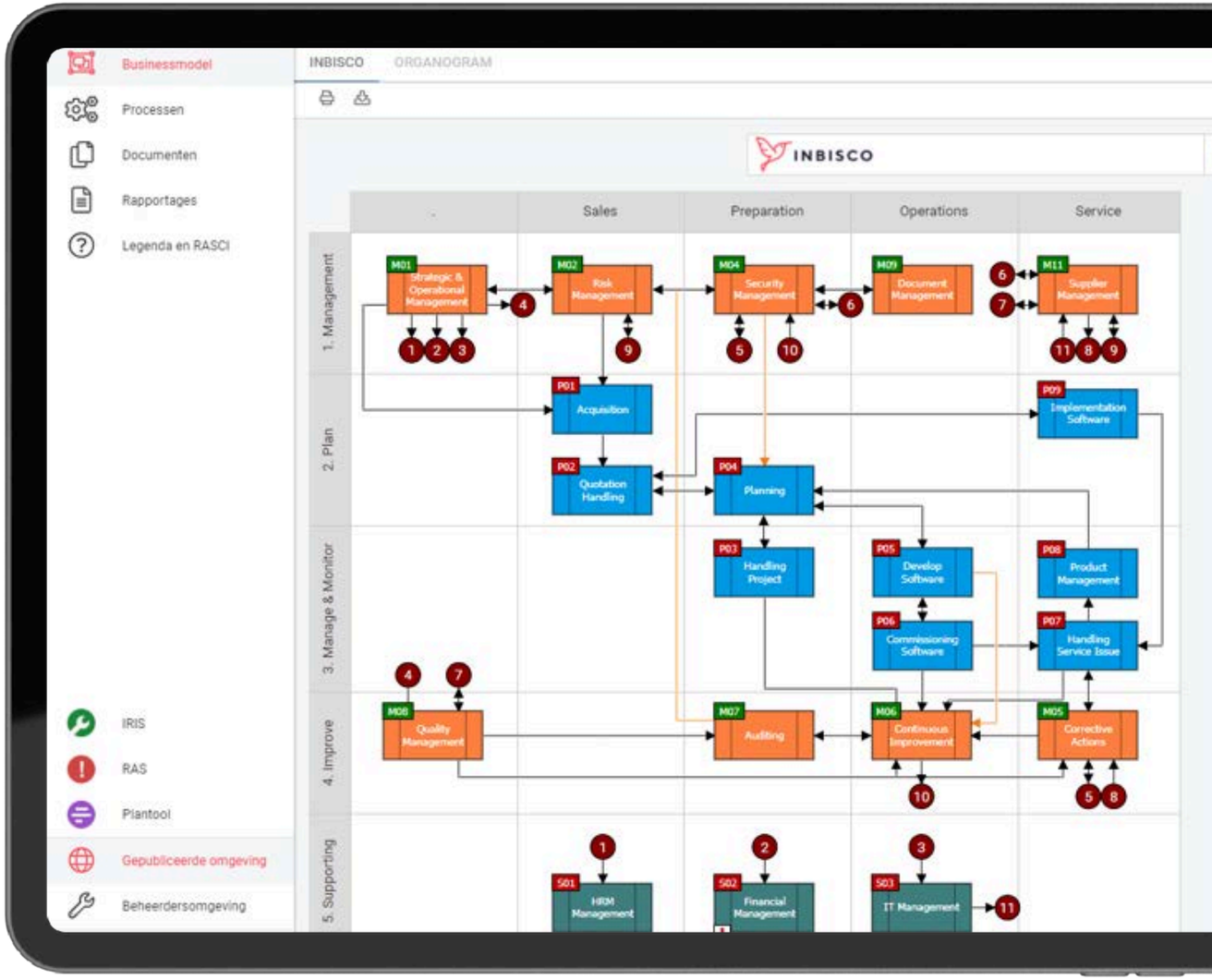
Project & Implementatie

Context van de organisatie

- Start met het projectplan
- Doelstellingen voor het ISMS opstellen
- Hoe definieer je de scope?

