Security Management at OP Financial Group

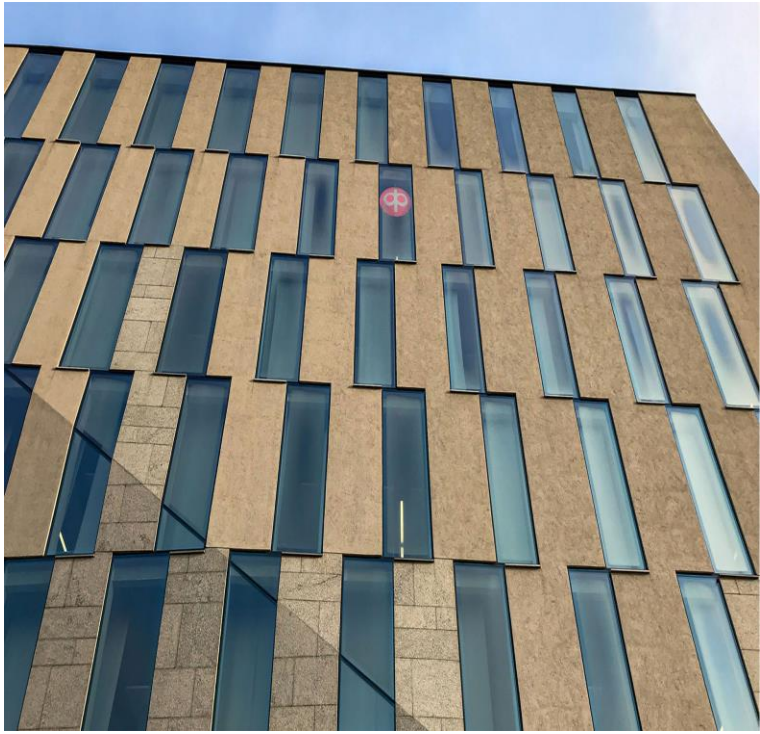
OP Financial Group

Content

1. Management of corporate security
2. Corporate security governance model
3. Information security governance model
4. Security organization
5. Security risk management
6. Security governance and policies
7. Security culture and competence development
8. Personnel security
9. Premises and operational security
10. Information and data security
11. Identity and access rights management
12. Application security
13. Infrastructure security
14. Third party and cloud services security
15. Detecting cyber threats
16. Business continuity and recovery management

