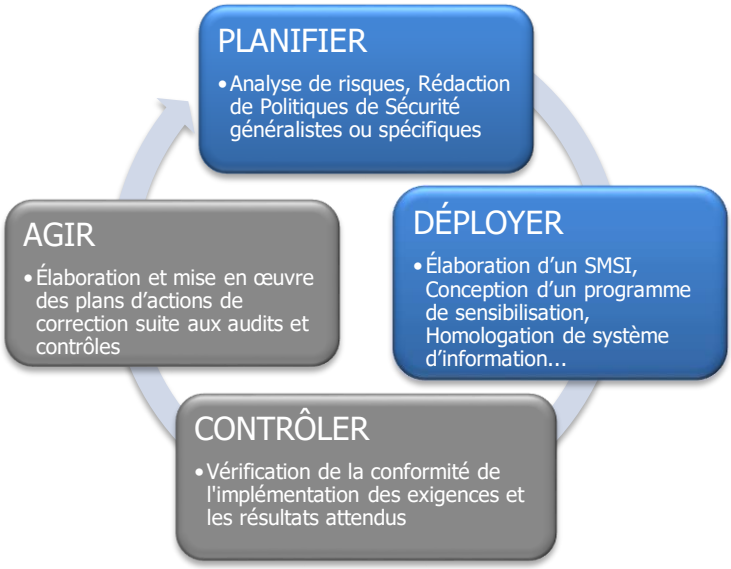
Politique du Système de Management de la Sécurité de l'information

1 Objectifs

L'approche globale du Système de Management de la Sécurité de l'Information (SMSI) est de garantir la pérennisation de la sécurité dans l'ensemble des processus inclus dans le périmètre au travers d'une approche PDCA. Cette approche implique une industrialisation de la sécurité du Système d'Information à tous les niveaux et une implication auprès de toutes les parties prenantes.



Cette approche tient compte des exigences :

- légales en vigueur en Belgique et en Grèce,
- réglementaires,
- de nos clients.

2 Périmètre d'applicabilité

Le système de management de la sécurité de l'information concerne :

- La Gestion opérationnelle de l'infrastructure informatique, le développement de logiciels, l'intégration et la maintenance, la consultance ainsi que le 'Managed Staffing'.
- Le Système d'Information de NRB, qui permet la réalisation des activités concernées.
- Les Data centers de NRB situés à Herstal.

2.1 Présentation de NRB

NRB a été fondée en 1987 et est aujourd'hui un des acteurs majeurs des services informatiques en Belgique.

NRB est à même de proposer un éventail complet de services et solutions ICT globale, pour accompagner ses clients tout au long du cycle de vie de leurs projets IT. Ainsi, NRB met en place et gère une infrastructure cloud privé et hybride. Parallèlement, NRB conçoit l'architecture et développe, gère et maintient les applications (mainframe ou open systems), qu'elles soient conçues sur mesure ou personnalisées et configurées à partir de progiciels ERP (Enterprise Resource Planning) [SAP], ECM (Entreprise Content Management) ou BI (Business Intelligence). NRB offre également des services de

Consulting et de Managed Staffing. Forte de plus de 35 années d'expérience, NRB fournit des solutions et des services informatiques à destination du secteur financier, du secteur public et social au niveau régional et fédéral, du secteur des soins de santé et du secteur des utilités publiques, de l'industrie et du secteur biotech.

2.2 Structure organisationnelle interne

L'organisation de NRB s'articule autour de trois composantes qui sont « Sales », « Delivery » et « Central Services », afin de garantir son offre de service auprès de ses clients.

Les entités Sales ont pour mission :

- de fidéliser les clients actuels et d'y développer le courant d'affaires rentables ;
- d'attirer de nouveaux clients avec des contrats rentables et de booster la croissance de NRB en offrant des solutions et des services prioritairement fournis par les Services Lines du Delivery de NRB, les succursales et les filiales.

Les entités Sales sont chacune responsables des secteurs spécifiques du marché répartis par branche d'activité. Trois entités transversales fournissent aux entités Sales des services de support en matière de Bid management et de Marketing.

Le Client Delivery se structurera en « Competence centers » au sein desquels les collaborateurs seront regroupés selon leur métier et domaines d'expertise. En fonction des besoins des clients et des compétences métiers que les projets (produits/services) nécessiteront, les membres seront mobilisés en équipes pluridisciplinaires au sein de « Delivery Units ».

