NRB

DARING TO COMMIT

RÈGLEMENTATION DORA : LIVRE BLANC PORTANT SUR L'APPROCHE DE NRB

1. Préambule

1.1 A QUI S'ADRESSE CE LIVRE BLANC ?

Le présent livre blanc s'adresse aux prospects et clients de NRB qui sont des entités financières soumises au règlement **(UE) 2022/2554** du Parlement Européen et du Conseil **sur la résilience opérationnelle numérique du secteur financier** (« DORA ») entré en vigueur le 17 janvier 2025.

Les enjeux de cette règlementation ne concernent pas uniquement les entités financières. Les «prestataires tiers de services TIC », comme les nomme DORA, entrent aussi dans son champ d'application. NRB, en tant que partenaire stratégique de certaines entités financières, est donc concernée et impactée par certains sujets de DORA.

1.2 POURQUOI CE LIVRE BLANC ?

Ce livre a pour vocation de communiquer aux entités financières concernées des informations relatives à NRB et à sa résilience opérationnelle, qui leur seront utiles dans leur trajet de mise en conformité à DORA ou de démonstration de celle-ci. Le présent livre blanc ne constitue pas un engagement contractuel de la part de NRB.

2. Programme de conformité de NRB

NRB dispose d'un programme de conformité solide qui adresse divers aspects nécessaires pour assurer la sécurité des données du client ainsi que la continuité de ses propres activités TIC. La présente section énonce quelques exemples du programme de conformité suivi par NRB.

2.1 CONFORMITÉ AU RGPD

Dans le cadre de la fourniture des services TIC, NRB est amenée à traiter des données à caractère personnel du client (« DACP »). NRB garantit leur protection conformément au Règlement Général sur la Protection des Données (RGPD). NRB assure que tous ses processus internes respectent les principes du RGPD, garantissant ainsi la confidentialité et la sécurité des données personnelles de ses clients.

2.2 POLITIQUE SMSI

L'approche globale du Système de Management de la Sécurité de l'Information (SMSI) de NRB vise à pérenniser la sécurité dans l'ensemble des processus inclus dans le périmètre. La politique SMSI de NRB se base notamment sur les règles suivantes :

- 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, intentionnelles ou accidentelles ;

- Déployer une approche par les risques ;
- Développer la résilience de l'organisation 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 l'ensemble du personnel;
- Piloter la sécurité du Système d'Information ;
- Améliorer continuellement les acquis.

2.3 CERTIFICATIONS ET RAPPORTS D'ASSURANCE

NRB accorde la plus grande vigilance et le plus grand soin à la sécurité de ses données et informations ainsi qu'à celles de ses clients. NRB maintient des programmes de qualité, de sécurité et de conformité rigoureux attestés par les certifications obtenues.

2.3.1 CERTIFICATIONS DE NRB

→ ISO 9001 : la preuve de l'engagement de NRB sur la qualité de ses processus

Le Système de Management de la Qualité (SMQ) de NRB est certifié conforme à la norme internationale ISO9001 depuis 2004. Cette certification atteste de l'engagement de NRB à améliorer continuellement ses processus et à satisfaire pleinement les exigences de ses clients.

→ ISO 20000 : la preuve de l'engagement de NRB à fournir des services IT de haute qualité

Cette certification en gestion des services atteste de la capacité de NRB à fournir des services informatiques de haute qualité, répondant ainsi aux exigences des clients et des parties prenantes.

→ ISO 27001 : la preuve de l'engagement de NRB envers la sécurité de l'information

Le Système de Management de la Sécurité des Informations (SMSI) de NRB est certifié conforme à la norme internationale ISO27001 depuis 2016. Cette certification démontre l'engagement de NRB à protéger les données de ses clients et à garantir la confidentialité, l'intégrité et la disponibilité des informations selon les standards internationaux les plus exigeants.

En adoptant les meilleures pratiques et des processus rigoureux en matière de gestion des risques et de sécurité, NRB s'assure que des mesures idoines sont en place pour prévenir les violations de données, réduire les risques de cybermenaces et répondre efficacement aux incidents potentiels.

La dernière version est disponible sur le site internet de NRB. NRB tient également à disposition de ses clients la déclaration d'applicabilité ainsi que la politique générale de sécurité.

2.3.2 RAPPORTS

Les différents rapports ISAE, réalisés par un auditeur indépendant, authentifient la robustesse et l'efficacité des contrôles internes de NRB.

