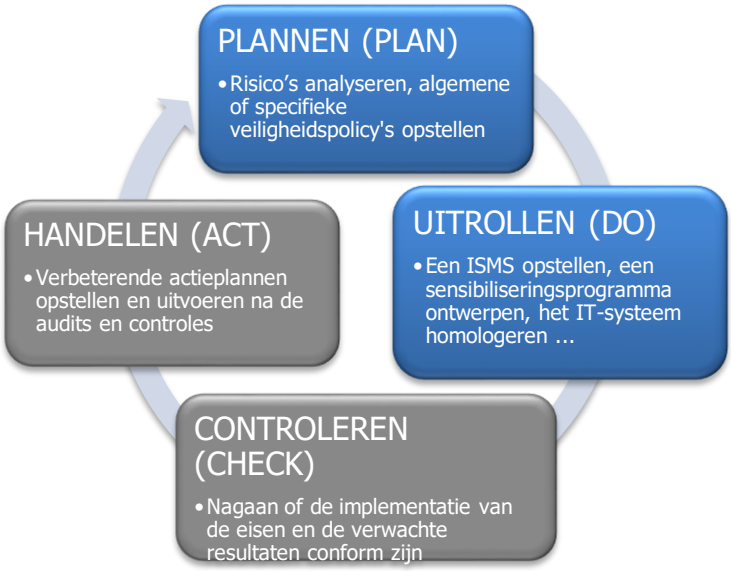
Beleid voor het Information Security Management System

1 Doelstellingen

De algemene aanpak van het Information Security Management System (ISMS) waarborgt de duurzaamheid van de beveiliging van alle processen uit de perimeter via een PDCA-aanpak *(Plan, Do, Check, Act).* Bij deze aanpak wordt de beveiliging van het IT-systeem op alle niveaus geïndustrialiseerd en worden alle stakeholders betrokken.



Deze aanpak houdt rekening met de volgende vereisten:

- wettelijke vereisten in België en Griekenland,
- regelgevende vereisten,
- vereisten van onze klanten.

2 Toepassingsgebied

Het Information Security Management System omvat:

- Operationeel beheer van IT-infrastructuur, softwareontwikkeling, -integratie en -onderhoud, consultancy en 'Managed Staffing.
- Het IT-systeem van NRB waarmee de betrokken activiteiten uitgevoerd kunnen worden.
- NRB's datacenters in Herstal.

2.1 Voorstelling van NRB

NRB werd opgericht in 1987 en is vandaag een van de belangrijkste spelers in de informaticasector in België.

NRB biedt een compleet scala aan globale ICT-diensten en -oplossingen aan, om zijn klanten gedurende de gehele levenscyclus van hun IT-projecten te ondersteunen. NRB zet een private en hybride cloudinfrastructuur op en beheert deze. Daarnaast ontwerpt NRB de architectuur en ontwikkelt, beheert en onderhoudt het applicaties (mainframe of open systems). Die zijn op maat gemaakt of gepersonaliseerd en worden vanuit ERP-softwarepakketten (Enterprise Resource Planning) [SAP], ECM (Entreprise Content Management) of BI (Business Intelligence) geconfigureerd. NRB biedt

ook Consulting- en Managed Staffing-diensten aan. Met meer dan 35 jaar ervaring op de teller levert NRB IT-oplossingen en -diensten aan de financiële sector, de openbare en sociale sector op het regionale en het federale niveau, aan de gezondheidssector, openbare nutsbedrijven, de industrie en de biotechsector.

2.2 Interne organisatiestructuur

NRB is georganiseerd rond drie componenten ('Sales', 'Delivery' en 'Central Services') om zijn dienstenaanbod bij zijn klanten te waarborgen.

De missie van de salesunits:

- getrouwheid creëren bij de huidige klanten en winstgevende bedrijfsstromen ontwikkelen;
- nieuwe klanten aantrekken met winstgevende contracten en de groei van NRB boosten door oplossingen en diensten aan te bieden die voornamelijk worden geleverd door de Service Lines van de Delivery van NRB, vestigingen en filialen.