Les entités Sales et les divisions Delivery bénéficient du soutien des Central Functions :

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

2.3 Périmètre d'applicabilité

2.3.1 Périmètre géographique

L'entreprise, dont le siège social est à Herstal, est présente en Belgique et en Grèce.

Le Data center de NRB se situe sur le site du siège social de l'entreprise à Herstal. NRB dispose également d'un data center à Villers-le-Bouillet (à 30 km du site de Herstal), propriété de BelgiumDC, une joint-venture dans laquelle NRB possède 50 % des parts.

Les activités de NRB S.A. sont effectuées à partir de différents sites d'exploitation, à savoir :

- Parc Industriel des Hauts Sarts, 2ème Avenue 65, 4040 Herstal, Belgique
- Interleuvenlaan 10, 3001 Heverlee, Belgique
- Ethnikis Antistasis Street 67, 15231 Chalandri, Grèce

Le périmètre géographique du SMSI comprend le centre de données de NRB ainsi que les sites d'exploitation.

Les filiales ne sont pas incluses dans le périmètre du SMSI. Seule NRB S.A. fait partie du périmètre du SMSI.

2.3.2 Périmètre humain

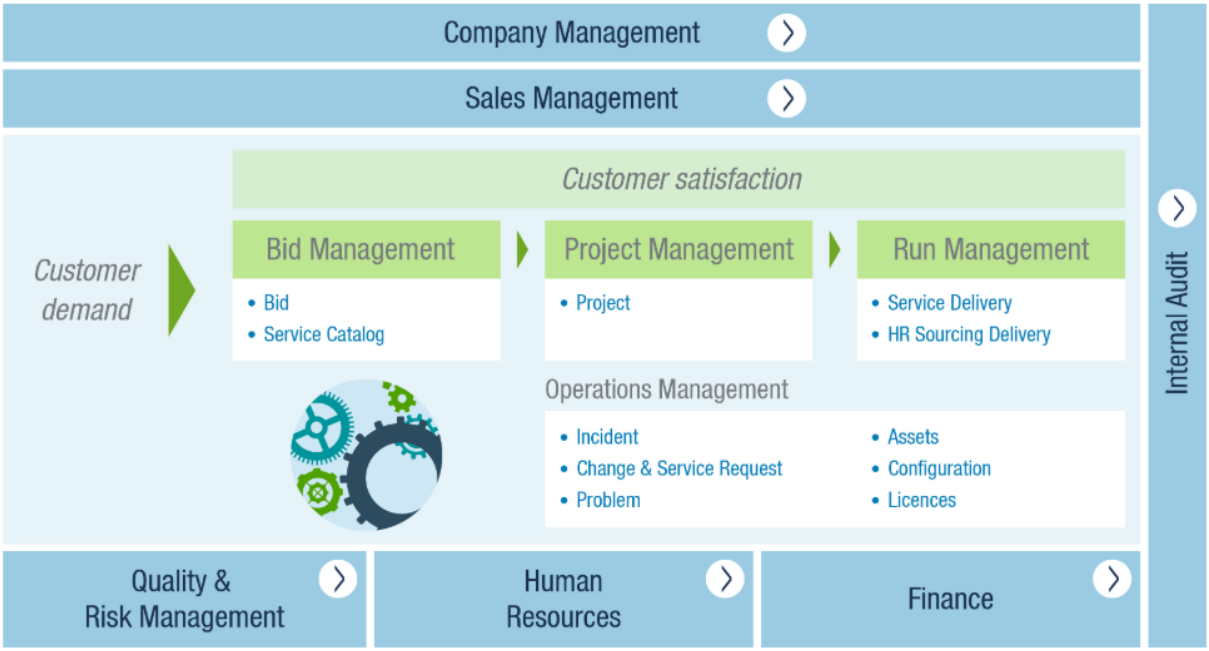
Le périmètre humain du SMSI comprend l'ensemble des équipes de NRB ayant en charge l'administration du Data center et des services métiers prestés par NRB.

Le personnel inclus dans le périmètre de la certification concerne les postes dont les activités sont incluses au sein du périmètre du SMSI.