→ ISAE3402 : ASSURANCE SUR LA SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Ce rapport atteste que les centres de données de NRB respectent des standards rigoureux internationaux en matière de **sécurité physique, environnementale et opérationnelle** et reflète l'engagement de NRB envers une gestion sécurisée et exemplaire.

En obtenant une opinion favorable sur son infrastructure et ses pratiques de sécurité, NRB offre à ses clients une transparence accrue et une pleine assurance quant à la protection de leurs données sensibles.

→ ISAE3000 : ASSURANCE SUR LES PROCESSUS CLÉS DU DÉPARTEMENT MAINFRAME

Ce rapport évalue la qualité des **systèmes de gestion des changements, des incidents, de la disponibilité, des données et de l'accès logique** au sein du département Mainframe de NRB. L'évaluation favorable des pratiques de NRB et de ses contrôles reflète l'engagement de NRB à maintenir des processus robustes et conformes, garantissant ainsi la confiance et la satisfaction de ses clients dans la gestion de leurs informations.

→ ISAE3000 : ASSURANCE SUR LA GESTION DE LA CONTINUITÉ (BCM)

La continuité d'activité de NRB est essentielle. Elle contribue à supporter la continuité d'activité des clients qui s'appuient sur les produits et services de NRB. Ce rapport ISAE vise à donner l'assurance que le processus BCM est effectivement mis en place et qu'il se base (i) sur les analyses de risques opérationnels et (ii) sur les BIA (Business Impact Analysis) pour établir et tester les plans de reprise (BCP) requis.

La mise en place d'une structure de gestion de crise est par ailleurs contrôlée. Il s'agit d'une composante vitale pour assurer la meilleure coordination de toute situation exceptionnelle.

3. NRB et les 5 piliers clés de DORA

Cette section vise à présenter comment NRB, dans son rôle de prestataire tiers de services TIC auprès d'une entité financière cliente, contribue effectivement à la conformité aux différentes exigences de chaque pilier de DORA :

- la gestion des risques liés aux TIC
- la gestion des incidents liés aux TIC
- les tests de résilience opérationnelle numérique
- la gestion des risques liés aux prestataires tiers de services
- le partage d'information

3.1 LA GESTION DES RISQUES LIÉS AUX TIC

DORA impose que les entités financières disposent d'un cadre complet de gestion des risques liés aux TIC prévoyant la gouvernance, la surveillance et le suivi de ceux-ci.

Les exigences de DORA en la matière vont au-delà des portes de l'entité financière. A titre d'exemple, l'article 8.5 de DORA prévoit que les entités financières doivent :

- identifier et documenter tous les processus qui dépendent de prestataires tiers de services TIC ;
- identifier les interconnexions avec des prestataires tiers de services TIC qui fournissent des services qui soutiennent des fonctions critiques ou importantes (CIF).

COMMENT NRB PEUT-ELLE AIDER ?

- Donner de l'information et de l'assurance au client sur les aspects relatifs au cadre de gestion des risques, mais vu de l'angle de NRB et en rapport avec les services qu'elle fournit.
- Conseiller le client et lui assurer que les services du contrat lui permettent de garantir la conformité face aux exigences de DORA.

QUELQUES ÉLÉMENTS CLÉS :

- **Gouvernance et organisation**. NRB dispose d'un cadre de gouvernance et de contrôle interne selon un modèle reposant sur trois lignes de défense, qui garantit une gestion efficace et prudente du risque lié aux TIC en vue d'atteindre un niveau élevé de résilience opérationnelle numérique.
- **Cadre de gestion du risque lié aux TIC.** L'approche de la gestion des risques de NRB est basée sur les meilleures pratiques et normes internationales, tout en tenant compte d'un principe de proportionnalité comme mentionné dans DORA. Ce cadre englobe notamment des stratégies, politiques et procédures solides et bien documentées qui permettent de parer aux risques liés aux TIC de manière rapide, efficiente et exhaustive et de garantir un niveau élevé de résilience opérationnelle numérique.
- **Identification.** NRB assure une identification, une évaluation et une atténuation proactive des risques. Cette méthodologie structurée permet de prévenir les incidents avant qu'ils ne surviennent, garantissant ainsi une protection continue des opérations de ses clients.
- **Protection et prévention.** NRB fournit des solutions TIC qui permettent aux entités financières de garantir la sécurité des données, de réduire au minimum le risque de corruption ou de perte de données.
- **Détection.** NRB a mis en place des mécanismes permettant de détecter rapidement les activités anormales, y compris les problèmes de performance des réseaux de TIC et les incidents liés aux TIC, ainsi que de repérer les points uniques de défaillance potentiellement significatifs.
- **Sauvegarde, réponse, rétablissement.** NRB dispose d'une politique de continuité des activités de TIC complète ainsi que de dispositifs, de plans, de procédures et mécanismes spécifiques pour répondre aux incidents liés aux TIC.
- **Apprentissage des leçons et améliorations au sein de NRB.** NRB recueille les informations sur les évènements perturbants ou susceptibles de perturber ses activités et services, tels que les incidents, vulnérabilités, menaces. NRB analyse leurs causes et, si nécessaire, détermine des améliorations à apporter aux opérations de TIC ou dans le cadre de la politique de continuité des activités de TIC.

