Dit is een presenteerbaar werkdocument voor de expertgroep "Actualiseren NORA-3" Het bevat views van de huidige situatie (Ist) en ideeën waar in opdracht naar toe kan worden gewerkt (Soll)

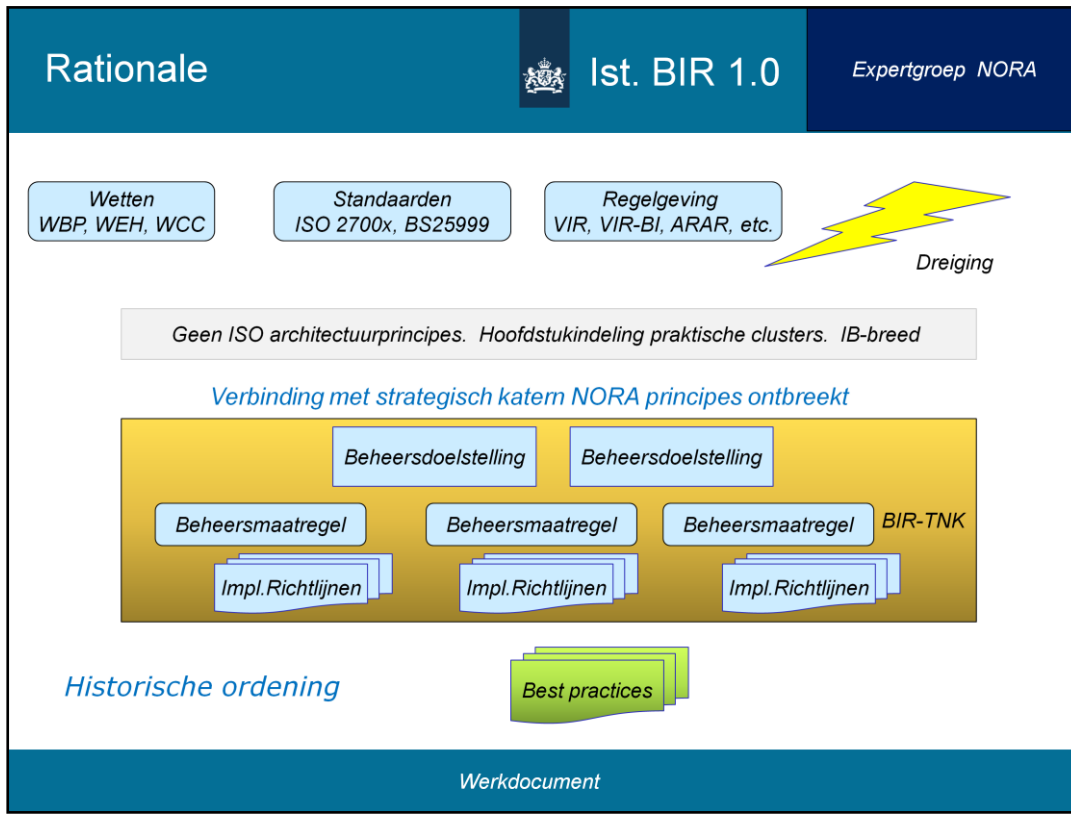
Presentatie

1. Doelen van katern beveiliging
2. Rationale en startpunt, BIR, rubricering, NORA 3
3. Werkingsgebied
4. Deliverables; NORA-Expertgroep/overig

Doelen

Harmoniseren IB-kaders overheid.