2.3.3 Périmètre et limites du SMSI

2.3.3.1 Périmètre du SMSI

NRB est organisée autour de processus. La cartographie ci-dessous matérialise le périmètre du SMSI, avec les différents processus :



Le périmètre inclut tous les services fournis par NRB à ses clients, à travers les processus susmentionnés et e, s'appuyant sur les équipements d'infrastructure dont NRB est propriétaire ou que NRB loue, à savoir :

- les baies de serveurs et de stockage,
- les serveurs informatiques,
- les installations d'hébergement,
- les liens télécoms,
- les infrastructures réseau dont la propriété incombe à NRB.

NRB est cliente de sa propre activité « data center » qui héberge les données de toute l'entreprise. Ce périmètre comprend :

- le système d'information interne à NRB (informations et toutes ressources permettant leur traitement quel qu'il soit) ;
- le système d'information d'administration du « data center » ;
- les applications dont NRB est propriétaire (le propriétaire des données utilise des applications internes mutualisées de NRB) ;
- les applications internes de NRB ;
- les données dont la propriété incombe à NRB.

2.3.3.2 Les limites du SMSI

Bien que NRB opère certains aspects de la sécurité de ses clients, sont exclus du périmètre du SMSI 27001 et donc en-dehors du périmètre de la certification ISO 27001 :

- les systèmes d'information et données des clients de NRB ;
- les équipements et logiciels dont la responsabilité de la gestion de la sécurité est laissée aux clients et fournisseurs.

Au besoin, une description détaillée et à jour des actifs du Système d'Information inclus dans le périmètre du SMSI est disponible dans la CMDB (Configuration Management Database) ainsi que dans l'Asset Management.

3 Engagement
Mission, vision et valeurs

La vision de NRB décrit notre ambition, l'influence que nous voulons avoir sur la société :
NRB façonne l'avenir numérique et contribue à une société plus connectée, sécurisée, inclusive et durable. Au travers de solutions technologiques impactantes et responsables, NRB simplifie et enrichit le quotidien de chacun.

La mission définit notre raison d'être. Elle explique sur quels marchés nous opérons, nos buts et nos particularités :
NRB accompagne les organisations privées et publiques européennes en prenant en charge l'ensemble de leurs besoins technologiques, tout en s'appuyant sur une compréhension approfondie de leurs métiers. Avec l'expertise de ses collaborateurs, un écosystème technologique solide et une approche souveraine, NRB agit comme un intégrateur de solutions complètes, permettant à ses clients de supporter leurs défis au quotidien.

À ce titre, et au vu des nouveaux risques induits par l'utilisation de la technologie, il est désormais inévitable de considérer la sécurité des systèmes d'information comme l'un des piliers de la fourniture de nos services. Afin de prouver notre engagement permanent à protéger le patrimoine informationnel de nos clients, nous sommes engagés dans le processus de certification ISO 27001:2013.

Etant donné que la sécurité de nos services et des données sont au cœur de notre plan stratégique, la certification ISO 27001:2022 constitue un précieux atout pour le développement de l'entreprise.

Les valeurs qui en découlent sont transparentes dans nos relations avec nos collaborateurs, nos partenaires, nos actionnaires, la société en général et, bien entendu, nos clients.