3.2 LA GESTION DES INCIDENTS LIÉS AUX TIC

DORA impose aux entités financières certaines exigences en matière de gestion, classification et notification des incidents liés aux TIC.

COMMENT NRB PEUT-ELLE AIDER ?

- **Conseiller le client et l'aider à mettre en place une gestion conforme des incidents.** NRB propose des services adaptés qui permettent de rencontrer cette exigence.
- **Surveiller en 24/7 les systèmes.** NRB propose un système de monitoring avancé utilisant des technologies de pointe et assurant une surveillance proactive de tous les éléments critiques de l'infrastructure du client. Cela permet à NRB d'identifier et de réagir rapidement aux menaces potentielles.
- **Gérer les incidents avec rapidité, efficacité et réactivité.** NRB dispose de procédures claires et d'équipes dédiées à la gestion des incidents afin de détecter, de gérer et de notifier au client les incidents liés aux TIC. En cas de détection d'incident, les protocoles de réponse de NRB sont déclenchés immédiatement pour contenir et résoudre le problème avec un minimum d'impact sur le client.
- **Communiquer avec transparence.** NRB est organisée pour communiquer au client tout incident susceptible de l'impacter ainsi que les informations dont le client a besoin pour respecter ses obligations en matière de notification des incidents majeurs liés aux TIC aux autorités compétentes.

3.3 LES TESTS DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

DORA impose l'obligation, pour les entités financières, d'établir et de maintenir un programme solide et complet de tests de résilience opérationnelle numérique couvrant ses fonctions critiques ou importantes, sur la base notamment de tests de pénétration fondés sur la menace.

COMMENT NRB PEUT-ELLE AIDER ?

- **Disposer d'un plan solide de continuité.** Le plan de continuité opérationnelle de NRB est organisé et aligné sur la norme ISO 22301. Les éléments clés sont les suivants :

  - **Politique de gestion de crise** : NRB a élaboré des procédures précises pour assurer une prise de décision rapide et coordonnée. La politique de NRB prévoit une réponse coordonnée en cas de crise, incluant des communications internes et externes claires, des procédures d'escalade et des rôles et responsabilités définis pour chaque membre de l'équipe. Ainsi, NRB s'assure que les crises sont gérées avec calme et efficacité.
  - **Scénarios de continuité testés régulièrement** : des exercices de simulation réguliers pour garantir l'efficacité des plans de NRB et l'adhérence de ses équipes.
  - **Plan de Continuité des Activités (PCA)** : NRB a développé un Plan de Continuité des Activités (PCA) robuste, assurant la disponibilité ininterrompue des services de NRB, même en cas de désastre ou d'incident inattendu. Le PCA inclut des stratégies de récupération rapides et efficaces, minimisant les interruptions potentielles. Il comprend des plans techniques de reprise après sinistre (DRP).

- **Tester ses systèmes de manière régulière.** NRB effectue régulièrement des tests de résilience pour évaluer la capacité de ses systèmes à résister et à se rétablir rapidement après des perturbations. Les tests effectués par NRB comprennent des simulations et scenarios variés. NRB sous-traite également à des sociétés externes des tests d'intrusion blackbox, greybox et Red Teaming sur son environnement mutualisé (au moins une fois par an). Dans le cadre de sa certification ISO27001, NRB est également auditée au moins une fois par an.

- **Collaborer aux tests d'intrusion du client.** NRB permet à ses clients d'effectuer des tests de sécurité sur leurs assets hébergés sur les infrastructures de NRB moyennant le respect de règles strictes afin d'éviter tout impact sur les systèmes.

