careium

IT Assurance Statement

Financial year 2024

Subject: Compliance with Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector

Issued by: Careium AB

Purpose: Careium is not a financial entity as defined in Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector and is therefore not required to comply with the Regulation. However, as a third-party supplier to financial entities Careium acknowledges that we need to maintain robust and resilient digital operational environments to prevent, mitigate, and recover from information and communication technology (ICT) related disruptions.

1. Governance and Oversight of ICT Risk

Careium has established a robust governance framework to manage ICT risk. Specifically:

- **ICT Risk Management Framework:** An ICT risk management framework has been adopted and integrated into our overall risk management system, as approved by group management. This framework identifies, assesses, and mitigates risks associated with information and communication technologies.
- **Roles and Responsibilities:** All risks have an owner that is responsible for the risk and reviews the risk at least annually. The highest risks are reviewed by the steering group for information security quarterly. Top risks are reviewed by group management and board of directors at least annually.
- **Policies and Procedures:** Comprehensive ICT policies, including incident response, monitoring, and recovery protocols, are documented, implemented, and regularly updated.

2. ICT Risk Management and Controls

Careium employs the following:

- **Identification and Protection:** Critical ICT systems and assets are identified and prioritized. Security measures, including encryption, firewalls, and multifactor authentication, protect these assets from cyber threats.
- **Monitoring:** Continuous monitoring tools and processes are in place to detect, respond to, and report ICT anomalies or incidents promptly for all mission-critical and customer facing systems.

- **Third-Party Risk Management:** Contracts with ICT third-party providers include robust service-level agreements (SLAs) and provisions for audit and termination rights. Continuous oversight of third-party service providers ensures compliance with Careium requirements.

3. ICT Incident Reporting and Response

Careium has implemented an ICT incident management process that includes:

- **Detection and Reporting:** A mechanism for detecting and reporting significant ICT incidents to relevant authorities, including incidents that could disrupt critical operations.
- **Incident Escalation Protocol:** An escalation procedure is in place to ensure that critical incidents are addressed and resolved promptly.
- **Record-Keeping:** A repository for recording ICT-related incidents, including their root causes, impacts, and mitigation measures.

4. Digital Operational Resilience Testing

Careium conducts regular digital operational resilience testing:

- **Testing Schedule:** Regular penetration testing and vulnerability assessments are performed on critical ICT systems.
- **Review of Results:** Findings from testing exercises are reviewed, and remediation measures are implemented and documented.

5. Information Sharing

Careium participates in information-sharing arrangements, ensuring that:

- Relevant information on ICT threats, vulnerabilities, and incidents is exchanged with customers and suppliers, according to contracts.
- Confidentiality and data protection requirements are strictly adhered to when sharing information.

6. Oversight of Critical ICT Third-Party Providers

Careium ensures:

- Continuous oversight and risk assessment of critical ICT third-party providers.
- Maintenance of exit strategies and contingency plans for ICT third-party dependencies to safeguard mission-critical continuity.

7. Compliance and Audit

Careium has established an internal audit function that evaluates the effectiveness of ICT risk management frameworks, policies, and controls, ensuring alignment with legal requirements and ISO 27001. Audit findings are reported to the relevant manager, and corrective actions are tracked.

External audits are done annually by DNV to maintain the ISO 27001 certification.

8. Declaration

We affirm that Careium has implemented the measures above. Our commitment to continuous improvement, as stated in our information security policy, ensures that our digital operational resilience capabilities remain robust, effective, and in line with evolving regulatory requirements.

This statement will be reviewed and updated annually.

Authorized Signatory:
Malmö 2025-01-02

Oskar Hägglund, CIO