Processen


Processen
Doel & SF's
INRICHTEN
Werk-instructies
KPI's & Rapportage
MANAGE


Businessmodel
Processen
Documenten
Rapportages
Legenda en RASCI
IRIS
RAS
Plantool
Gepubliceerde omgeving
Beheerdersomgeving
INBISCO
ORGANOGRAM
INBISCO
Sales
Preparation
Operations
Service
1. Management
2. Plan
3. Manage & Monitor
4. Improve
5. Supporting
M01 Strategic & Operational Management
M02 Risk Management
M04 Security Management
M09 Document Management
M11 Supplier Management
P01 Acquisition
P09 Implementation Software
P02 Quotation Handling
P04 Planning
P03 Handling Project
P05 Develop Software
P08 Product Management
P06 Commissioning Software
P07 Handling Service Issue
M08 Quality Management
M07 Auditing
M06 Continuous Improvement
M05 Corrective Actions
S01 HRM Management
S02 Financial Management
S03 IT Management

Beheersing van de meest kritische aspecten

Context of the organization

Wat zijn de meest kritische aspecten?

- Processen
- Leveranciers en Partners
- Klanten
- Assets
- Software
- Hardware
- Medewerkers
- Stakeholders
- Ev.

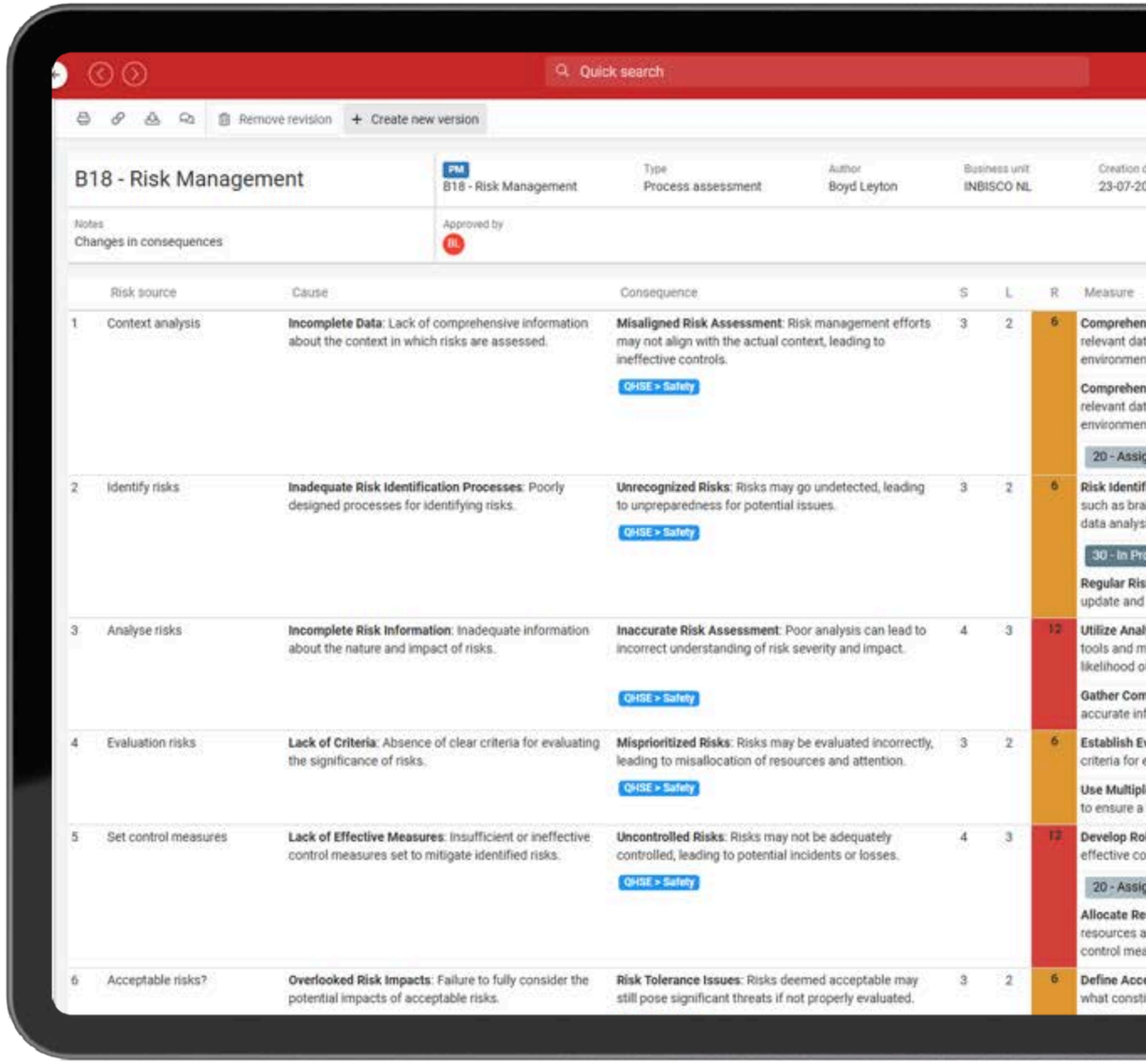
Beschikbaarheid, Integriteit en vertrouwelijkheid

