NRB
DARING TO COMMIT

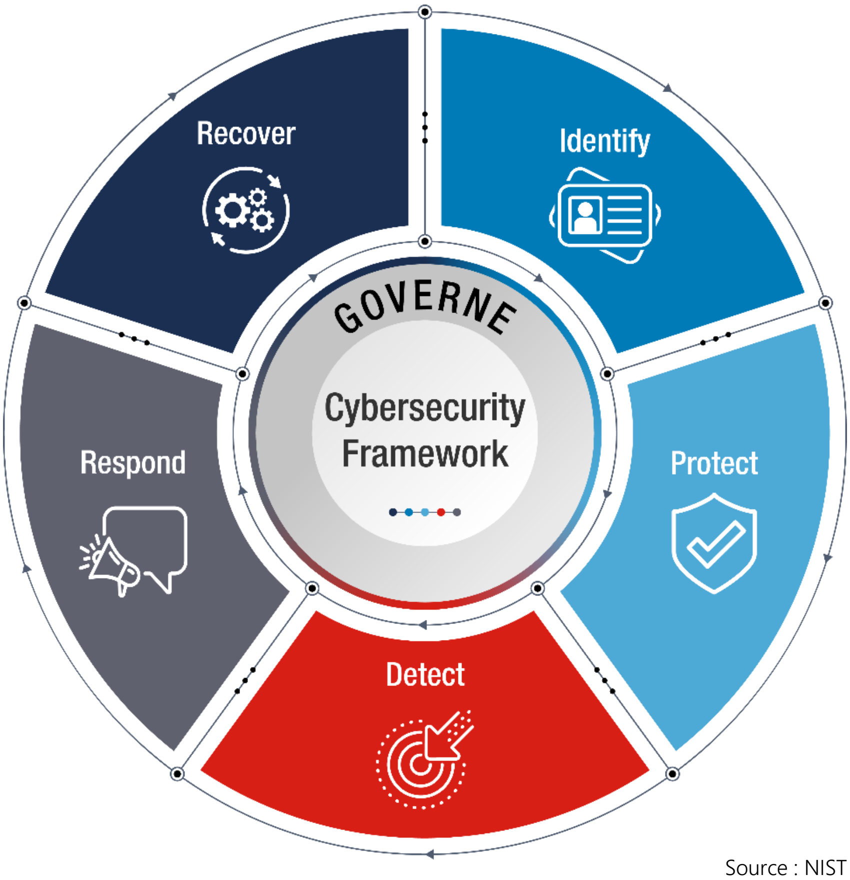
CYBERSECURITY POLICY

SECURITY IS A PRIORITY AT NRB!

NRB hosts and supports the IT systems of key organisations at the European level, whether in the public, private or healthcare sectors. We therefore have a crucial responsibility to ensure the continuity and quality of our services. The security of information systems and data is naturally one of the top priorities in the provision of our services and the protection of our infrastructures.

HOW IS NRB HELPING TO PROTECT ITS CUSTOMERS AGAINST CYBER THREATS?

- Thanks to the confidence reinforced by ISO27001 certification, awarded by an independent audit company, which attests to the integration of security into the organisation and the implementation of measures designed to maintain the confidentiality, integrity and availability of data.
- By using a framework covering all aspects of security, which enables NRB to respond to current and future threats.



Source : NIST

THIS FRAMEWORK IS BASED ON SIX FUNCTIONS THAT ORGANISE CYBERSECURITY ACTIVITIES:

Govern: Identify what NRB can do to achieve and prioritise the outcomes of the other five functions in the context of its mission and the expectations of its stakeholders.

Identify: Develop an understanding of the organisation's assets, its suppliers and the associated cybersecurity risks. Identify opportunities for improvement that support cybersecurity risk management.

Protect: Develop and implement appropriate countermeasures to prevent or reduce the likelihood and impact of negative cybersecurity events on critical assets and services.

Detect: Develop and implement activities to discover and analyse anomalies, indicators of compromise and other potentially adverse events that may indicate that cybersecurity attacks and incidents are underway.

Respond: Develop and implement appropriate activities to contain the effects of cybersecurity incidents.