De salesunits zijn elk verantwoordelijk voor de specifieke sectoren van de markt verdeeld per activiteitentak. Drie transversale units leveren de salesunits ondersteunende diensten m.b.t. Bid Management en Marketing.

Client Delivery wordt gestructureerd in “Competence Centers” waar medewerkers worden gegroepeerd op basis van hun vakgebied en expertise. Afhankelijk van de behoeften van klanten en de zakelijke vaardigheden die projecten (producten/diensten) vereisen, zullen leden worden gemobiliseerd in multidisciplinaire teams binnen “Delivery Units”.

De salesunits en de Delivery-afdelingen worden ondersteund door de Central Functions:

- Finance, Acquisitions & Subsidiaries
- HR & Internal Communication
- Quality & Risk Management
- Secretary General
- Chief Security Officer & Partner Management

2.3 Toepassingsgebied

2.3.1 Geografische perimeter

De onderneming heeft zijn hoofdkantoor in Herstal en is actief in België en Griekenland.

Het datacenter van NRB bevindt zich op de site van de zetel van de onderneming in Herstal. NRB heeft ook een datacenter in Villers-le-Bouillet (op 30 km van de site in Herstal), dat eigendom is van BelgiumDC, een joint venture waarin NRB een belang van 50% heeft.

De activiteiten van NRB nv worden uitgevoerd vanuit verschillende bedrijfssites:

- Parc Industriel des Hauts-Sarts, 2e Avenue 65, 4040 Herstal, BELGIË
- Interleuvenlaan 10, 3001 Heverlee, België
- Ethnikis Antistasis Street 67, 15231 Chalandri, Griekenland

De geografische perimeter van het ISMS omvat het datacenter van NRB en de bedrijfssites.

De filialen zijn niet inbegrepen in de perimeter van het ISMS. Enkel NRB nv maakt deel uit van de perimeter van het ISMS.

2.3.2 Menselijke perimeter

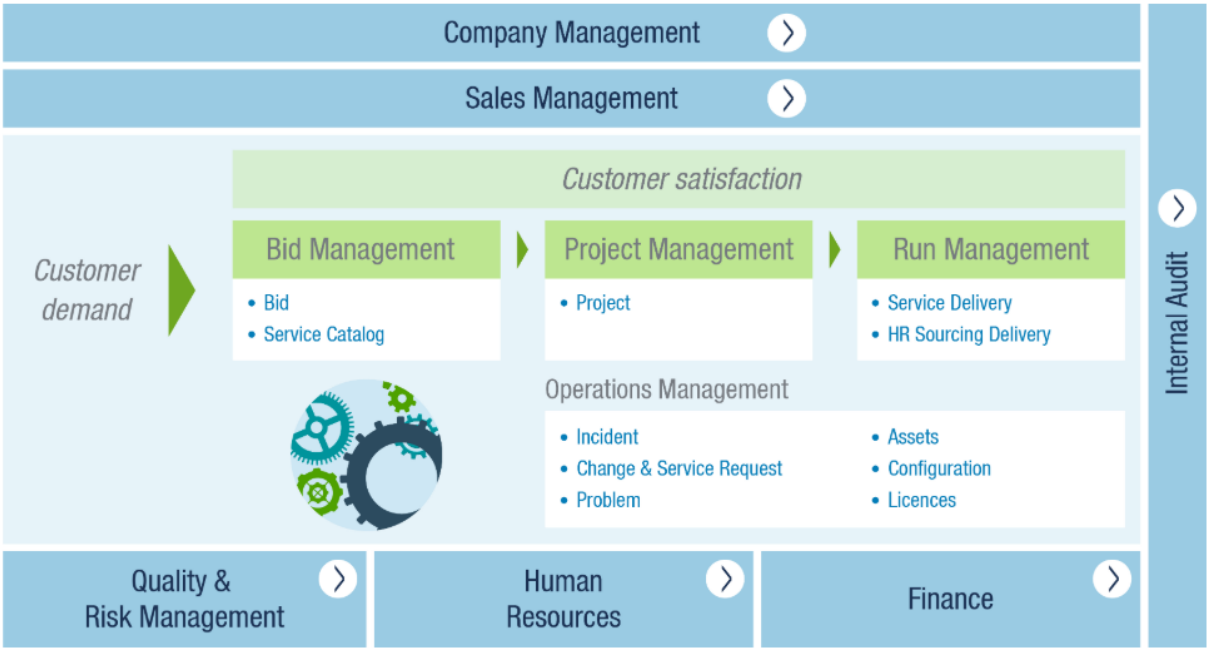
De menselijke perimeter van het ISMS omvat alle NRB-teams die verantwoordelijk zijn voor het beheer van het datacenter en businessdiensten gepresteerd door NRB.