1. **Normatieve uitspraken** voor Rijk, decentrale overheden en semi-overheidsorganisaties of IB-maatregelen op orde zijn
2. **Richtinggeven en toetsbaar** maken van beveiliging, voor ontwerp en exploitatie van Informatievoorzieningen.
3. **Kennisdeling**



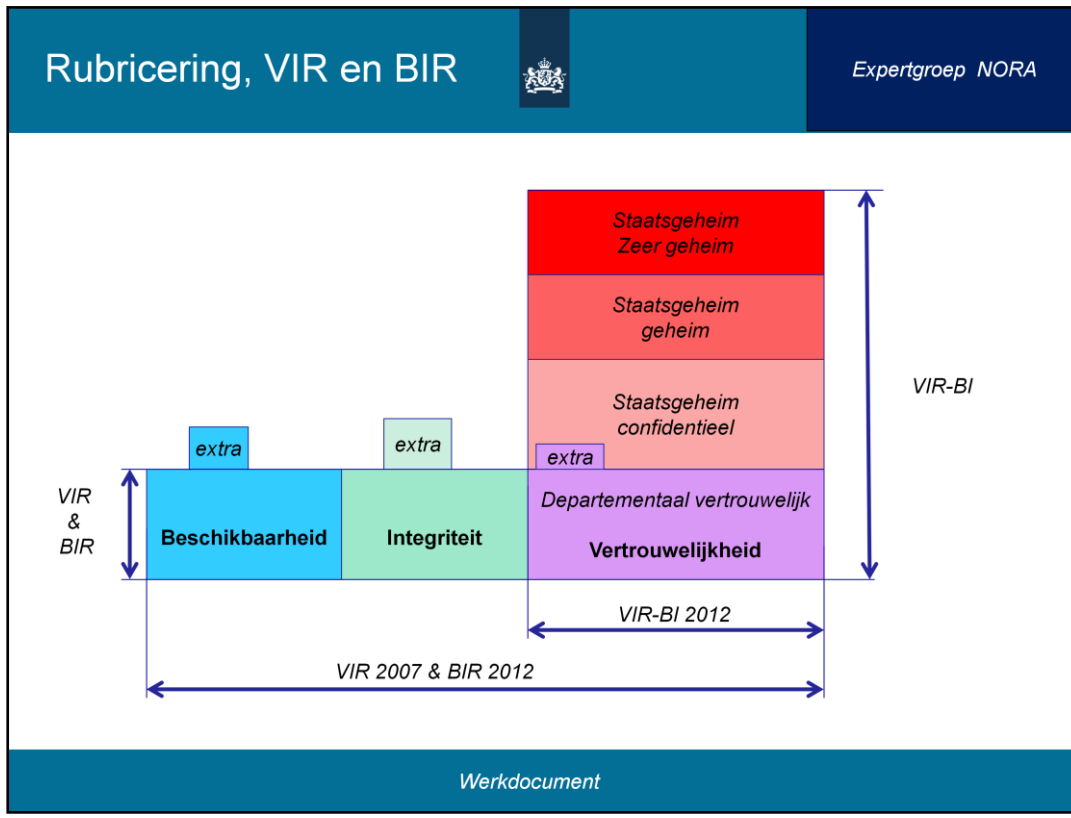
Het BIR bestaat uit de ISO norm + rijksspecifieke implementatierichtlijnen, die op Dep.V niveau zijn gespecificeerd. Deze rijksspecifieke implementatierichtlijnen zijn in de BIR met (R) gemarkeerd.

Bij toepassing van de ISO/BIR als ontwerpkader moet een afleiding gemaakt worden van wet-en regelgeving naar onderwerp- gebaseerde beveiligingsgebieden en beheersdoelstellingen. Per individueel beveiligingsdoel is dit haalbaar, maar niet voor informatieketens die op basis van bedrijfsfuncties (en beveiligingsfuncties) ontworpen en gebouwd moeten worden.

Eigenschappen van de ISO-27002 zijn dat dit kader geen beveiligingsfuncties onderkend. Het maakt tevens geen onderscheid tussen normen voor beleid en uitvoering, tussen product- en procesnormen en tussen normen voor klant en leverancier.

De praktijk leert, dat de ISO (en de daaraan gekoppelde BIR) om deze redenen niet zinvol kan worden gebruikt in het ontwerpproces voor informatievoorzieningen. Organisaties die informatiesystemen implementeren in hun bedrijfsprocessen, maken daarom een vertaling vanuit de ISO naar hun eigen ontwerpprincipes in de vorm van een specifieke set van eisen.

