NRB

DARING TO COMMIT

DORA REGULATIONS: WHITE PAPER ON THE NRB APPROACH

1. Preamble

1.1 WHO IS THIS WHITE PAPER AIMED AT?

This white paper is aimed at NRB's prospects and customers who are financial entities subject to the Regulation **(EU) 2022/2554** of the European Parliament and of the Council **on the digital operational resilience of the financial sector** ("DORA"), which came into force on 17 January 2025.

The issues raised by these regulations are not limited to financial entities. "Third-party ICT service providers", as DORA calls them, also fall within its scope. NRB, as a strategic partner of certain financial entities, is therefore concerned by and impacted by certain DORA topics.

1.2 WHY THIS WHITE PAPER?

The purpose of this paper is to provide relevant financial entities with information about NRB and its operational resilience, which will be useful to them in their journey towards DORA compliance or in demonstrating such compliance. This white paper does not constitute a contractual commitment from NRB.

2. NRB's compliance program

NRB has a robust compliance program that addresses various aspects necessary to ensure the security of customer data as well as the continuity of its own ICT activities. This section sets out some examples of the compliance program followed by NRB.

2.1 GDPR COMPLIANCE

As part of the provision of ICT services, NRB may process customer's personal data ("DACP"). NRB guarantees their protection in accordance with the General Data Protection Regulation (GDPR). NRB ensures that all its internal processes comply with the principles of GDPR, guaranteeing the confidentiality and security of its customers' personal data.

2.2 ISMS POLICY

The global approach of NRB's Information Security Management System (ISMS) aims to ensure the long-term security of all processes within its scope. NRB's ISMS policy is based, among other things, on the following rules:

- Assume responsibility through the governance of information system security and the Executive Committee;
- Protect data center information from internal and external threats, whether intentional or accidental;
- Deploy a risk-based approach;
- Develop the resilience of the organisation in a secure way;

- Reduce exposure to internal and external threats;
- Implement permanent and periodic control of the various safety requirements;
- Raise awareness and train all staff;
- Manage the Information System security;
- Continuous improvement of the achievements.

2.3 CERTIFICATIONS AND INSURANCE REPORTS

NRB takes the utmost attention and care to the security of its data and information, as well as that of its customers. NRB maintains rigorous quality, security and compliance programs, as evidenced by the certifications it has obtained.

2.3.1 CERTIFICATIONS OF NRB

→ ISO 9001: proof of NRB's commitment to the quality of its processes

NRB's Quality Management System (QMS) has been certified compliant with the international ISO9001 standard since 2004. This certification testifies to NRB's commitment to continuously improving its processes and fully satisfying its customers' requirements.

→ ISO 20000: proof of NRB's commitment to providing high-quality IT services

This certification in service management attests to NRB's ability to deliver high-quality IT services that meet the requirements of customers and stakeholders.

→ ISO 27001: proof of NRB's commitment to information security

NRB's Information Security Management System (ISMS) has been certified compliant with the international standard ISO27001 since 2016. This certification demonstrates NRB's commitment to protecting its customers' data and guaranteeing the confidentiality, integrity and availability of information in accordance with the most demanding international standards.

By adopting best practice and rigorous risk management and security processes, NRB ensures that appropriate measures are in place to prevent data breaches, reduce the risk of cyber threats and respond effectively to potential incidents.

The latest version is available on the NRB website. NRB also makes the statement of applicability and the general security policy available to its customers.

2.3.2 REPORTS

The various ISAE reports, carried out by an independent auditor, attest to the robustness and effectiveness of NRB's internal controls.

→ ISAE3402: PHYSICAL AND ENVIRONMENTAL SECURITY ASSURANCE

This report certifies that NRB's data centers comply with rigorous standards in terms of **physical, environmental and operational security** and reflects NRB's commitment to secure and exemplary management.

By obtaining a favourable opinion on its infrastructure and security practices, NRB offers its customers increased transparency and complete assurance regarding the protection of their sensitive data.

→ ISAE3000: ASSURANCE ON THE MAINFRAME DEPARTMENT'S KEY PROCESSES

This report assesses the quality of **change, incident, availability, data and logical access management systems** within NRB's mainframe department. The favourable assessment of NRB's practices and controls reflects NRB's commitment to maintaining robust and compliant processes, ensuring the confidence and satisfaction of its customers in the management of their information.