Het personeel uit de certificeringsperimeter vervult functies waarvan de taken in de perimeter van het ISMS zitten.

2.3.3 Perimeter en beperkingen van het ISMS

2.3.3.1 Perimeter van het ISMS

NRB is georganiseerd rond processen. Het schema hieronder licht de perimeter van het ISMS toe, met de verschillende processen:



De perimeter omvat alle diensten die NRB aan zijn klanten levert, via bovengenoemde processen en op basis van infrastructuurapparatuur die eigendom is van NRB of wordt gehuurd, namelijk:

- de server- en opslagracks,
- de IT-servers,
- de hostinginstallaties,
- de telecommunicatieverbindingen,
- de netwerkinfrastructuren waarvan NRB eigenaar is.

NRB is klant van zijn eigen 'datacenteractiviteit', die de gegevens van de volledige onderneming host. Deze perimeter omvat:

- het interne IT-systeem van NRB (informatie en alle middelen waarmee hun verwerking mogelijk is, ongeacht de aard van de verwerking);
- het administratie-informatiesysteem van het 'datacenter';
- de applicaties waarvan NRB eigenaar is (de eigenaar van de gegevens gebruikt de gedeelde interne applicaties van NRB);
- de interne applicaties van NRB;
- de gegevens waarvan NRB eigenaar is.

2.3.3.2 De grenzen van het ISMS

Hoewel NRB bepaalde beveiligingsaspecten van zijn klanten uitwerkt, zijn de volgende aspecten niet in de perimeter van het ISMS 27001 en dus niet in de perimeter van de ISO 27001-certificering opgenomen:

- de informatiesystemen en data van de klanten van NRB.
- de apparatuur en software waarvan de klanten en de leveranciers instaan voor het veiligheidsbeheer.

Een gedetailleerde en bijgewerkte omschrijving van het informatiesysteem is indien nodig opgenomen in de perimeter van het ISMS en is beschikbaar in de CMDB (Configuration Management DataBase) en het Asset Management.

3 Engagement
Missie, visie en waarden

De visie van NRB beschrijft onze ambitie, de invloed die we willen uitoefenen op de maatschappij:
NRB geeft vorm aan de digitale toekomst en draagt bij aan een meer verbonden, veilige, inclusieve en duurzame samenleving. Door middel van impactvolle en verantwoorde technologische oplossingen vereenvoudigt en verrijkt NRB ieders dagelijks leven.

De missie bepaalt onze bestaansreden. Ze legt uit op welke markten we actief zijn, onze doelstellingen en onze bijzonderheden :
NRB ondersteunt Europese organisaties uit de private en publieke sector door te voorzien in al hun technologische behoeften, gebaseerd op een diepgaand begrip van hun activiteiten.

Met de expertise van zijn medewerkers, een solide technologisch ecosysteem en een soevereine benadering treedt NRB op als integrator van complete oplossingen, waardoor zijn klanten hun dagelijkse uitdagingen kunnen ondersteunen.We, as the NRB community, commit to deliver optimal, secured, end-to-end ICT solutions and services, in a long term partnership with customers from the public and private sectors, to simplify technological, economical and societal transformation, through proven innovation, shared expertise and our empowered people."

In dat opzicht en met het oog op de nieuwe risico's die het gebruik van de technologie met zich meebrengt, moeten we de veiligheid van de informatiesystemen voortaan als een van de pijlers van onze dienstverlening beschouwen. We zijn begonnen met de 'ISO 27001:2013'-certificeringsprocedure

om te laten zien dat we ons permanent engageren om de informatiemiddelen van onze klanten te beschermen.