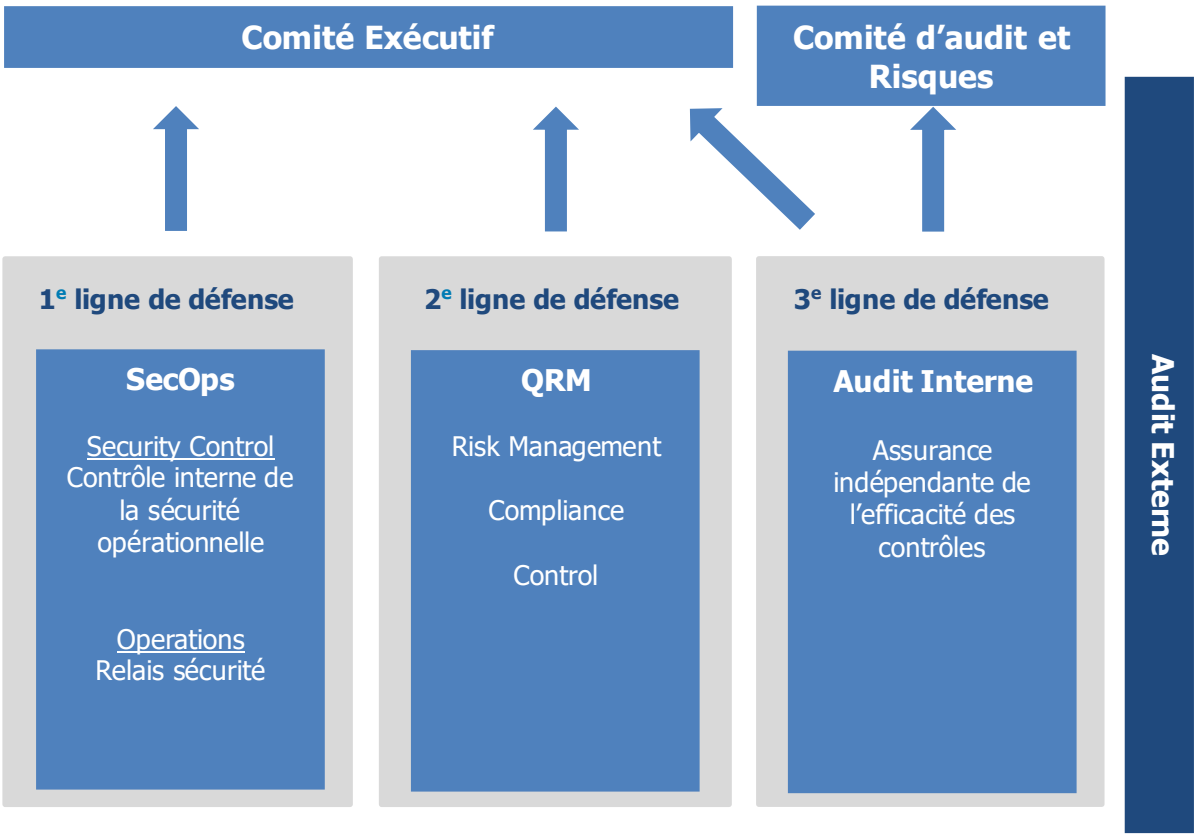
- Intégrité : nous respectons nos engagements, nous valorisons la transparence et l'honnêteté. Guidés par notre éthique professionnelle, nous établissons des relations basées sur la confiance et la fiabilité ;
- Enthousiasme : nous créons tous un environnement de travail dynamique et favorisons une atmosphère positive. Nous prenons plaisir à ce que nous faisons ensemble et célébrons nos réussites ;
- Empathie : nous écoutons activement pour comprendre les besoins de nos collègues, clients et partenaires. Nous collaborons au travers de relations respectueuses et authentiques ;
- Performance : ensemble, nous travaillons pour atteindre ou dépasser nos objectifs grâce à l'efficacité, la qualité et l'amélioration continue ;
- Ingéniosité : en collaborant, nous remettons en question les normes et proposons de façon proactive des solutions pragmatiques et innovantes. Nous surmontons les obstacles grâce à notre curiosité.

La présente politique est approuvée par le Comité Exécutif de NRB qui s'engage à fournir les moyens nécessaires pour la mettre en œuvre.

La responsabilité du SMSI est confiée au Responsable de la Sécurité des Systèmes d'Information. Chaque collaborateur de NRB est également tenu de respecter la politique du SMSI.

4 Rôles et responsabilités

La gouvernance du SMSI est basée sur une structure formée de 3 lignes de défense. Le pilotage et la communication sont effectués à travers plusieurs comités.



4.1 Première ligne – Département Security Operations

Le directeur du département SecOps (Chief Security Officer ou CSO) est responsable de la première ligne de défense, c.-à-d. l'intégration de la sécurité dans les processus opérationnels. Il assure la liaison avec la seconde ligne de défense, auprès du RSSI (Responsable de la Sécurité des Systèmes d'Information).

A ce titre, il est en charge de :

- la gestion de la sécurité opérationnelle,
- la gestion des équipes de contrôle de sécurité opérationnelle et des relais sécurité,
- la gestion des compétences des membres de l'équipe de contrôle de sécurité opérationnelle,
- l'alignement de la sécurité opérationnelle avec la politique de sécurité telle que définie par le RSSI,
- la mise en œuvre du plan et des objectifs de sécurité définis par le RSSI,
- l'identification des écarts avec les politiques, processus et standards définis,
- l'organisation du Steering Committee de sécurité.