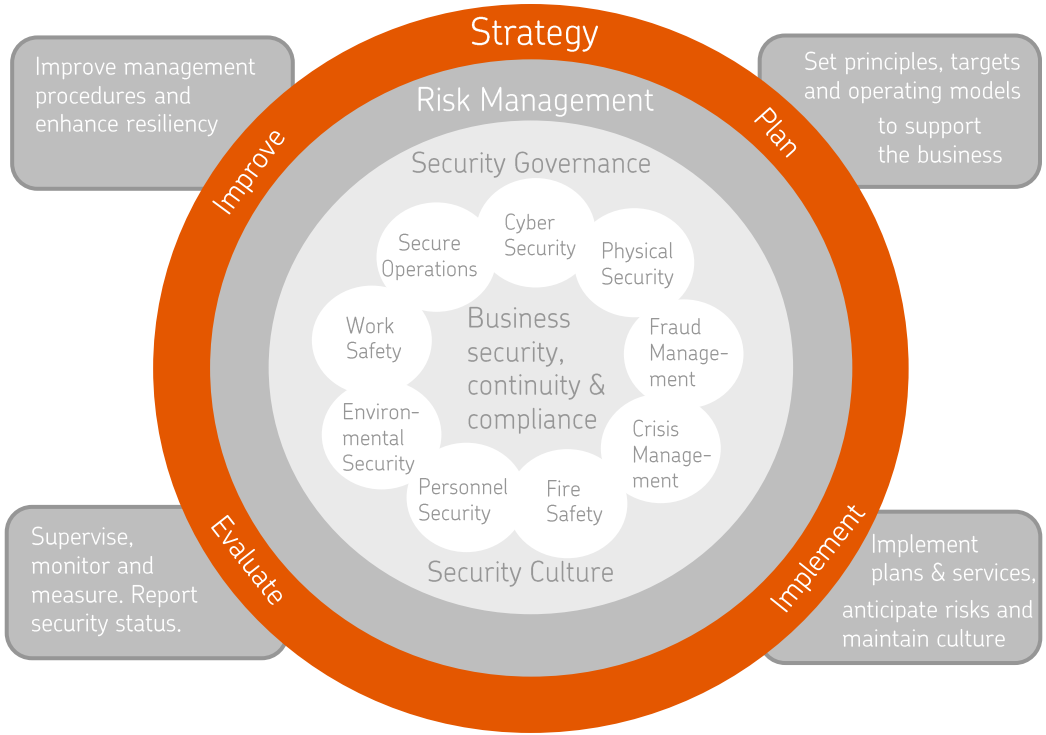
1. Management of corporate security

- Corporate security concerns the security of all operations within a company. Corporate security is a way of securing the company's business goals, operational continuity, the wellbeing and safety of employees, the company's assets, data we control, and our reputation.
- Management of corporate security at OP is based on respect for the Group's values and good business practices, while highlighting our goal of being worthy of our owners' and customers' trust. Corporate security management is an integral part of company management. Security management assists business management by identifying and managing security risks posing a threat to business. As such, it must be systematic and goal-based, and its impact must be monitored.
- Security management's development is based on the Group's strategic targets and goals, business and customer requirements, and requirements set by legislation and OP's key principles and policies.



2. Corporate security governance model

- Steering of the security management procedures is based on a continuous development model:
  - Plan - Identify the values to be protected, the compliance requirements and risks. Establish operating models and set targets.
  - Implement- Implement the protection systematically, maintain a security-aware culture and detect and resolve violations.
  - Evaluate - monitor the efficiency of the procedures and create a situational overview.
  - Improve – improve the procedures and enhance corporate resilience.



OP Financial Group

3. Information security governance model

- The OP information security governance model covers all sub-areas of information security and fosters continuous improvement. The sub-areas of the governance model are divided into four upper-level categories:
  - Govern – Ensure that the necessary strategy, structures, policies, procedures and practises are in place to maintain and enhance security capabilities
  - Protect – Proactive protection against cyber incidents by developing, implementing, and enhancing the controls related to users, data, infrastructure and applications
  - Detect – Ability to discover internal and external threats by leveraging threat intelligence, and proactively mitigating them, or minimizing any adverse impacts to the organization.
  - React – Support business resilience through incident management capabilities and exercised recovery procedures.

4. Security organization

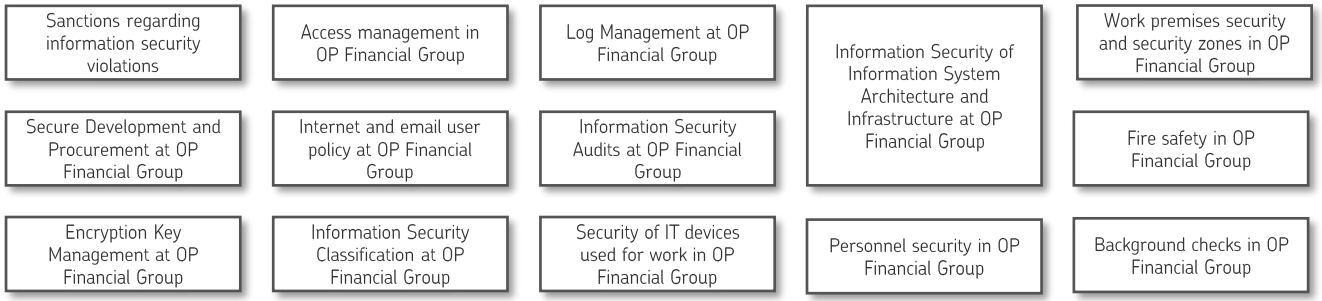
- Corporate security is centrally organized in OP Financial group and is lead by our Chief Security Officer (CSO). The CSO reports to the Chief Risk Officer (CRO) that is part of OP's executive board.
- Information security is centrally organized in OP Financial group and is lead by our Chief Information Security Officer (CISO). The CISO reports to the Chief Information Officer (CIO) that is part of OP's executive board. A board level information security committee headed by the CIO meets regularly.
- OP has a broad range of dedicated security specialists supporting the group in all security matters e.g., personnel security, physical security, cyber security governance, risk management, testing and auditing, security and privacy champions, incident response, certificate and key management, architects and product owners.