Aangezien de beveiliging van onze diensten en gegevens centraal staat in ons strategisch plan, is de ISO 27001:2022-certificering een waardevolle troef voor de ontwikkeling van de onderneming.

De waarden die daaruit voortvloeien zijn transparant op het vlak van onze relaties met onze medewerkers, onze partners, onze aandeelhouders, de onderneming in het algemeen en, uiteraard, onze klanten.

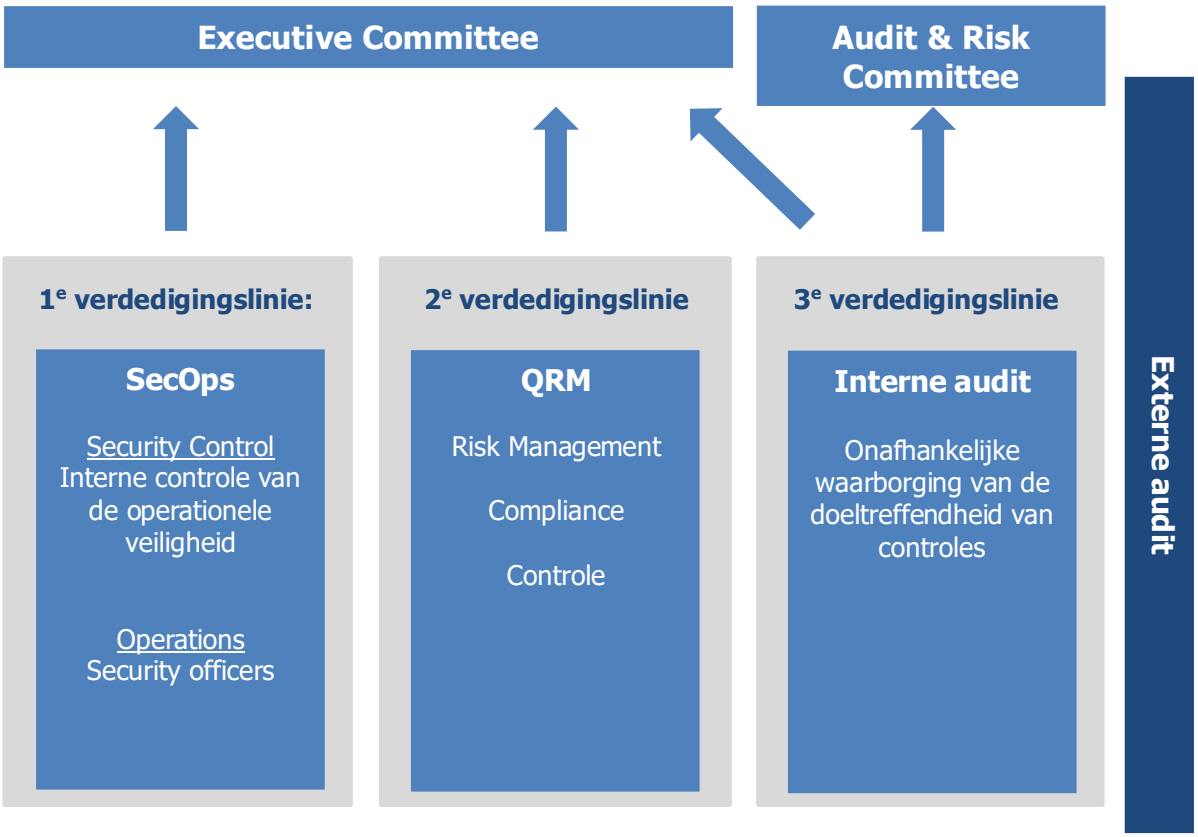
- Integriteit : We respecteren onze verplichtingen en hechten waarde aan transparantie en eerlijkheid. Geleid door onze bedrijfsethiek bouwen we relaties op die gebaseerd zijn op vertrouwen en betrouwbaarheid ;
- Enthousiasme: We creëren een dynamische werkomgeving en bevorderen een positieve sfeer. We houden van wat we bouwen en vieren succes ;
- Empathie: We luisteren actief om de behoeften van onze collega's, klanten en partners te begrijpen. We werken samen in authentieke en respectvolle relaties ;
- Prestatie: Samen streven we ernaar onze doelstellingen te halen of te overtreffen door efficiëntie, kwaliteit en voortdurende verbetering ;
- Vindingrijkheid: Samen challengen we proactief de normen en stellen we pragmatische, innovatieve oplossingen voor. Dankzij onze nieuwsgierigheid kunnen we obstakels overwinnen.