4.1.1 Contrôle interne de la sécurité opérationnelle

Le département de contrôle interne de sécurité est dirigé par le CSO et supervise les activités opérationnelles de sécurité. Ce département prend en charge des activités suivantes :

- le pilotage de la mise en œuvre et des améliorations des processus opérationnels de la gestion de la sécurité,
- le contrôle de la conformité des processus implémentés,
- le pilotage de la résolution des incidents de sécurité,
- le suivi des problèmes ouverts à la suite des incidents de sécurité,
- la mise en place et la remontée des indicateurs de performance des mesures de sécurité,
- la validation d'opérations de sécurité (SRQ avec risque élevé),
- la validation de la conformité des procédures et solutions techniques mises en œuvre par le Delivery,
- les tests techniques de sécurité.

4.1.2 Relais sécurité

Le relais sécurité est un expert en sécurité dans un domaine technologique spécifique. Il est en charge des tâches opérationnelles de sécurité et vient en support du contrôle de la sécurité opérationnelle avec son expertise. Il :

- il rapporte tout écart constaté avec les standards et processus définis vers SecOps et QRM ;
- il participe à la rédaction des procédures de sécurité en collaboration avec SecOps, et des politiques de sécurité avec QRM ;
- il s'assure que SecOps et QRM soient informés des projets INTERNES ayant un impact sécurité qui sont réalisés dans son équipe via les revues mensuelles de la roadmap ;
- il s'assure de partager à son équipe les informations pertinentes sur les projets discutées lors des revues mensuelles de la roadmap.

4.2 Deuxième ligne - Service Quality & Risk Management

Le directeur du département Quality & Risk Management est responsable de :

- approuver le plan et les objectifs de sécurité à faire valider par le Comité Exécutif,
- organiser et participer à la réunion d'évaluation de la gestion de la sécurité avec le Comité Exécutif.

4.2.1 Responsable de la Sécurité des Systèmes d'Information (RSSI)

Le RSSI est le garant de la sécurité du système d'information de NRB. Il intervient de manière transversale sur l'ensemble des Systèmes d'Information de l'organisation d'un point de vue organisationnel et technique, en synergie avec les différentes entités et leurs différents projets.

De façon schématique, les objectifs du RSSI se traduisent en activités de gestion, d'encadrement, et de pilotage telles que présentées ci-dessous :

Exigences et référentiel de sécurité

- Définit, en étroite collaboration avec les collaborateurs, les politiques de sécurité en y incluant les exigences qualitatives et quantitatives.
- Maintient en conditions opérationnelles le référentiel sécurité.
- Contrôle la conformité aux politiques et exigences.
- Valide la conformité des processus et solutions techniques mises en œuvre par le service SecOps.

Gestion des risques et projets

- Met en place une gestion des risques de sécurité en adéquation avec la stratégie métier et maintient une exposition aux menaces acceptable et validée par le Comité Exécutif.
- S'assure que des cahiers des charges des projets soient définis et que les risques et les besoins en matière de sécurité de l'information soient identifiés.
- Revoit régulièrement les risques et définit des plans de mitigation.

Pilotage & schéma directeur de la sécurité

- Coordonne l'ensemble des actions liées à la sécurité entre les différents intervenants et met en évidence toute information considérée comme importante auprès du Comité Exécutif.
- Supervise la veille règlementaire.
- Propose la stratégie Sécurité en adéquation avec les objectifs de NRB.
- Décline le schéma directeur validé en plan d'action.
- Élabore un tableau de bord de sécurité à destination des parties prenantes.

Gestion des compétences et de la sensibilisation

- Accompagne la direction dans la définition des rôles et responsabilités en relation avec la sécurité.
- Organise et définit les plans d'actions de formation, sensibilisation, gestion de la culture d'entreprise en matière de sécurité.

Gestion des incidents

- Contrôle le processus du traitement des incidents de sécurité.

Résilience

- Définit les exigences en matière de sécurité de l'information et de continuité du système de management en accord avec la stratégie de continuité d'affaires définie par le Business Continuity Manager.

4.3 Troisième ligne - Audit interne

La fonction d'audit interne rapporte administrativement et fonctionnellement au Chief Executive Officer, et simultanément au Comité d'audit et risques (tel que délégué par le Conseil d'administration). La fonction d'audit interne dispose à tout moment d'un accès direct au Président du Comité d'audit.

La **mission** de l'audit interne est de fournir une assurance indépendante et objective visant à ajouter de la valeur et à améliorer les opérations de NRB. L'audit interne aide l'organisation à atteindre ses objectifs en apportant une approche systématique et disciplinée pour évaluer et améliorer l'efficacité des processus de contrôle, de gestion des risques et de gouvernance.

