Oberbank

Version 1 / 24.08.2026

Informationssicherheitsmanagementsystem (ISMS) der Oberbank

1 Informationssicherheit

Informations- und Cyber Security hat für die Oberbank hohe Priorität.

Die Daten unserer Kund:innen, Geschäftspartner und Mitarbeiter:innen werden mit höchster Sorgfalt behandelt und gesichert. Ein wesentliches Ziel der Oberbank ist es einen angemessenen Schutz jeglicher Informationen und Daten durch ein Informationssicherheitsmanagementsystem (ISMS) zu gewährleisten. Folgende Sicherheitsziele hat Oberbank definiert, um dies zu erreichen:

- Gewährleistung von Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität und Rechtsmäßigkeit für Informationen und Daten
- Aufbau und kontinuierliche Stärkung einer gelebten Sicherheitskultur durch verpflichtende, rollenbasierte Trainings und Sensibilisierungsmaßnahmen.
- Aufrechterhaltung eines branchenüblichen Sicherheitsniveaus im Einklang mit anerkannten Standards.
- Sämtliche IKT-Risiken dauerhaft innerhalb des festgelegten IKT-Risikotoleranzniveaus halten und wirksam steuern.
- Aufrechterhaltung von resilienten IKT-Dienstleistungen durch entsprechendes IKT-Dienstleistermanagement, insbesondere für wesentliche IKT-Dienstleister.
- Einhaltung gesetzlicher Vorgaben und Meldeverpflichtungen im Bereich Informationssicherheit.

Das ISMS der Oberbank ist konsequent an allen relevanten gesetzlichen, regulatorischen und internen Anforderungen ausgerichtet. Es schafft einen verbindlichen Rahmen, um Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten und durch geeignete technische sowie organisatorische Maßnahmen zu steuern. Das ISMS ist damit ein zentraler und unverzichtbarer Bestandteil der Informationssicherheit innerhalb der Oberbank.

2 Governance und Rollen

Die Informationssicherheit wird gemäß dem Model der drei Verteidigungslinien implementiert, um das Prinzip der Funktionstrennung zu gewährleisten.

Die Sicherheitsvorgaben und - Dokumente für das Institut liegen vor und werden regelmäßig auf Aktualität überprüft. Diese definieren die organisatorischen und technischen An forderungen zur Informationssicherheit, die Ziele, Prinzipien als auch die notwendigen Rollen bzw. Verantwortlichkeiten oder der Umgang mit externen Anforderungen zur Informationssicherheit definiert.

3 Strategie

Oberbank gestaltet ihr ISMS nach regulatorischen Anforderungen, insbesondere der DORA-Verordnung (Digital Operational Resilience Act, EU-Verordnung 2022/2554). Wesentliche Elemente zu Steuerung der Informationssisherheit umfasst die Strategie zu Informationssicherheit und zur digitalen operationalen Resilienz, die international anerkannte Sicherheitsstandards und Sicherheitsgrundsätze berücksichtigt.

4 IKT-Risikomanagement

Das IKT-Risikomanagement zu Risikoermittlung, Risikobewertung und Risikobehandlung der IKT-Risiken wird angewendet, Es berücksichtigt sowohl strategische als auch operative Risiken und umfasst interne wie externe Einflussfaktoren und ist in das unternehmensweite Risikomanagement der Oberbank integriert.

5 IKT-Vorfälle

Zur Gewährleistung einer effektiven Behandlung von IKT-Sicherheitsvorfällen hat die Oberbank entsprechende Incident-Management Prozesse definiert. Diese umfassen klare Rollen, Melde- und Eskalationswege, Incident Response Pläne, die Bewertung von Ereignissen, strukturierte Reaktions- und Wiederherstellungsmaßnahmen, Beweissicherung, sowie Lessons Learned. Alle Aktivitäten werden nachweislich dokumentiert, überwacht und im Rahmen des ISMS kontinuierlich verbessert.

6 Krisenmanagement

Krisen- und Notfallpläne zu unterschiedlichen Szenarien im Rahmen des im Unternehmen etablierten Business Continuity Managements sind in der Oberbank etabliert.

7 Testing

Die Oberbank führt tourlich risikobasierte Tests zur Sicherstellung und Überprüfung der digitalen operationalen Resilienz durch. Entsprechende Planung, Steuerung und Dokumentation sind eingerichtet.

8 Berichtswesen

Die Berichtserstattung zu den Themen Informationssicherheit und digitale operationale Resilienz erfolgt regelmäßig an den Vorstand und wird anlassbezogen auch dem Aufsichtsrat zur Kenntnis gebracht.

9 Kontinuierliche Verbesserung

Das ISMS der Oberbank unterliegt einem kontinuierlichen Verbesserungsprozess und wird regelmäßig auf seine Wirksamkeit überprüft. Wesentliche Aktivitäten und Ergebnisse in Bezug auf die Informationssicherheit werden identifiziert, bewertet, Maßnahmen abgeleitet und überwacht, in Kennzahlen dargestellt. Das ISMS wird regelmäßig auf seine Wirksamkeit überprüft und der jeweilige Reifegrad ermittelt.

10 Schulung und Awareness

Zur Förderung des Sicherheitsbewusstseins der Mitarbeiter:innen führt die Oberbank ein zielgerichtetes Programm zur Bewusstseinsbildung und Schulung durch. Die Mitarbeiter:innen müssen regelmäßig verpflichtende webbasierte Trainings absolvieren.