EIMSKIP GROUP

INFORMATION SECURITY MANAGEMENT POLICY

EIMSKIP

Eimskip is a leading transportation company in the North Atlantic providing container and reefer liner services with connections to international markets and is specialized in worldwide freight forwarding services with a focus on frozen and chilled commodities.

OVERVIEW

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

EIMSKIP´S VALUES

INTRODUCTION

FRAMEWORK

- Identify
- Protect
- Detect
- Respond
- Recover

RESPONSIBILITY

REVIEW

OUR VALUES

ACHIEVEMENT

We simplify things for our customers. That’s how we achieve our goals.

PROGRESSIVE
– we’re always thinking ahead, we are ambitious, driven by initiative and eager to create new ideas and implement innovative solutions.

PASSIONATE
– we inspire others with our drive for excellence. We celebrate the big and small wins and aim for success.

COOPERATION

We offer outstanding solutions and services. We do that through cooperation.

TEAMWORK
– we believe our continued success and great achievements are only possible with teamwork and colla- boration.

POSITIVE
– we have fun and smile, we enjoy our work, we celebrate successes, and we´re team players.

TRUST

We show responsibility towards customers, shareholders, society, and the environment. That’s how we earn trust.

RESPONSIBLE
- we’re caring. We work for a better society, preserve and protect the environment and strive to be a role models when it comes to responsibility and trust.

ACCOMPLISHED
- we connect the world. We make the trip safe, we provide excellent service – and we have been doing it for over 100 years.

INTRODUCTION

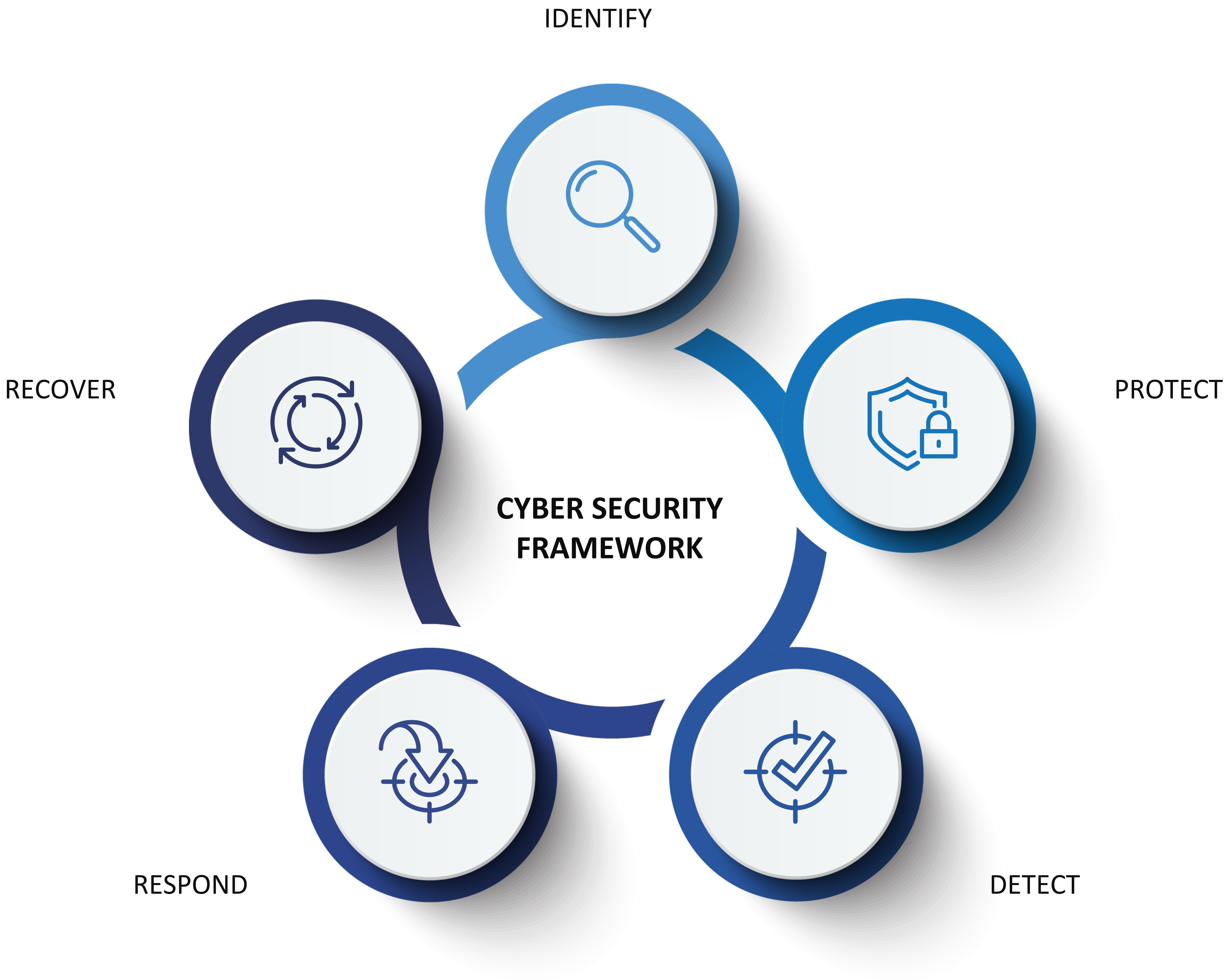
EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