Dit beleid is goedgekeurd door het Executive Committee van NRB dat alles in het werk stelt om de nodige middelen te verschaffen voor de implementatie ervan.

De verantwoordelijkheid voor het ISMS is toevertrouwd aan de Information Systems Security Manager.
Elke medewerker van NRB moet het beleid van het ISMS ook naleven.

4 Rollen en verantwoordelijkheden

De governance van het ISMS is gebaseerd op 3 verdedigingslinies. De coördinatie en de communicatie verlopen via meerdere comités.



4.1 Eerste lijn - Afdeling Security Operations

De directeur van de SecOps-afdeling (Chief Security Officer of CSO) is verantwoordelijk voor de eerste verdedigingslinie, d.w.z. de integratie van beveiliging in de bedrijfsprocessen. Hij onderhoudt contacten met de tweede verdedigingslinie, bij de ISSM (Information Systems Security Manager).

In die hoedanigheid is hij verantwoordelijk voor:

- het beheer van de operationele veiligheid,
- het beheer van operationele securitycontroleteams en security officers,
- het competentiebeheer van de leden van het operationele securitycontroleteam,
- de afstemming van de operationele beveiliging op het door de ISSM vastgestelde beveiligingsbeleid,
- de uitvoering van het beveiligingsplan en de doelstellingen die door de ISSM zijn bepaald,
- de feedback over afwijkingen van vastgestelde beleidslijnen, processen en normen,
- de organisatie van het Steering Committee security

4.1.1 Interne controle van de operationele veiligheid

De afdeling Interne Veiligheidscontrole staat onder leiding van de CSO en houdt toezicht op de operationele beveiligingsactiviteiten. Deze afdeling is verantwoordelijk voor de volgende activiteiten:

- de coördinatie van de roll-out en verbetering van operationele processen van het beveiligingsbeheer,
- controle van de conformiteit van de geïmplementeerde processen,
- de coördinatie van de oplossing van beveiligingsincidenten,
- de follow-up van openstaande kwesties na security-incidenten,
- de roll-out en rapportage over prestatie-indicatoren voor beveiligingsmaatregelen,
- de validatie van beveiligingsoperaties (SRQ met hoog risico),
- de validering van de conformiteit van de procedures en technische oplossingen die door de Delivery worden geïmplementeerd.
- technische veiligheidstests.

4.1.2 Security relays

De security relays is een security-expert in een specifiek technologisch domein. Hij is belast met operationele beveiligingstaken en ondersteunt de operationele veiligheidscontrole met zijn expertise. Hij:

- rapporteert afwijkingen van gedefinieerde standaarden en processen aan SecOps en QRM;
- neemt deel aan het opstellen van beveiligingsprocedures in samenwerking met SecOps en beveiligingsbeleid met QRM;
- zorgt ervoor dat SecOps en QRM via de maandelijkse roadmapreviews op de hoogte worden gebracht van de INTERNE projecten met een beveiligingsimpact die door zijn team worden uitgevoerd;
- zorgt ervoor dat relevante informatie over projecten die tijdens de maandelijkse roadmapreviews worden besproken, wordt gedeeld met zijn team.

4.2 Tweede lijn - Service Quality & Risk Management

De directeur van de afdeling Quality & Risk Management is verantwoordelijk voor:

- de goedkeuring van het plan en de beveiligingsdoelstellingen, die door het Executive Committee moeten worden gevalideerd,
- het organiseren van en deelnemen aan de evaluatievergadering over het securitybeheer met het Executive Committee.

4.2.1 Verantwoordelijke voor de beveiliging van de informatiesystemen (ISSM)

De ISSM waarborgt de beveiliging van het informatiesysteem van NRB. Hij treedt op een transversale manier op in alle informatiesystemen van de organisatie. Dat doet hij vanuit een organisatorisch en technisch standpunt en hij werkt daarvoor nauw samen met de verschillende units en hun verschillende projecten.