In de NORA 3 van 2010 is deze vertaling gemaakt in het dossier “Normen IT-voorzieningen” en wel zodanig, dat deze opzet universeel toepasbaar is voor elke willekeurige (ook niet-overheid) organisatie.



Op strategisch niveau bestaat het Voorschrift Informatiebeveiliging Rijksdienst (VIR), dat het laatst in 2007 is geactualiseerd. Het VIR is gericht op Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie.

Voor staatsgeheime informatie bestaat het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI). Dit document is in 2012 geactualiseerd en richt zich uitsluitend op Vertrouwelijkheid.

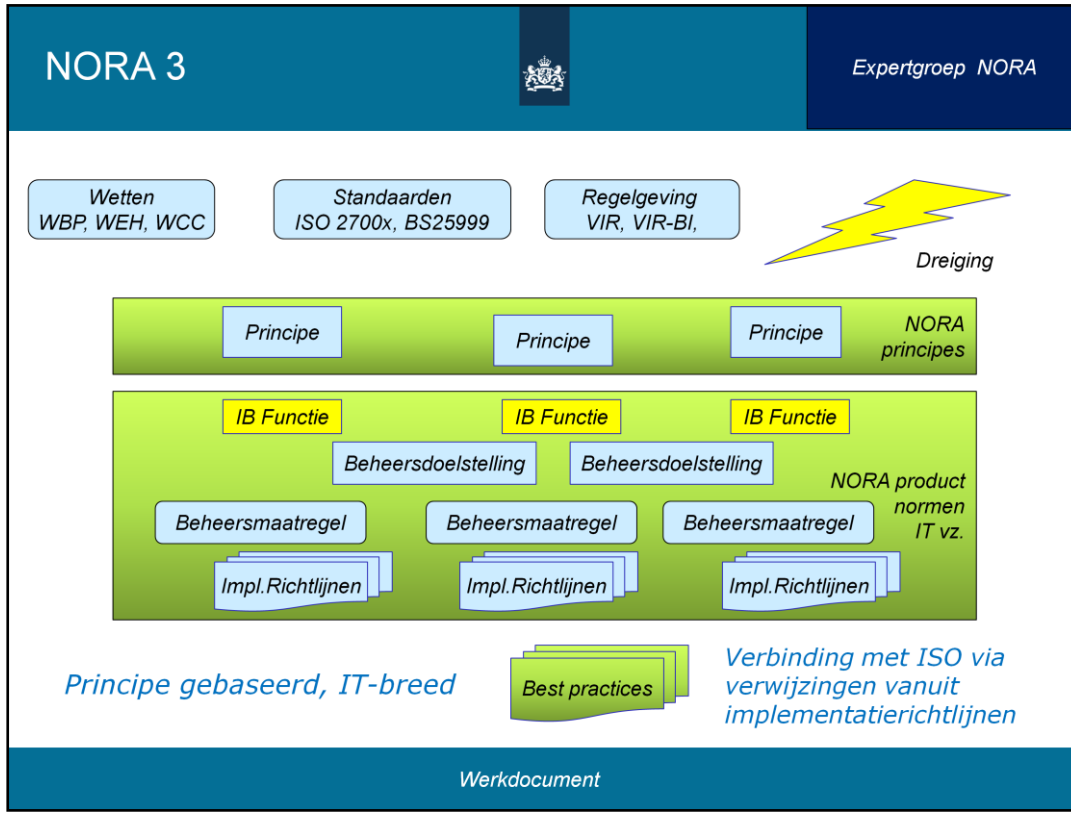
Horizontaal het is verband tussen de VIR-kaders en het BIR weergegeven en verticaal het rubriceringsniveau dat de kaders onderscheiden.