Un **plan d'audit triennal** de haut niveau et un plan d'audit annuel sont établis en consultation avec le Comité Exécutif et le Comité d'audit et risques, basés sur une évaluation des risques.

L'audit interne a pour **objet** de déterminer si la gestion des risques, les activités de contrôle, la technologie et les processus de gouvernance, tels qu'ils sont conçus et représentés par la direction de NRB, sont adéquats et fonctionnent de manière à garantir que :

- les risques sont identifiés et gérés de façon appropriée ;
- l'interaction avec les divers organes de gouvernance et les fonctions de contrôle s'effectue au besoin ;
- les informations financières, de gestion et d'exploitation importantes sont exactes, fiables et opportunes ;
- les actions des employés sont conformes aux politiques, standards, procédures et lois et réglementations applicables ;
- les ressources sont acquises de façon économique, utilisées de façon efficiente et adéquatement protégées ;
- les objectifs des programmes et des plans sont atteints ;
- la qualité et l'amélioration continue sont favorisées dans le processus de contrôle de l'organisation ;
- les questions juridiques ou réglementaires importantes qui pourraient avoir une incidence sur NRB sont reconnues et réglées en temps opportun et de façon appropriée.

Des opportunités d'amélioration des contrôles internes, de l'efficacité opérationnelle et de la réputation de NRB peuvent également être identifiées au cours des audits. Elles seront communiquées au niveau de direction approprié.

L'audit interne assure l'exécution dudit plan d'audit interne et couvre les **domaines** suivants :

- Les activités opérationnelles ;
- Les certifications des systèmes de management (entre autres ISO 9001 et ISO 27001) ;
- Les activités financières ;
- La gestion des risques et la conformité ;
- La gestion des informations et des systèmes d'information, y compris les aspects liés à la sécurité et au contrôle ;
- Toutes les autres activités, y compris les ressources humaines et les fonctions administratives.

5 Les Comités

5.1 Le Comité Exécutif

Présidé par le CEO, le Comité Exécutif est chargé de :

- valider l'adéquation de la PSSI avec les enjeux de NRB.
- suivre les indicateurs stratégiques du SMSI.
- approuver l'orientation stratégique de la sécurité (plan annuel et objectifs de sécurité).
- valider les budgets et les effectifs relatifs à la sécurité.
- tenir une revue de direction reprenant les aspects de sécurité de l'information au minimum 1 fois l'an.

Participants :
Les membres qui composent le Comité Exécutif sont le Chief Executive Officer (CEO), le Chief Financial Officer (CFO), le Chief HR Officer (CHRO), le Chief Operations Officer – Infrastructure (COO-I), le Chief Operations Officer – Applications (COO-A) et le Chief Commercial Officer (CCO).
Le directeur Quality & Risk Management (QRM), surtout pour les matières relatives à la sécurité, est un invité permanent. Le Chief Security Officer (CSO) peut également être invité au besoin.

5.2 Le Comité d'audit et risques

Le Comité d'audit et risques, tel que délégué par le Conseil d'administration :

- valide la Charte d'audit interne. La Charte définit les principes, les rôles de base et les responsabilités de la fonction d'audit interne au sein de l'organisation. La Charte définit la position de l'audit interne au sein de l'organisation, y compris la nature de la relation fonctionnelle entre l'audit interne, la direction (Comité de direction), le Conseil d'administration et le Comité d'audit.
- valide le Plan d'audit triennal.
- revoit les résultats de tous les audits et les risques identifiés.
- suit l'implémentation des plans d'actions.
-

5.3 Le Steering Committee sécurité

Le steering committee (SteerCo) sécurité, organe de suivi tactique du SMSI, est dirigé par le Chief Security Officer et se réunit au moins **une fois par mois**.

Objectifs :

- Assurer le suivi du programme de sécurité.
- Approuver la stratégie tactique de sécurité.
- Suivre les indicateurs stratégiques du SMSI.
- Suivre les plans d'actions importants consécutifs aux audits.
- Remonter les informations sur les incidents et problèmes de sécurité importants.