De doelstellingen van de ISSM vertalen zich in bestuurs-, leiderschaps- en coördinatieactiviteiten zoals die hieronder in het kort toegelicht worden:

Eisen en veiligheidsrichtlijnen

- De securitypolicy's met de kwalitatieve en kwantitatieve eisen in nauwe samenwerking met de medewerkers definiëren.
- De veiligheidsrichtlijnen operationeel houden.
- Monitort de naleving van de policy's en de vereisten.
- Valideert de conformiteit van de processen en technische oplossingen die door de SecOps-dienst worden geïmplementeerd.

Risico- en projectbeheer

- Het beheer van de veiligheidsrisico's in functie van de businessstrategie implementeren en een blootstelling aan bedreigingen handhaven die aanvaardbaar is en door het Executie Committee gevalideerd werd.
- Ervoor zorgen dat lastenboeken van projecten worden vastgesteld en dat de risico's en behoeften op het vlak van informatiebeveiliging worden geïdentificeerd.
- Regelmatig de risico's herzien en mitigatieplannen definiëren.

Coördinatie en richtschema van de veiligheid

- Alle veiligheidsacties tussen de verschillende partijen coördineren en alle belangrijke informatie aan het Executive Committee doorgeven.
- Houdt toezicht op de regelgeving.
- De veiligheidsstrategie in functie van de doelstellingen van NRB voorstellen.
- Het gevalideerde richtschema omzetten in een actieplan.
- Een dashboard m.b.t. de veiligheid opstellen voor de stakeholders.

Beheer van competenties en sensibilisering

- De directie begeleiden bij het definiëren van de rollen en verantwoordelijkheden met betrekking tot de veiligheid.
- De actieplannen voor opleiding, sensibilisering en het beheer van de bedrijfscultuur organiseren en definiëren op het vlak van beveiliging.

Incidentenbeheer

- Controle van het proces van de behandeling van beveiligingsincidenten.

Veerkracht

- Bepaalt de vereisten op het vlak van informatiebeveiliging en continuïteit van het beheersysteem in overeenstemming met de door de Business Continuity Manager vastgestelde businesscontinuïteitsstrategie.

4.3 Derde lijn - Interne audit

De functie van interne audit rapporteert administratief en functioneel aan de Chief Executive Officer, en tegelijk aan het Audit & Risk Committee (zoals gedelegeerd door de raad van bestuur). De functie interne audit heeft te allen tijde rechtstreeks toegang tot de voorzitter van het auditcomité.

De **missie** van interne audit is het verschaffen van onafhankelijke en objectieve zekerheid gericht op het toevoegen van waarde en het verbeteren van de activiteiten van NRB. De interne audit helpt de organisatie haar doelstellingen te bereiken door te voorzien in een systematische en gedisciplineerde aanpak om de doeltreffendheid van de controle-, risicobeheers- en governanceprocessen te beoordelen en te verbeteren.

Een **driejarig auditplan** op hoog niveau en een jaarlijks auditplan worden opgesteld in overleg met het Executive Committee en het Audit & Risk Committee, op basis van een risicobeoordeling.

Het **doel** van de interne audit is bepalen of de risicobeheersing, controleactiviteiten, technologie en governanceprocessen, zoals ontworpen en vertegenwoordigd door de directie van NRB, geschikt zijn en functioneren om te waarborgen dat:

- De risico's worden geïdentificeerd en op passende wijze worden beheerd.
- De interactie met de verschillende governance en toezichtsfuncties plaatsvindt zoals vereist.
- De financiële, beheers- en operationele informatie nauwkeurig, betrouwbaar en correct zijn.
- De acties van de werknemers in overeenstemming zijn met de toepasselijke beleidslijnen, normen, procedures en wet- en regelgeving.
- De resources op economische wijze worden verworven, efficiënt worden gebruikt en afdoende worden beschermd.
- De doelstellingen van de programma's en plannen worden bereikt.
- Kwaliteit en voortdurende verbetering worden bevorderd in het controleproces van de organisatie.
- Significante wet- of regelgevingskwesties die gevolgen kunnen hebben voor NRB tijdig en op passende wijze worden onderkend en aangepakt.