Het VIR-2007 omvat de strategische uitgangpunten en randvoorwaarden die het ministerie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;

Het VIR BI -2012 onderscheidt op het niveau van vertrouwelijkheid vier rubriceringen.

Het BIR-2012 definieert het hoge basisniveau voor de Rijksdienst op het niveau van Departementaal Vertrouwelijk (Dep.V). Dit vertrouwelijkheidsniveau komt overeen met de classificering WBPII+ (Wet Bescherming Persoonsgegevens Risicoklasse II verhoogd risico.

Bovenop dit basisniveau; ook wel het ‘platte dak’ van het BIR genoemd, kunnen als de dienstverlening dit vereist extra maatregelen worden toegevoegd.

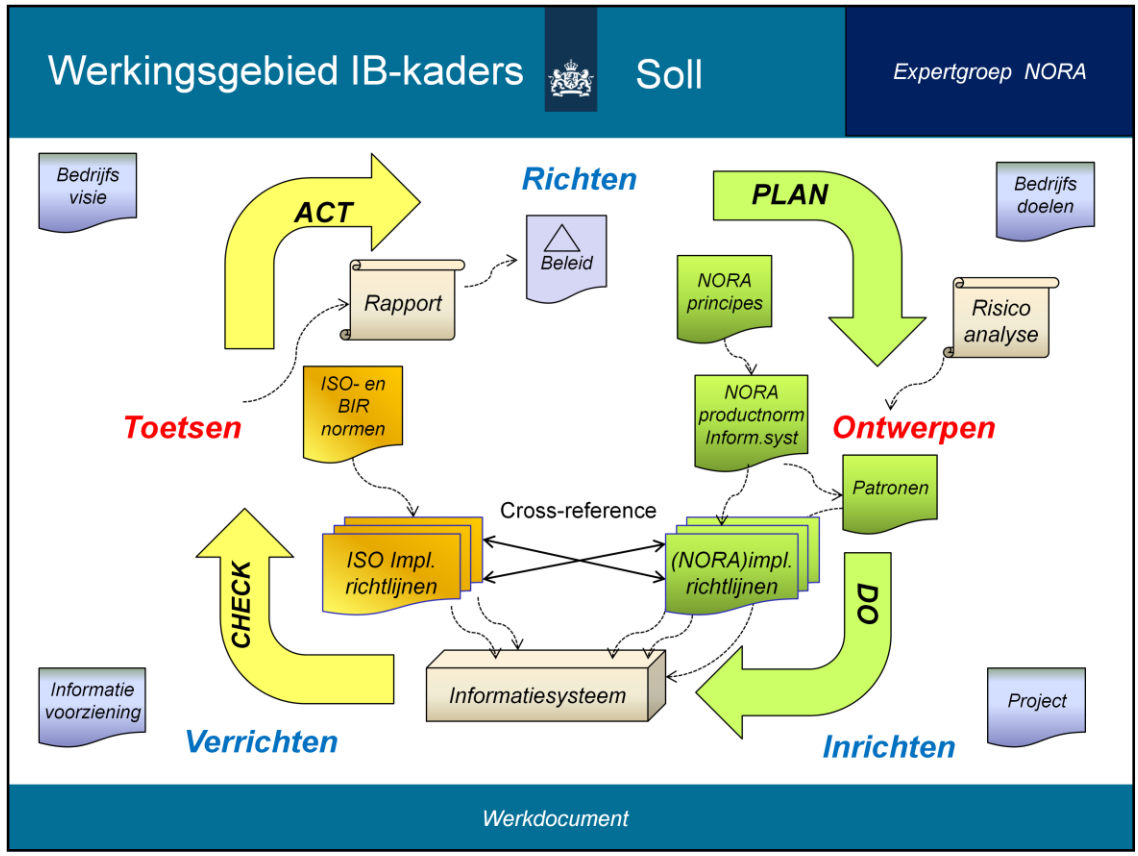


Deze plaat schetst de NORA-3 opzet van 2010 (voor beveiliging van IT-voorzieningen)

Van boven naar beneden zien we de afleiding vanuit de wet- en regelgeving en dreigingen naar bedrijfsprincipes, beveiligingsfuncties,beheersmaatregelen en tenslotte naar implementatierichtlijnen.