INBISCO

Nulmeting

Risicomanagement

- Kritische aspecten van de organisatie (kroonjuwelen)
- Risico inventarisatie op basis van de context



INBISCO

Nulmeting

Risico inventarisatie

De verklaring van toepasselijkheid

Context en planning

Scope bepaling

- Organisatie
- Kritische risico's
- Beheersmaatregelen

INBISCO

Planning

Security plan

- Doelstellingen
- Meetbaar
- **Wat zal er worden gedaan?**
  Welke middelen zijn er nodig?
  Wie is verantwoordelijk?
  Wanneer voltooid?
  En hoe worden de resultaten geëvalueerd?

INBISCO

Uitleg van de norm

ISO27001:2022

- Hoofdstuk 4 - Context van de organisatie
- Hoofdstuk 5 - Leiderschap
- Hoofdstuk 6 - Planning
- Hoofdstuk 7 - Ondersteuning
- Hoofdstuk 8 - Uitvoering
- Hoofdstuk 9 - Evaluatie
- Hoofdstuk 10 - Continu verbeteren

Op basis van het plan

ISO27001:2022

Hoofdstuk 7 - Ondersteuning

- Middelen
- Competentie
- Bewustzijn
- Communicatie
- Beheersing van gedocumenteerde informatie

INBISCO

Uitleg van de norm

ISO27001:2022

- Hoofdstuk 4 - Context van de organisatie
- Hoofdstuk 5 - Leiderschap
- Hoofdstuk 6 - Planning
- Hoofdstuk 7 - Ondersteuning
- Hoofdstuk 8 - Uitvoering
- Hoofdstuk 9 - Evaluatie
- Hoofdstuk 10 - Continu verbeteren

Uitvoering

Verklaring van toepasselijkheid icm Risico assessment

- Kritische risico's
- Beheersmaatregelen uit de verklaring van toepasselijkheid
- Processen, procedures en beleid