→ ISAE3000: CONTINUITY MANAGEMENT ASSURANCE (BCM)

NRB's business continuity is essential. It helps supporting the business continuity of customers who rely on NRB's products and services. This ISAE report aims to provide assurance that the BCM process is effectively implemented and that it is based (i) on operational risk analyses and (ii) on BIA (Business Impact Analysis) to establish and test the required recovery plans (BCPs).

The implementation of a crisis management structure is also monitored. This is a vital component in ensuring the best possible coordination of any exceptional situation.

3. NRB and the 5 key pillars of DORA

The purpose of this section is to show how NRB, as a third-party ICT service provider to the financial and insurance sector, effectively contributes to compliance with the various requirements of each pillar of DORA:

- ICT risk management
- ICT incident management
- digital operational resilience testing
- managing the risks associated with third-party service providers
- information sharing

3.1 ICT RISK MANAGEMENT

DORA requires financial entities to have a comprehensive ICT risk management framework, including governance, supervision and follow-up of these risks.

DORA's requirements in this area extend beyond the boundaries of the financial entity itself. For example, Article 8.5 of DORA states that financial entities must:

- identify and document all processes that depend on third-party ICT service providers;
- identify the interconnections with third-party ICT service providers that deliver services supporting critical or important functions (CIF).

HOW CAN NRB HELP?

- Provide customer with information and assurance on aspects related to the risk management framework, but from NRB's perspective and in relation to the services it provides.
- Advise the customer and ensure that the contracted services guarantee compliance with DORA's requirements.

SOME KEY POINTS:

- **Governance and organisation**. NRB has a governance and internal control framework based on a three lines of defense model, which ensures effective and prudent management of ICT risk to achieve a high level of digital operational resilience.
- **ICT risk management framework.** NRB's approach to risk management is based on international best practice and standards, while taking into account a principle of proportionality as set out in DORA. This framework includes robust and well-documented strategies, policies and procedures to address ICT-related risks quickly, efficiently and comprehensively, and to ensure a high level of digital business resilience.
- **Identification.** NRB ensures that risks are identified, assessed and mitigated proactively. This structured methodology makes it possible to prevent incidents before they occur, guaranteeing ongoing protection for its customers' operations.
- **Protection and prevention.** NRB provides ICT solutions that enable financial entities to guarantee data security and minimise the risk of data corruption or loss.
- **Detection.** NRB has mechanisms in place to quickly detect abnormal activity, including ICT network performance issues and ICT incidents, as well as potentially significant single points of failure.
- **Backup, response, recovery.** NRB has a comprehensive ICT business continuity policy and specific arrangements, plans, procedures and mechanisms for responding to ICT incidents.
- **Learning lessons and making improvements within NRB.** NRB collects information on events that disrupt or are likely to disrupt its activities and services, such as incidents, vulnerabilities and threats. NRB analyses their causes and, if necessary, identifies improvements to be made to ICT operations or as part of the ICT business continuity policy.

3.2 ICT INCIDENT MANAGEMENT

DORA imposes certain requirements on financial entities in terms of managing, classifying and reporting of ICT-related incidents.

HOW CAN NRB HELP?

- **Advise and help the customer to implement compliant incident management.** NRB offers tailored services that meet this requirement.
- **24/7 system monitoring.** NRB offers an advanced monitoring system using state-of-the-art technology and ensuring proactive monitoring of all critical elements of the customer's infrastructure. This enables NRB to identify and respond quickly to potential threats.
- **Managing incidents quickly, efficiently and responsively.** NRB has clear procedures and dedicated incident management teams to detect, manage and notify the customer of ICT-related incidents. If an incident is detected, NRB's response protocols are triggered immediately to contain and resolve the problem with minimum impact on the customer.
- **Communicate transparently.** NRB is organised to communicate to the customer any incident likely to affect them, as well as the information the customer needs to comply with their obligations regarding the notification of major ICT-related incidents to the competent authorities.

3.3 DIGITAL OPERATIONAL RESILIENCE TESTING

DORA imposes an obligation on financial entities to establish and maintain a robust and comprehensive digital operational resilience testing program covering its critical or important functions, based among other things on threat-based penetration testing.

HOW CAN NRB HELP?