5. Security risk management

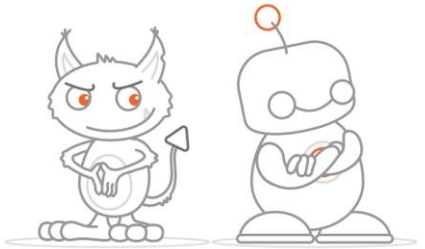
- OP Financial Group's risk management and regulatory procedures are built around the principle of three lines of defence. The first line of defence comprises business lines, the second line of defence comprises the assuring risk management and compliance functions independent of the business lines/divisions, and the third line of defence comprises Internal Audit. Each line of defence has its own role in performing the risk management process efficiently.
- The business units fulfilling OP Financial Group's strategy, are responsible for planning their own operations, and their efficient and effective implementation, and for their internal control. Only the unit concerned makes business decisions and is expressly responsible for the quality of its customer service, its business continuity as well as its earnings and risks.
- The second line of defence has prepared risk management frameworks within the limits of which the first line of defence implements risk-taking and risk management related to its daily business. The second line of defence is required to support the first line of defence by consulting them especially in matters that are part of their own expertise (e.g. cyber security, privacy). The second line of defence also oversees compliance with the guidance frameworks and carries out an independent analysis related to the balance between earnings, risks and capital and liquidity acting as buffers as well as ensuring business continuity during incidents.
- Internal Audit that is independent of other lines of defence and acts as the third line of defence.

6. Security governance and policies

- OP Financial group has a three-level policy structure. On the highest level are the ”Corporate Security principles” that are approved by the Board of Directors.
- To secure the principles, the security procedures are defined in ”Security Management Procedures” that are approved by an executive management committee.
- The procedures are then described in more detail in the level 3 policies that are approved by the Chief Information Security Officer (CISO) or Chief Security Officer (CSO):



7. Security culture and competence development



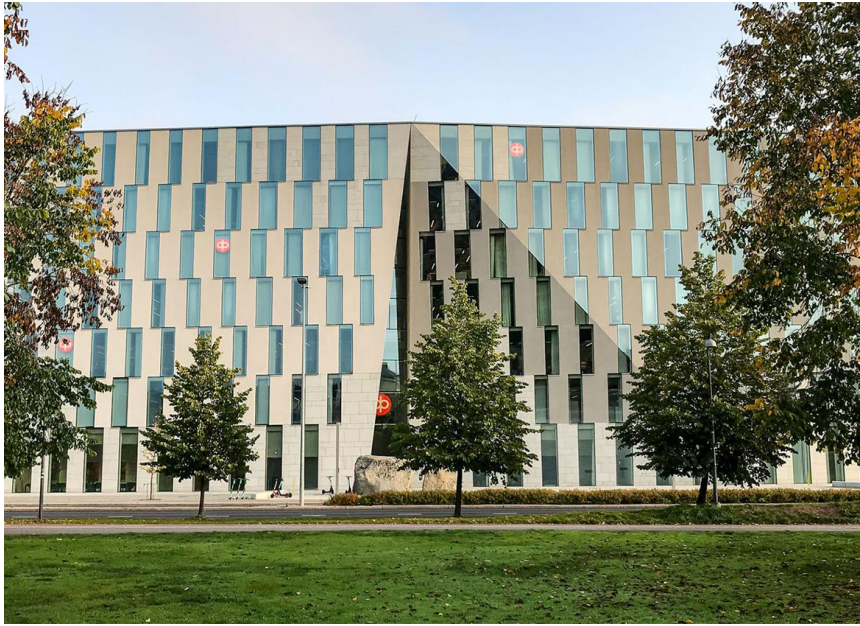
- Knowledge and training are used to maintain the security competences of OP's employees and external workers. Supervisors are responsible for documenting any orientation provided and monitoring the related training. Competence development is multichannel, as follows:
  - Competences are based on the online security courses available on OP's training platform. Some online courses are mandatory for all staff, while others are for people in certain roles. Competences must also be maintained: for example, mandatory information security training and courses on threatening situations must be completed annually.
  - An OP Introduction Day is arranged by HR for new employees, to explain the key safety and security regulations governing daily work.
  - Awareness is maintained and fostered using Cyber Security's information security awareness programme.
  - Training in the detection and reporting of social manipulation and suspicious emails is provided through anti-phishing exercises, training messages, and micro courses in addition to daily work.

8. Personnel security

- Trust and responsibility are the foundations of our activities in the financial sector. At OP, the trustworthiness of managers, employees and external workforce are ensured by background checks during recruitment or procurement. Background checks can also be performed if the person's role changes during the employment relationship. The scope of a background check depends on the task performed and the related authorisations.
- In addition to a background check, every person working at or for OP must sign a non-disclosure agreement and an information security and data protection agreement.