Tijdens de audits kunnen ook mogelijkheden aan het licht komen om de interne controles, de operationele efficiëntie en de reputatie van NRB te verbeteren. Zij worden meegedeeld aan het passende directieniveau.

De interne audit zorgt voor de uitvoering van het genoemde interne auditplan en bestrijkt de volgende **gebieden**:

- Operationele activiteiten
- Certificeringen van beheersystemen (waaronder ISO 9001 en ISO 27001).
- Financiële activiteiten.
- Risicobeheer en conformiteit.
- Beheer van informatie en informatiesystemen, met inbegrip van beveiligings- en controleaspecten.
- Alle andere activiteiten, met inbegrip van personeels- en administratieve functies.

5 De Committees

5.1 Het Executive Committee

Het directiecomité, waarvan de CEO voorzitter is, moet:

- de geschiktheid van de ISSP voor de uitdagingen van NRB valideren;
- de strategische indicatoren van het ISMS presenteren.
- de strategische richting van de beveiliging (jaarplan en beveiligingsdoelstellingen) goedkeuren.
- de budgetten en het personeelsbestand met betrekking tot security valideren;
- minstens 1 keer per jaar een directiebespreking houden waarin alle aspecten m.b.t. de informatiebeveiliging aan bod komen.

Deelnemers:
De leden van het directiecomité zijn de Chief Executive Officer (CEO), de Chief Financial Officer (CFO), de Chief HR Officer (CHRO), de Chief Operations Officer (COO-I) - Infrastructure, de Chief Operations Officer (COO-A) – Applications en de Chief Commercial Officer (CCO).
De directeur Quality & Risk Management (QRM) is een permanente gast, met name voor zaken met betrekking tot beveiliging. Indien nodig kan ook de Chief Security Officer (CSO) worden uitgenodigd.

5.2 Het Audit & Risk Committee

Het Audit & Risk Committee, zoals gedelegeerd door de raad van bestuur:

- valideert het charter van de interne audit. Het charter bepaalt de principes, de basisrollen en de verantwoordelijkheden van de interne-auditfunctie binnen de organisatie. Het charter bepaalt de positie van de interne audit binnen de organisatie, met inbegrip van de aard van de functionele relatie tussen de interne audit, de directie (directiecomité), de raad van bestuur en het auditcomité.
- valideert het driejarig auditplan.
- evalueert de resultaten van alle audits en vastgestelde risico's.
- houdt toezicht op de implementatie van de actieplannen.

5.3 Het Steering Committee security

Het steering committee (SteerCo) security, het tactische controleorgaan van het ISMS, staat onder leiding van de Chief Security Officer en komt ten minste **eenmaal per maand** bijeen.

Doelstellingen:

- Follow-up van het securityprogramma.
- Goedkeuring van de tactische beveiligingsstrategie.
- De strategische indicatoren van het ISMS presenteren.
- Follow-up van belangrijke actieplannen na audits.
- Informatie over belangrijke beveiligingsincidenten en -problemen rapporteren.

Deelnemers:

De leden van het security-steerco zijn

- De Chief Security Officer
- De directeur QRM
- De verantwoordelijke voor de beveiliging van de informatiesystemen (ISSM)
- Op uitnodiging: Projectmanager of betrokken partijen bij securityprojecten

5.4 De Operationele Veiligheidscommissie

De Operationele Veiligheidscommissie (Ops Security Steerco), het operationele toezichtsorgaan voor het ISMS, staat onder leiding van de verantwoordelijke voor de beveiliging van de informatiesystemen en komt ten minste één keer om de 2 weken bijeen.

Doelstellingen:

- Opvolgen van prestatie-indicatoren voor beveiligingsmaatregelen
- Follow-up van beveiligingsincidenten en -problemen
- Follow-up van actieplannen na audits
- Beveiligingswaarschuwingen en beleidsafwijkingen rapporteren
- Beveiligingsinformatie doorgeven

Deelnemers:

De leden van het stuurcomité zijn:

- De Information Systems Security Manager,
- De Chief Security Officer of zijn vertegenwoordiger,
- Af en toe de stakeholders, afhankelijk van de besproken onderwerpen (Security Control, Internal IT, functies).