- **Have a solid continuity plan.** NRB's business continuity plan is organised and aligned with the ISO 22301 standard. The key elements are as follows:

  - **Crisis management policy**: NRB has developed precise procedures to ensure rapid and coordinated decision-making. NRB's policy provides for a coordinated response in the event of a crisis, including clear internal and external communications, escalation procedures and defined roles and responsibilities for each team member. In this way, NRB ensures that crises are managed calmly and effectively.
  - **Regularly tested continuity scenarios**: regular simulation exercises to ensure the effectiveness of NRB's plans and the adherence of its teams.
  - **Business Continuity Plan (BCP)**: NRB has developed a robust Business Continuity Plan (BCP), ensuring the uninterrupted availability of NRB's services, even in the event of a disaster or unexpected incident. The BCP includes rapid and effective recovery strategies, minimising potential interruptions. It includes technical disaster recovery plans (DRP).

- **Test systems on a regular basis.** NRB regularly carries out resilience tests to assess the ability of its systems to withstand and recover quickly from disruptions. The tests carried out by NRB include various simulations and scenarios. NRB also subcontracts blackbox, greybox and Red Teaming

intrusion tests on its shared environment to external companies (at least once a year). As part of its ISO27001 certification, NRB is also audited at least once a year.

→ **Assisting with the customer's penetration tests.** NRB allows its customers to carry out security tests on their assets hosted on NRB infrastructures, subject to compliance with strict rules to avoid any impact on the systems.

3.4 MANAGING THE RISKS ASSOCIATED WITH THIRD-PARTY ICT SERVICE PROVIDERS

3.4.1 DUE DILIGENCE

The key principles for good risk management in relation to third-party ICT service providers require financial entities, in accordance with the principle of proportionality, to carry out assessment processes of these providers before entering into a contractual agreement on the use of ICTs.

HOW CAN NRB HELP?

→ NRB's teams **are available** to the financial entity throughout the selection and evaluation process to respond quickly to any questions the financial entity may have, whether these concern NRB itself or the services it provides.
→ NRB pays particular attention to **risk management** in order, for example, to avoid conflicts of interest and to guarantee irreproachable ethics, as evidenced by NRB's ethics charter.
→ Where necessary and authorised in the contracts between NRB and its client, NRB may use subcontractors to carry out certain activities. Before concluding a contract with a subcontractor, NRB **checks the reliability of** the subcontractor and the services offered, as well as their suitability for the requirements of the customer and DORA.

3.4.2 ADAPTING CONTRACTS

Article 30 of DORA summarises the requirements that must be covered in the contractual agreements between the financial entity and its third-party ICT service provider.

HOW CAN NRB HELP?

→ **Offer customer contracts that are clear, appropriate and balanced.** NRB ensures that the contractual documents covering the ICT services it provides to the customer:

⇢ clearly set out the rights and obligations of the parties, taking into account the criticality and/or importance of the services;
⇢ cover the elements required by article 30 of the DORA regulation and by the technical regulation standards (RTS) in force.

NRB's model contract with clauses adapted to DORA is available on request.

- **Ensuring security and continuity in the subcontracting chain.** NRB takes particular care to ensure that the contracts it concludes with its subcontractors take into account DORA requirements applicable to them.

3.4.3 INFORMATION REGISTERS

Establishing and updating the information register requires financial entities to have certain information about their third-party ICT service providers and their subcontractors.

HOW CAN NRB HELP?

- **Identify subcontractors.** Authorised subcontractors are identified in the contract between NRB and its client and/or in the data processing agreement (DPA), where applicable.
- **Be available and transparent.** NRB is available to provide the information the customer needs to maintain and update the information register regarding NRB and its subcontracting chain. To this end, certain administrative information concerning NRB and its parent company is provided in section 4.

3.5 SHARING INFORMATION

DORA includes provisions for the exchange of information and intelligence on cyber threats between financial entities, as well as the conditions and modalities for participation in these exchanges, in particular by third-party ICT service providers.

HOW CAN NRB HELP?

- **Communicate transparently**. Wherever possible, NRB facilitates the sharing of critical information while complying with applicable standards. NRB can help its customers adopt a proactive and collaborative approach to cyber security.
- **Communicate securely.** NRB uses communication channels and information transfer methods that comply with the highest security standards to protect the data of all stakeholders.

4. Administrative information

4.1 ABOUT NRB SA

Network Research Belgium. Company number: BE0430.502.430

Registered office: Parc Industriel des Hauts-Sarts, 2nd Avenue, 65 4040 Herstal, Belgium

4.2 ABOUT ITS PARENT COMPANY

Ethias SA. Company number: BE0404.484.654. Head office in Liège, Belgium.

4.3 CONTACT

Any questions regarding this White Paper can be addressed to risk@nrb.be