In ontwerp- en exploitatiefase kan de digitale veiligheid van *informatievoorzieningen* getoetst worden, gebruik makend van één kader..

De verbinding met de ISO-standaard is geregeld via cross-references tussen NORA implementatierichtlijnen en overeenkomstige ISO implementatierichtlijnen.



De toepassing en samenhang van ontwerp- en toetsingskaders voor beveiliging van bedrijfsprocessen van de overheid is weergegeven in bovenstaande figuur.

Inrichten. Vanuit bedrijfsdoelen en inrichtingsprincipes worden informatiesystemen ontworpen. Daarbij worden door projecten NORA beveiligingsprincipes gehanteerd, die via IB-functies worden geconcretiseerd in patronen en NORA implementatierichtljnen voor het informatiesysteem. Daarvoor geldt het regiem"pas toe of leg uit". De normen uit het NORA katern fungeert daarbij als *ontwerpkader* voor informatiesystemen van de overheid. Op basis daarvan wordt het systeem gebouwd en beveiligingsmechanismen geconfigureerd. Best practices zoals patronen worden toegepast

Toetsen. De werking van beveiligingsmechanismen in de informatievoorziening wordt in exploitatie (periodiek) getoetst op basis van de voor het informatiesysteem relevante beheersdoelstellingen en daarvan afgeleide implementatierichtlijnen. Daarvoor geldt het regiem "pas toe of leg uit". De ISO + verbrede BIR fungeert daarbij het *toetsingskader* voor de overheid. ISO staat daarbij centraal, het BIR in de nieuwe addendum-vorm zorgt voor *toepasselijkheid* binnen de overheid.

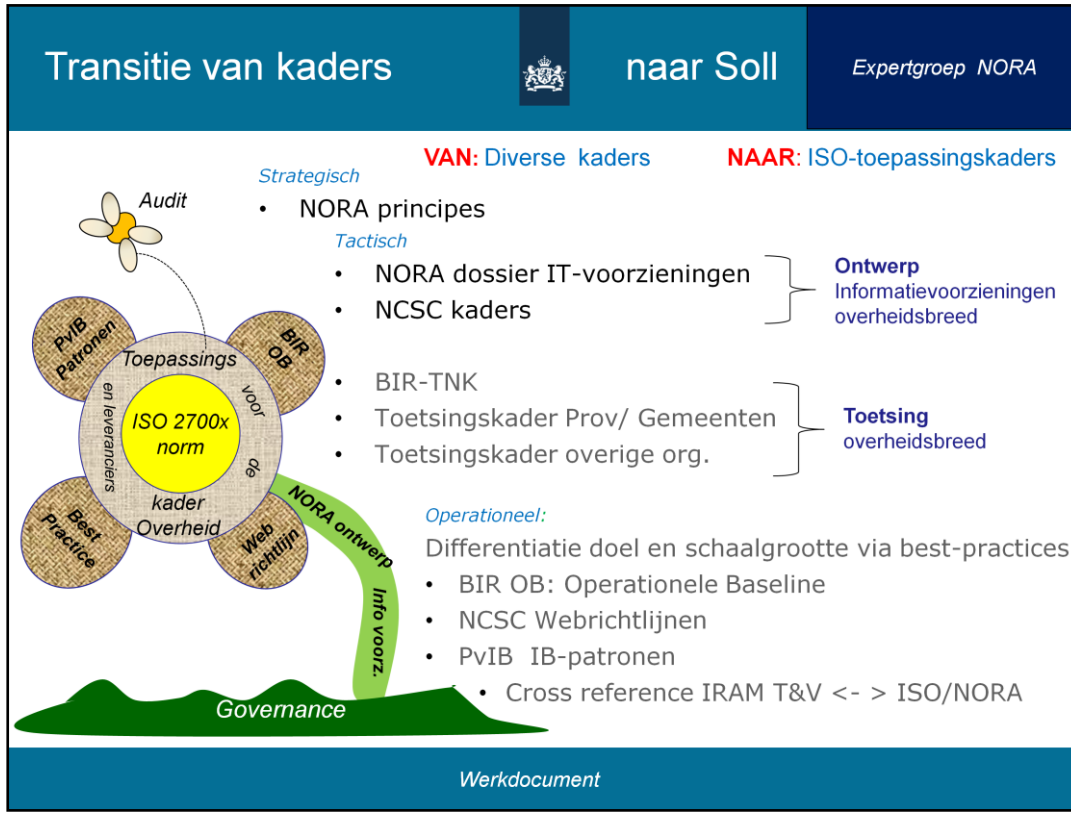
Kwetsbaarheden en afwijkingen van de norm in de informatievoorziening leiden tot maatregelen of bijstelling van het beleid en beveiligingsdoelen, die meegenomen worden in verbeteracties voor organisatie, proces of techniek.