5.5 Verslagen van comitévergaderingen

Van de vergaderingen van al deze comités worden notulen opgesteld.

5.6 RACI

	Executive Committee	Directeur QRM	ISSM	CSO SecOps	Operationele actoren	Elke persoon in dienst bij NRB
Voorstellen		C	A/R	R		
Valideren	A	C	R	C		
De toepassing controleren	A		R	R		
Toepassen/Naleven						A
Behouden		C	A/R	R		
Communiceren		A	R	R	C	I

R = responsible = de persoon die verantwoordelijk is voor de uitvoering van de activiteit.
A = accountable = de persoon met de eindverantwoordelijkheid voor de activiteit, diegene die over de voortgang en de kwaliteit van de activiteit moet rapporteren.
C = consulted = de personen waaraan anderen advies kunnen vragen.
I = informed = de personen die geïnformeerd moeten worden.

6 De richtlijnen/basisregels

- Verantwoordelijkheid aanmoedigen via de governance van de veiligheid van het informatiesysteem en het Executive Committee;
- De informatie van de datacenters beschermen tegen interne en externe bedreigingen, of ze nu opzettelijk of onopzettelijk zijn;
- Een risicogebaseerde aanpak implementeren;
- De veerkracht van de organisatie (BCM/DRP/ISCP) op een beveiligde manier verhogen;
- Zijn blootstelling aan interne en externe bedreigingen beperken;
- De verschillende veiligheidseisen voortdurend en regelmatig controleren;
- Het personeel als geheel sensibiliseren en opleiden;
- De veiligheid van het informatiesysteem coördineren;
- De verworven kennis voortdurend verbeteren.

7 De geïmplementeerde maatregelen en controles

Om te waarborgen dat de activiteiten van de businesses en de IT-activiteiten m.b.t. de veiligheid van de informatiesystemen op elkaar afgestemd zijn, werd een procedure voor het risicobeheer geïmplementeerd. Deze procedure is gebaseerd op de 'ISO 27005:2018'-norm.

Om risico's te evalueren worden vier criteria gehanteerd:

- **Vertrouwelijkheid:** de vertrouwelijkheid van de informatie van de klanten moet gewaarborgd worden. Bovendien moet de toegang tot de verschillende delen van het datacenter gecontroleerd worden;
- **Integriteit:** de integriteit van de informatie van klanten moet gewaarborgd worden;
- **Beschikbaarheid:** de informatie moet beschikbaar zijn voor de medewerkers die het datacenter onderhouden en voor de klanten die gebruik maken van de diensten van het datacenter, zoals gedefinieerd in de procedures van de onderneming en de verplichtingen m.b.t. de kwaliteit van de dienstverlening aan de klanten;
- **Bewijsmateriaal:** de traceerbaarheid van de toegang tot klanteninformatie of de eigen informatie van NRB moet worden gewaarborgd.

De methodologie voor de analyse van veiligheidsrisico's die we bij NRB gebruiken, wordt uitgebreid beschreven in het document 'Methode voor de risicoanalyse van de veiligheid'.

8 Review

Het huidige beleid wordt jaarlijks systematisch herzien.
Naast deze jaarlijkse herziening, wordt dit beleid aangepast bij elke grote verandering in de organisatorische structuur die een impact heeft op het ISMS. Zo kunnen we rekening houden met de wijzigingen en de veiligheidsrisico's zo optimaal mogelijk beheren.

9 Bijlagen

9.1 Referenties

De referentiedocumenten:

- Methode voor de analyse van beveiligingsrisico's
- ISO/IEC 27001: 2022

9.2 Beheer document

Redacteur	Thibault Dutrieux			
Updates	Versie	Datum	Omschrijving	
	4.4	12/12/2024	Kleine update met de nieuwe missies, visie en waarden van NRB	
Validation	4.4	16/12/2024	Nagelezen en gevalideerd door Emmanuelle Lhermitte	Finaal
	4.3	21/11/2023	Directiecomité	Finaal
	4.4	20/12/2024	Executive Committee	Finaal
Status van het document	**Goedgekeurd door het Executive Committee van NRB**			