This information security policy revolves around the cyber security framework: Identity – Protect – Detect – Respond – Recover. These five concepts focus on the organization’s efforts to manage information security risks.

The purpose of this policy is to support the mission and goals of Eimskip. To achieve that purpose, information security needs to be managed to an acceptable level.

CYBER SECURITY FRAMEWORK

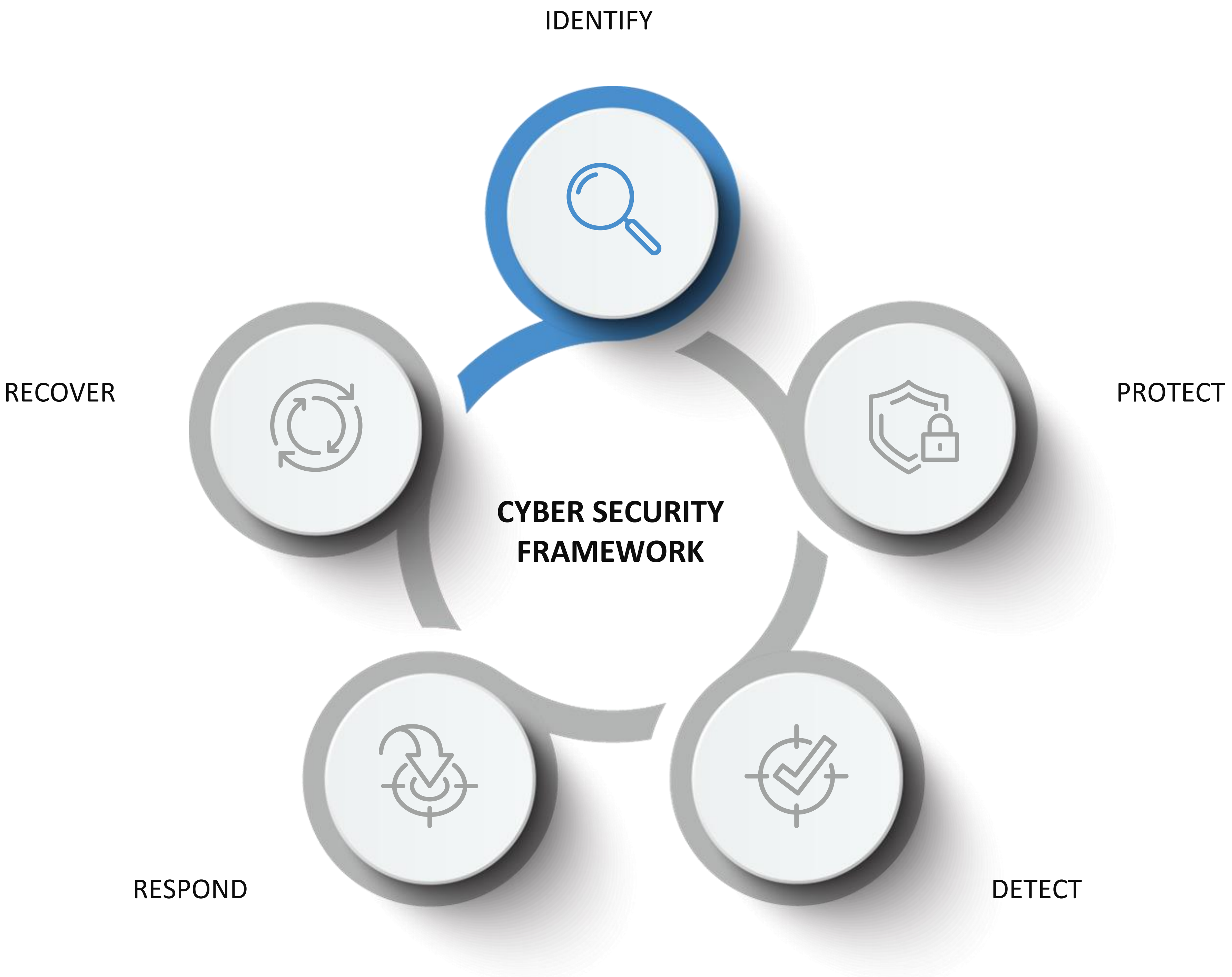
EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY



IDENTIFY

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

- Risks are identified and assessed on a regular basis, risk treatment plans are produced and supported by management. The risk assessment methodology is according to international standards, sector-specific guidance, and best practices.
- All systems and information have been identified and classified in accordance with the needs and purpose of the organization.
- Critical systems and necessary supporting functions have been identified.
- All laws and contractual and regulatory requirements are identified, defined, and met.
- Vendor risk is identified and managed by the organization. Clear guidelines and frameworks are in place to determine important vendors, and internal audits are performed to evaluate vendors as required and necessary.
- Threat actors and scenarios that have the possibility to cause disruptions to operational or information security have been identified and defined. Threats to cyber-security, including international or regional instabilities, are monitored and addressed in accordance with the likelihood of causing harm.

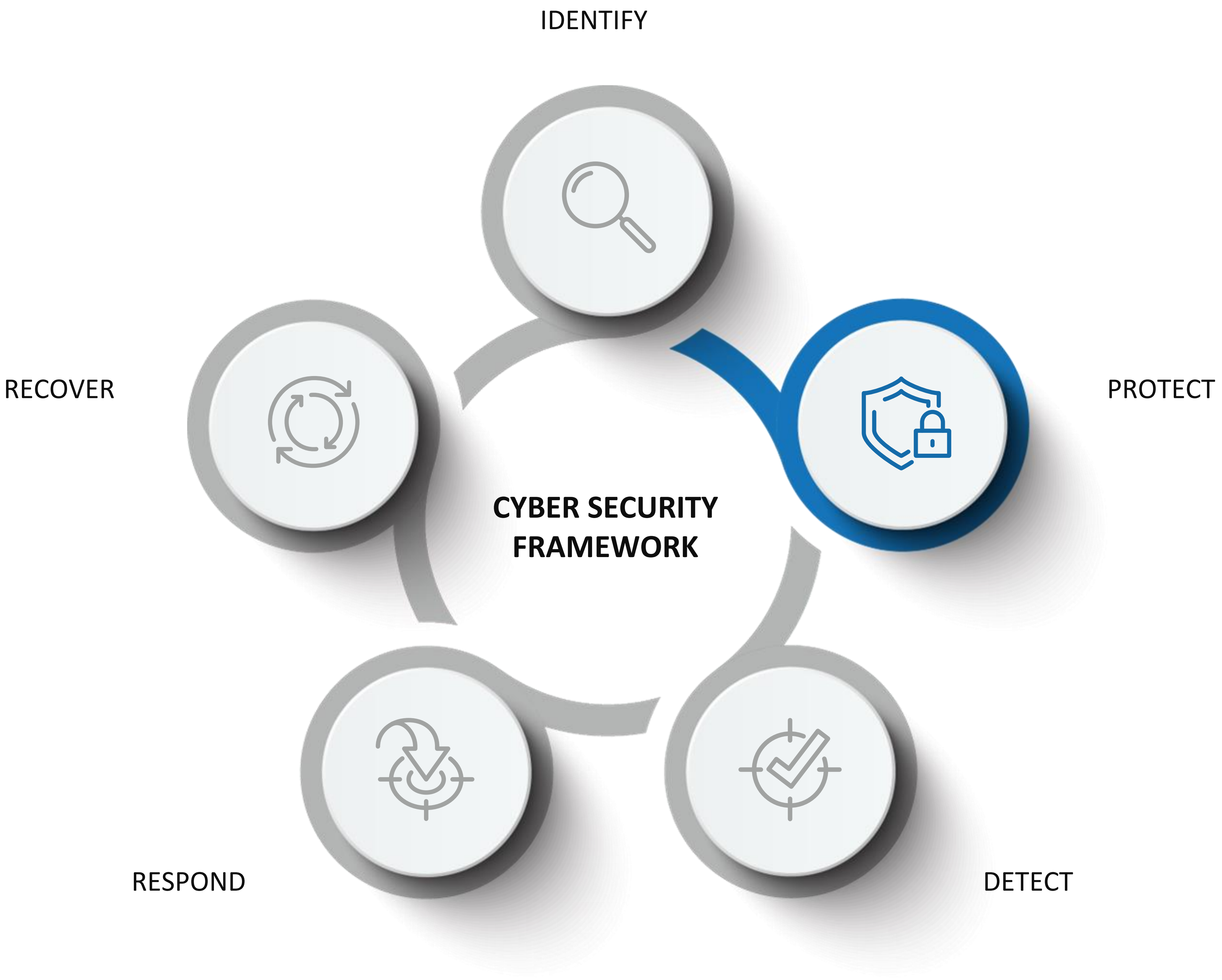


PROTECT

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

Access is limited to be as required and in accordance with the needs of the user and possible risks to systems and information security.