De verbinding tussen ISO /BIR – en NORA normen is de cross-reference van implementatierichtlijnen.

Op deze manier benutten we het beste van twee werelden: NORA princpes en productnormen voor inrichten van informatiesystemen onder architectuur en de ISO als internationale norm voor toetsing, inclusief mogelijkheden voor certificering en toepassen van standaard tools en BI(R) voor toepasbaarheid.

Tevens ontkoppelen we hiermee de voortbrengingsfase van een informatiesysteem en het gebruik in exploitatie daarvan, zodat we "security by design" eisen kunnen stellen aan producten van leveranciers.

Samengevat staat de ISO-norm centraal. Overheidsbreed normaliseert NORA naar **toepassingskaders**



Dit is de SOLL- situatie met de ISO norm centraal afgebeeld als toetsingskader, waarbij de NORA productnorm de inrichting van de informatievoorziening normeert.

- Het hart van de 'bloem' vormt de ISO norm, die bestaat uit ISO 27001 en ISO 27002
- Het lichtbruine deel zijn de overheidsspecifieke toetsingsnormen bovenop de ISO. Streven is één addendum.
- De steel is het NORA kader voor de ontwerp en inrichting van informatievoorzieningen.
- De bruine bladeren vormen het stelsel van best-practices, open source en overige in de markt, waarin de nodige differentiatie van beveiligingsdoelen van grote en kleine organisaties wordt uitgewerkt.
- Nieuwe versies van de ISO kunnen in deze opzet zonder veel moeite ingevoerd worden. In 2013 en 2014 worden nieuwe ISO-27002 versies verwacht. Alleen addenda en cross-references behoeven te worden geactualiseerd.
- Governance is de basis. Het governance model van de BIR is vertrekpunt voor het overheids-governancemodel.

Deliverables katern IB

Expertgroep NORA

1. Samenhang van normenkaders Beveiliging voor de overheid
2. Actualisering NORA dossier "Normen voor IT-voorzieningen" tot ISO-toepassingskader voor ontwerp: "Normen voor informatievoorzieningen", met met integratie van relevante normen uit kaders als NCSC en BIR.
3. Opstellen cross-reference ISO <-> NORA Normen voor Informatievoorzieningen
4. Nieuwe content in lijn brengen met NORA principes, Wiki etc.
5. Kennisdeling

Randvoorwaarden:

a. Besluit: Onderscheid ontwerp- en toetsingskaders

b. Besluit: Verbreding BIR tot ISO-toepassingskader voor toetsing overheid

c. Opschaling van BIR-governance model ->overheidsbreed

Overig, (niet in katern)

- Verbreding BIR tot ISO-toepassingskader voor toetsing overheid
- Integratie bestaande overige kaders zoals NCSC voor toetsing
- Best practices voor overheidsorganisaties

Werkdocument

.