3.4 LA GESTION DES RISQUES LIÉS AUX PRESTATAIRES TIERS DE SERVICES TIC

3.4.1 DUE DILIGENCE

Les principes clés pour une bonne gestion des risques liés aux prestataires tiers de services TIC imposent aux entités financières, dans le respect du principe de proportionnalité, de mener des processus d'évaluation de ces prestataires avant de conclure un accord contractuel sur l'utilisation des TIC.

COMMENT NRB PEUT-ELLE AIDER ?

- Les équipes de NRB **se tiennent à disposition** de l'entité financière tout au long des processus de sélection et d'évaluation pour répondre rapidement aux différentes interrogations que pourrait avoir l'entité financière, que ces questions concernent NRB elle-même ou les services qu'elle fournit.
- NRB porte une attention toute particulière à la **gestion des risques** afin, par exemple, d'éviter les conflits d'intérêt et de garantir une éthique irréprochable comme peut en attester la charte éthique de NRB.
- Lorsque cela est nécessaire et autorisé dans les contrats entre NRB et son client, NRB peut avoir recours à des sous-traitants pour l'exécution de certaines activités. Avant de conclure un contrat avec un sous-traitant, NRB **vérifie la fiabilité** de celui-ci et des services proposés ainsi que leur adéquation avec les exigences du client et de DORA.

3.4.2 ADAPTATION DES CONTRATS

L'article 30 de DORA synthétise les exigences qui doivent être couvertes dans les accords contractuels entre l'entité financière et son prestataire tiers de services TIC.

COMMENT NRB PEUT-ELLE AIDER ?

- **Proposer au client des contrats clairs, adaptés et équilibrés.** NRB veille à ce que les documents contractuels qui couvrent les services TIC qu'elle fournit au client :

    - comportent clairement les droits et obligations des parties en tenant compte de la criticité et/ou de l'importance des services ;

- couvrent les éléments requis par l'article 30 du règlement DORA ainsi que par les normes techniques de règlementation (RTS) en vigueur.

Le modèle de contrat de NRB avec les clauses adaptées à DORA est disponible sur demande.

- **Assurer la sécurité et la continuité dans la chaine de sous-traitance.** NRB veille particulièrement à ce que les contrats qu'elle conclut avec ses sous-traitants tiennent compte des exigences de DORA qui leur sont applicables.

3.4.3 LES REGISTRES D'INFORMATION

DORA impose aux entités financières l'établissement et la mise à jour d'un registre d'information.

COMMENT NRB PEUT-ELLE AIDER ?

- **Identifier les sous-traitants.** Les sous-traitants autorisés sont identifiés dans le contrat entre NRB et son client et/ou dans le contrat de traitement de données personnelles (DPA) le cas échéant.
- **Être disponible et transparent.** NRB se tient à la disposition de son client pour lui fournir les informations relatives à NRB et à la chaine de sous-traitance dont le client a besoin pour tenir et mettre à jour son registre d'information. A cet effet, certaines informations administratives concernant NRB et sa maison mère sont déjà communiquées au point 4.

3.5 LE PARTAGE D'INFORMATION

DORA prévoit des dispositions pour l'échange, entre les entités financières, d'informations et des renseignements sur les cybermenaces ainsi que les conditions et modalités de participation à ces échanges, notamment de la part des prestataires tiers de services TIC.

COMMENT NRB PEUT-ELLE AIDER ?

- **Communiquer de manière transparente**. Autant que possible, NRB facilite le partage d'informations critiques tout en respectant les normes applicables. NRB peut aider ses clients à adopter une approche proactive et collaborative à la cybersécurité.
- **Communiquer de manière sécurisée.** NRB utilise des canaux de communication et des méthodes de transfert de l'information respectant les plus hauts standards de sécurité afin de protéger les données de toutes les parties prenantes.

4. Informations administratives

4.1 A PROPOS DE NRB SA

Network Research Belgium. Numéro d'entreprise : BE0430.502.430

Siège social : Parc Industriel des Hauts-Sarts, 2ième Avenue, 65 4040 Herstal, Belgique

4.2 A PROPOS DE SA MAISON-MÈRE

Ethias SA. Numéro d'entreprise : BE0404.484.654. Siège social à Liège, en Belgique.

4.3 CONTACT

Toute question relative au présent livre blanc peut être adressée à risk@nrb.be