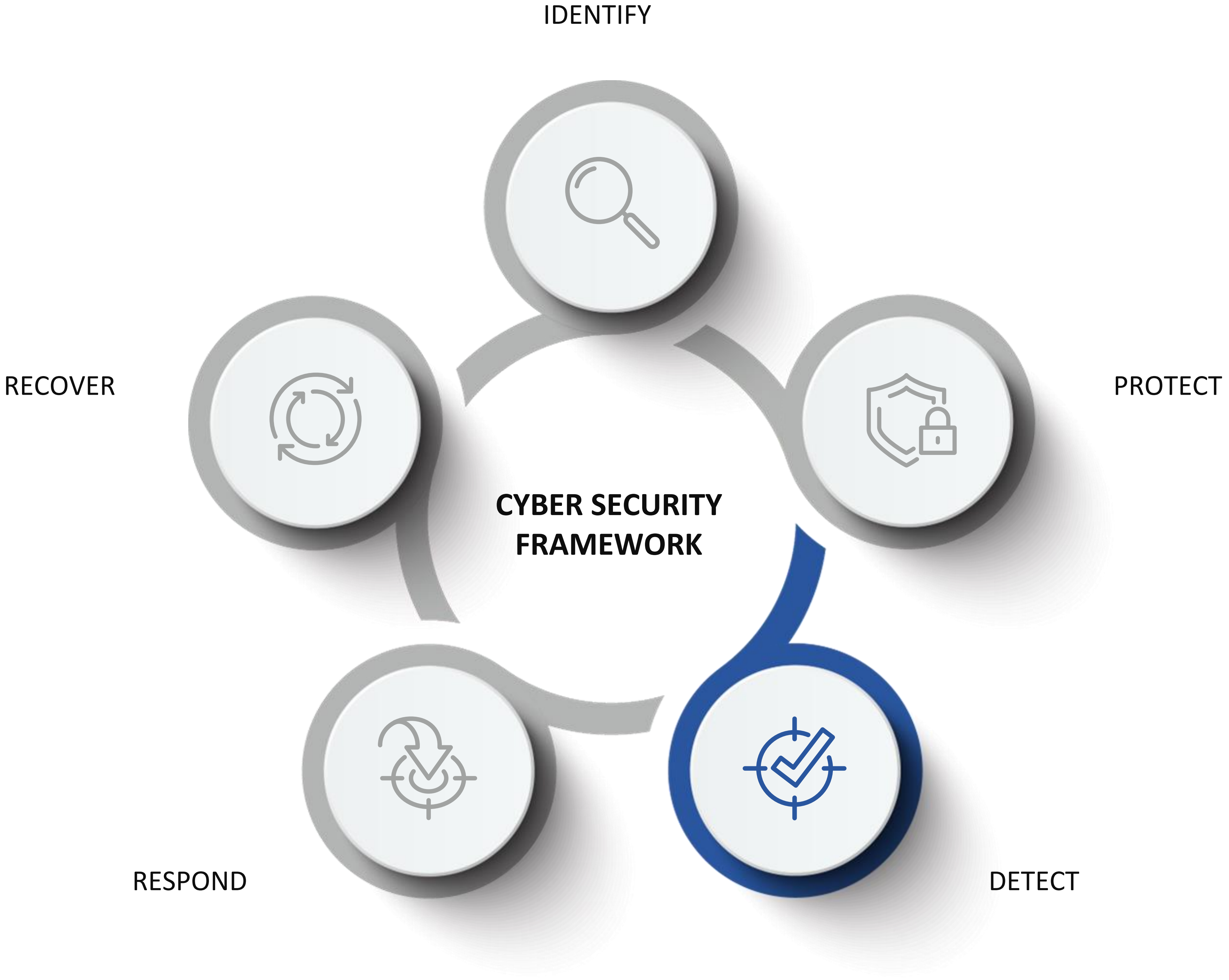
- Additional requirements are made to access points open to the internet. Multi-factor authentication is implemented where possible.
- These limitations also apply to all physical locations run by Eimskip, including any server rooms or other areas holding technical equipment.
- Access rights are reviewed by the relevant system owner in relation to possible risks and the importance of the relevant information system or location.
- All relevant changes to information systems and data are managed by the organization, irrelevant of whether the change is performed by internal or external actors.
- Controls from international standards, sector-specific guidance, and best practices are implemented to mitigate possible cyber-risks and minimize disruptions to critical systems.
- Necessary information and awareness of this policy are provided to all stakeholders.



DETECT

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

- Eimskip actively scans and searches for vulnerabilities in internal and external systems.
- Patches and settings of equipment are according to best practices to limit the possible risks from insecure systems.
- Internal audits are performed on a regular basis. The purpose of internal audits is to determine if the organization’s rules are followed and locate areas for improvement.
- Measurements to monitor the performance of information security matters have been determined. Possible and active risks are monitored for possible escalation or alterations. Key risk indicators have been determined.