Recover: Develop and implement appropriate activities to support the rapid restoration of normal operations in order to reduce the effects of cybersecurity incidents, and to enable appropriate communication during recovery efforts.

IN PRACTICE, HOW IS THIS FRAMEWORK IMPLEMENTED AT NRB?

FUNCTION	OBJECTIVES AND ACTIVITIES
Govern	→ Security governance structured around 3 lines of defence has been implemented. → A cybersecurity strategy is defined, aligned with organisational objectives and taking account of risks and regulations. → NRB's activities comply with the GDPR*, the NIS2* directive and the ISO27001 standard. → Cybersecurity policies and procedures are regularly reviewed to keep pace with changing threats and regulatory requirements. → The performance of security measures is regularly monitored and assessed by reporting corporate KPIs to the Executive Committee. → A culture of cybersecurity is promoted and encouraged, so that all employees recognise their role in protecting digital assets.
Identify	→ NRB has a risk management process with its own methodology, inspired by the ISO27005 standard, as well as recurring analyses and action plans. → NRB identifies and maintains an inventory of all assets (devices, systems, data) in a centralised database, including their level of importance in the information system. → NRB inventories the relationships between the various systems in a CMDB to provide a global view of dependencies and potential impacts on systems. → Based on the information provided by the customer, NRB integrates the customer's critical services and assets into its processes. → NRB assesses the cybersecurity risks associated with partners, suppliers and other third parties, and puts in place measures to manage them. → Together with the customer, NRB defines the organisation and communication channels with regard to security. → NRB carries out regular Pentests (at least once a year) to assess the level of maturity of its protection and detection processes.

Protect	→ NRB's datacenters have been designed and operate to ensure security and continuity (level equivalent to Tier 3+ Uptime Institute). → Data storage is secure, with strong encryption in particular. → Data is backed up and the integrity of the backups is checked. → Critical data is backed up using immutable backups. → Business continuity and disaster recovery plans are in place and tested at least annually. → Hardening and patching are ensured through our vulnerability management process. → Systems are protected by firewalls and anti-malware (XDR) which send alerts to our SIEM/SOC. → Rigorous, automated identity management via our IAM tool and rigorous access control, including multi-factor authentication, are put in place to restrict staff access to only the systems and information they need. → All NRB employees receive ongoing, tailored security training on an e-learning platform.
Detect	→ NRB's network and systems are constantly monitored and any abnormal behaviour in relation to the defined baseline generates an alert. → End-user activities are monitored to detect abnormal access attempts. → Security events are collected and correlated by our Security Information and Event Management tool. → Security events and alerts are analysed 24/7 by our Security Operation Centre. → Technical audits are carried out on a regular basis to identify potential weaknesses. → Constant monitoring is carried out to identify new threats and incorporate them into our tools and processes.
Respond	→ NRB has put in place incident management and crisis management processes to deal with cyber incidents effectively and ensure continuity of services. → Communication protocols are in place to inform internal and external stakeholders in a timely manner before, during and after an incident. → Incidents are analysed and categorised in order to execute predefined action plans. → Incidents are contained and mitigated to limit their impact. → The NRB CSIRT (Computer Security Incident Response Team) carries out the necessary forensic investigations and analyses, in collaboration with specialized external service providers where necessary. → For each major incident, a post-mortem analysis is carried out to identify lessons learned and update response processes and strategies accordingly. → NRB works with partners (Cert.be, CCB, MSSP) to exchange information on threats and incidents.
Recover	→ Recovery plans are executed to restore critical services, systems and operations after a cybersecurity incident. → Priorities are set for restoring essential functions and operational capabilities in order to minimise service interruptions. → Relationships with internal and external parties are maintained throughout the recovery process to ensure transparency and trust. → After resolution and recovery, incidents and actions taken are analysed to improve management processes and action plans.

*GDPR (General Data Protection Regulation): The aim of the GDPR is to provide a framework for practices relating to the collection, processing and use of personal data.

*NIS2 (Network and Information system Security): The NIS2 Directive is a regulatory framework designed to strengthen the resilience of critical infrastructures, improve response to cyber incidents and harmonize cybersecurity practices across EU member states.