INBISCO

Uitvoering

Risicobehandelplan

- Beheersmaatregelen toepassen
- Maatregelen om risico's te reduceren

Uitvoering en Evaluatie

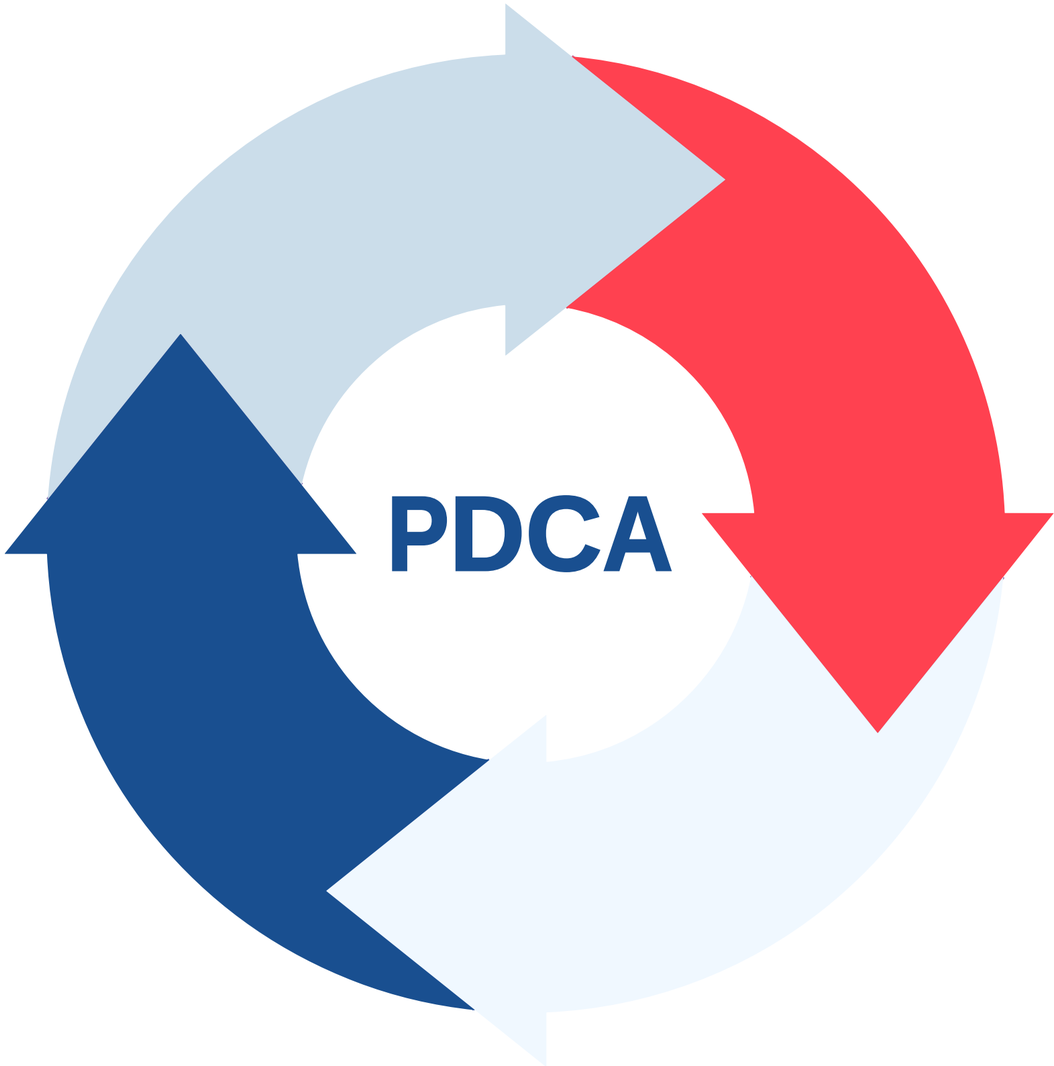
Meten is Weten

- Meten, Analyse & Rapportages
- Intern auditprogramma
- Awareness creëren
- Incident Management
- Management of change
- Directiebeoordeling