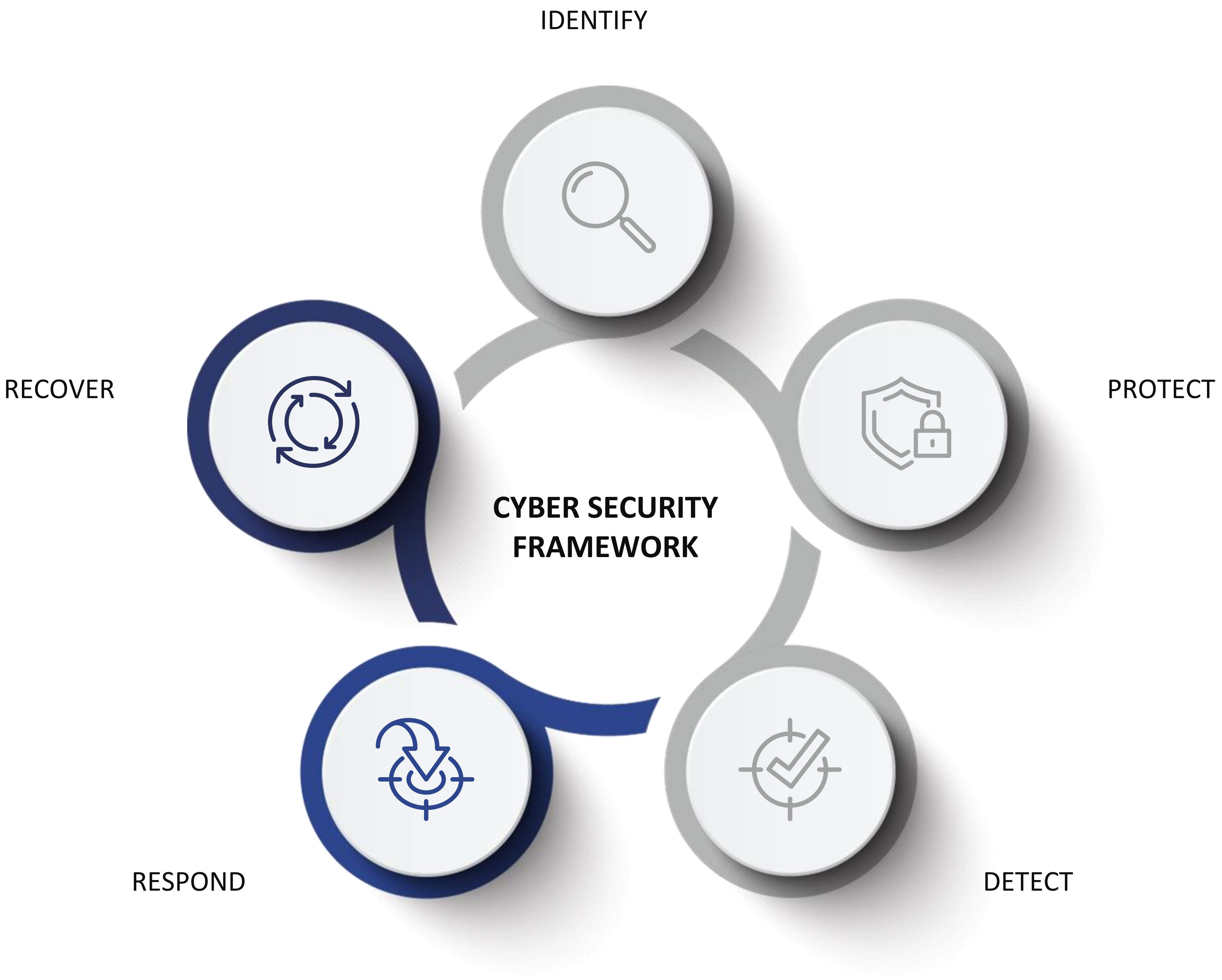


RESPONSE & RECOVER

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

- Incidents are recorded and reviewed, either from automated or manual sources. Incidents can be an important indication of areas where further inspection or audits are needed.
- Responses to incidents are documented as needed to reduce the likelihood of recurrence and limit the possible impact.
- Information is backed up as necessary to ensure a quick recovery in the case of adverse conditions. Recovery time objectives have been determined by relevant system owners.
- Disaster recovery response procedures have been identified and tested. Procedures for business continuity have been determined for various possible events.
- Required supporting utilities for business continuity have been defined. Tests are performed regularly to ensure that all necessary utilities and plans perform as expected during a possible disaster scenario.

We will always strive for continuous improvements to information security and systems.



RESPONSIBILITY

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

- It is the responsibility of all employees to follow the procedures delivered by this policy and the rules set to ensure information security within the organization.
- External actors and other relevant stakeholders need to follow this policy and other rules as applicable.
- It is the responsibility of the Eimskip Executive Team to approve this policy and to ensure that all employees follow the policy.
- It is the responsibility of the information technology department within Eimskip to execute this policy in collaboration with the Executive Team and other managers.

REVIEW

EIMSKIP GROUP – INFORMATION SECURITY MANAGEMENT POLICY

The policy is approved by the Executive Team.
CIO will initiate a review of this policy every two years. The policy is published on the internal Eimskip Policy Portal.

Approved by the Executive Team of Eimskipafélag Íslands
hf. Reykjavík, 30.8. 2022.

EIMSKIP