Participants :
Les membres constituant le Steerco sécurité sont :

- Le Chief Security Officer
- Le Directeur QRM
- Le Responsable de la Sécurité des Systèmes d'Information (RSSI)
- Sur invitation : Project Manager ou parties prenantes de projets de sécurité

5.4 Le Comité de Sécurité Opérationnelle

Le Comité Sécurité Opérationnelle (Ops Security Steerco), organe de suivi opérationnel du SMSI, est piloté par le Responsable de la Sécurité des Systèmes d'Information et se réunit au moins une fois toutes les 2 semaines.

Objectifs :

- Suivre les indicateurs de performance des mesures de sécurité.
- Effectuer le suivi des incidents et problèmes de sécurité.
- Suivre les plans d'actions consécutifs aux audits.
- Remonter les alertes de sécurité et les déviations en regard des politiques.
- Relayer les informations de sécurité.

Participants :
Les membres constituant le Copil sont :

- Le Responsable de la Sécurité des Systèmes d'Information,
- Le Chief Security Officer ou son représentant,
- Les parties prenantes, ponctuellement en fonction des thèmes abordés (Security Control, Internal IT, métiers).

5.5 Enregistrements des réunions du comité

Des enregistrements sont produits pour les réunions de tous ces comités.

5.6 RACI

	Comité Exécutif	Directeur QRM	RSSI	CSO SecOps	Acteurs opérationnels	Toute personne au service de NRB
Proposer		C	A/R	R		
Valider	A	C	R	C		
Contrôler l'application	A		R	R		
Appliquer/ Respecter						A
Maintenir		C	A/R	R		
Communiquer		A	R	R	C	I

R = responsible = celui qui a la responsabilité de réaliser l'activité
A = accountable = celui qui a la responsabilité finale de l'activité, c'est-à-dire qui doit rendre des comptes sur l'avancement et la qualité de l'activité
C = consulted = les personnes qui doivent être consultées
I = informed = les personnes qui doivent être informées

6 Les principes directeurs/les règles de base

- Engager des responsabilités à travers la gouvernance de la sécurité du système de l'information et du Comité Exécutif ;
- Protéger les informations des centres de données des menaces internes et externes, délibérées ou accidentelles ;
- Déployer une approche par les risques ;
- Développer la résilience de l'organisation (PCA/PRA/PCSI) de façon sécurisée ;
- Réduire son exposition aux menaces internes et externes ;
- Mettre en œuvre du contrôle permanent et périodique des différentes exigences de sécurité ;
- Sensibiliser et former le personnel dans sa globalité ;
- Piloter la sécurité du Système d'Information ;
- Améliorer continuellement les acquis.

7 Les mesures et contrôles mis en place

Afin de s'assurer que les activités métiers et IT sont harmonisées au regard de la sécurité des Systèmes d'Information, un processus de management des risques a été mis en œuvre. Ce processus est basé sur la norme ISO 27005:2018.

Quatre critères sont utilisés pour évaluer les risques :

- **Confidentialité :** la confidentialité des informations des clients doit être assurée. En outre, les accès aux différentes parties du data center doivent être contrôlés ;
- **Intégrité :** l'intégrité des informations des clients doit être assurée ;
- **Disponibilité :** les informations doivent être disponibles pour les collaborateurs maintenant le data center et les clients qui bénéficient des services de celui-ci, comme défini dans les procédures de l'entreprise et les obligations de qualité de service vis-à-vis des clients ;
- **Preuve :** la traçabilité des accès aux informations des clients ou aux informations propres de NRB doit être assurée.

Le détail de la méthodologie d'analyse des risques de sécurité utilisée chez NRB est documenté dans le document « Méthode d'analyse des risques de sécurité ».

8 Examen

La présente politique est passée systématiquement en revue annuellement.
Outre cette révision annuelle, cette politique est modifiée à chaque changement majeur de l'organisation ayant un impact sur le SMSI, afin de tenir compte des modifications et ainsi garantir un maintien optimum de la maitrise des risques de sécurité.

9 Annexes

9.1 Références

Documents de référence :

- Méthode d'analyse des risques de sécurité
- ISO/CEI 27001:2022

9.2 Gestion du document

Rédacteur	Thibault Dutrieux			
Mises à jour	Version	Date	Description	
	4.4	12/12/2024	Update mineur avec les nouvelles missions, vision et valeurs de NRB	
Validation	4.4	16/12/2024	Relu et validé par Emmanuelle Lhermitte	Final
Approbation	4.3	21/11/2023	Comité de Direction	Final
	4.4	20/12/2024	Comité Exécutif	Final
Statut du document	**Approuvé par le Comité Exécutif de NRB**			