Verbetering

Nieuwe jaarcyclus

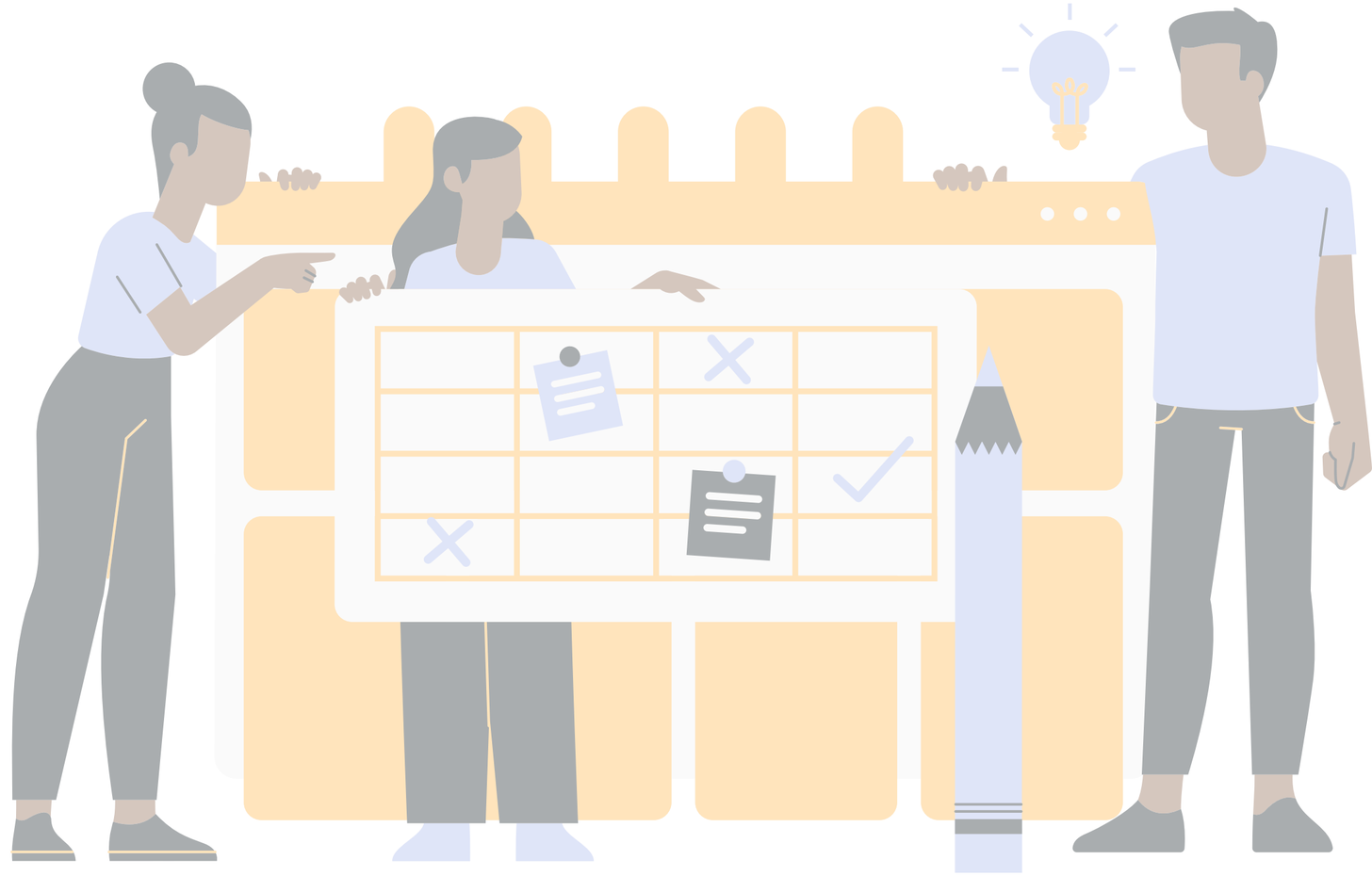
- Zaken uit de managementreview
- Zaken uit de interne audits
- Nieuw jaarplan (verbeterplan)



Evaluatie

Externe audit

- Voorbereiding externe audit
- De externe audit



INBISCO

Uitleg van de norm

ISO27001:2022

- Hoofdstuk 4 - Context van de organisatie
- Hoofdstuk 5 - Leiderschap
- Hoofdstuk 6 - Planning
- Hoofdstuk 7 - Ondersteuning
- Hoofdstuk 8 - Uitvoering
- Hoofdstuk 9 - Evaluatie
- Hoofdstuk 10 - Continu verbeteren

INBISCO

Verschillen

ISO27001:2013 en 2022

ISO 27001:2013:

- Beheersmaatregelen waren statisch en niet volledig afgestemd op moderne technologieën zoals cloud computing of AI.
- 114 maatregelen in 14 categorieën.

ISO 27001:2022:

- Nieuwe beheersmaatregelen toegevoegd om te focussen op actuele bedreigingen, zoals:
  - Threat Intelligence
  - Cloud Security
  - Data Masking
  - Monitoring activiteiten
- Vereenvoudiging en hergroepering van bestaande maatregelen:
  - Veel maatregelen zijn samengevoegd om overlap te verminderen.
- Aantallen: Van 114 naar 93 maatregelen, gegroepeerd in 4 nieuwe categorieën.

Verschillen

ISO27001:2013 en 2022

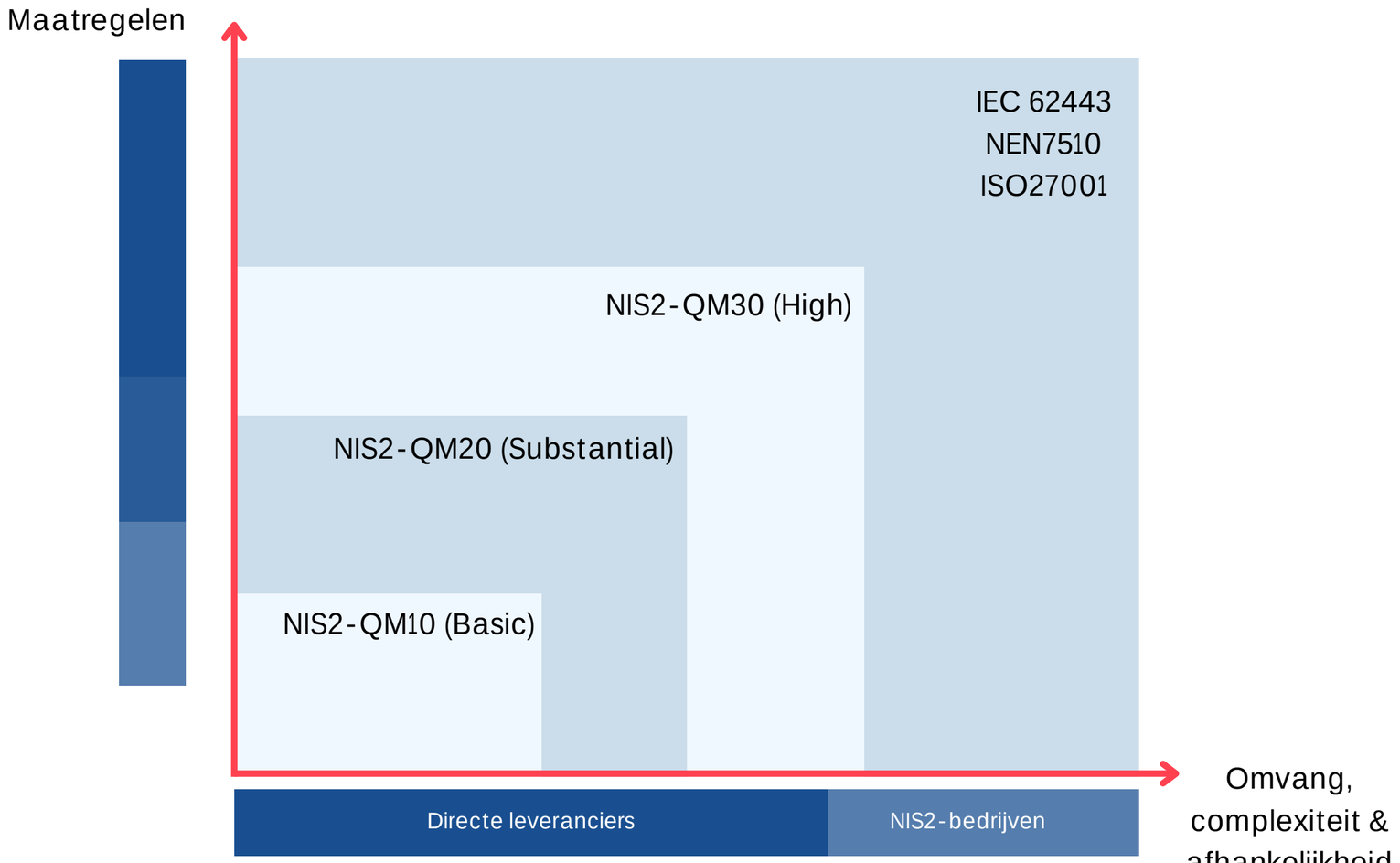
De 2022-versie richt zich meer op hedendaagse ontwikkelingen in beveiliging:

- Cybersecurity:
  - Meer aandacht voor moderne dreigingen, zoals ransomware en supply chain-risico's.
-
- Technologische ontwikkelingen:
  - Specifieke maatregelen voor cloud-omgevingen
  - Bring Your Own Device (BYOD)
  - Hybride werken

- Praktische toepassing:
  - Meer nadruk op het toepassen van risico-gebaseerde besluitvorming.

Verschillen

ISO27001 en NIS2



Verschillen

ISO27001 en NIS2

- ISO 27001 is een vrijwillige certificering gericht op het verbeteren van interne processen rondom informatiebeveiliging. Het is geschikt voor een brede groep organisaties.

- NIS2 is een verplichte richtlijn voor specifieke sectoren binnen de EU, gericht op het verbeteren van de cyberveiligheid en veerkracht van kritieke infrastructuur.

INBISCO

ISO27001 en NIS2

NIS 2 is

- ISO 27001
- + Een meldplicht analoog aan die van privacy
- + Controle over de keten (zit ook in ISO27001:2022)
- + Registratie van de entiteit (net zoals je een FG aan moet melden bij de AP)
- + Verplichte cybersecurity opleiding voor directie