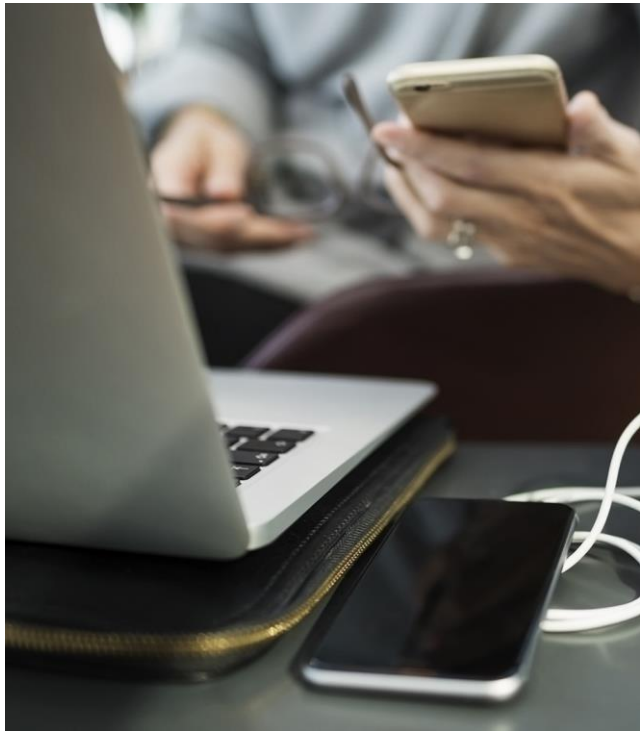
9. Premises and operational security

- Operational security at OP is supported by guidelines, security services and a range of structural and technical security solutions. These measures are used to protect staff and customers, property and information from external threats.
- Premises are divided into security zones, on which security measures are based.
- Rescue procedures involve the prevention of fires and other accidents, and the use of fast and correct procedures in reaction to an accident. OP's organisations must independently prepare for hazardous situations and ensure that their buildings are maintained in a way that minimises the risk of accidents and hazardous situations.



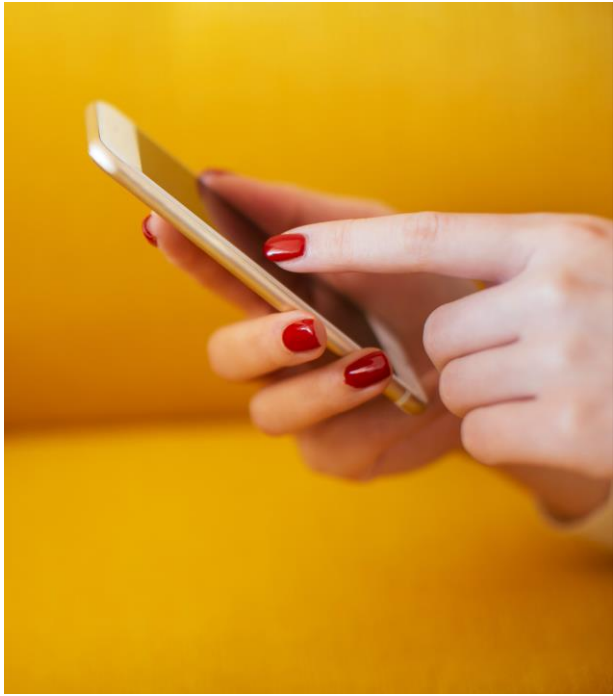
10. Information and data security

- All data created at or brought into OP Financial Group must be classified, secured and processed in the manner required by OP's Information Security Classification. This applies to all data processed within OP, regardless of the format (such as physical, electronic, digital and spoken communication).
- OP has a Data Loss Prevention (DLP) system used to detect insufficient limitation of access rights and inappropriately located data on OP's network. The DLP system enables processing of confidential data and is used in a limited way, compliant with Finnish legislation, in areas such as data protection and communications.
- The security policies states the requirements regarding encryption of data, encryption keys and certificate management, which OP and its partners must follow regarding stored data and data communications.
- In addition to the security classification and secure processing of data, the data life cycle concerns different statutory times (minimum and maximum) set for data storage and the proper erasure of data when the storage time ends.



11. Identity and access rights management

- Employment, agency workforce and consultants' contractual data maintained by HR management forms the basis of the centralised identity management. Information system access rights are therefore integral to life cycle management in such a manner that changes in an employment relationship are appropriately registered in the information system's user information. No one without a valid employment or contractual relationship can have access rights to OP's information systems.
- Access rights management in OP is based on the centralised access rights management system used to manage user IDs at Group and organisational level. Access rights are granted in accordance with a person's role.
- Processes and the related supportive tools for adding, changing, removing and regularly reviewing access rights form part of the implementation of access management principles. Granted access rights are reviewed regularly to identify risky combinations of tasks and to ensure the principle of least privilege and segregation of duties.



12. Application security

- Application owners are responsible for ensuring information security throughout the system/software life cycle.
- Information security risks concerning a new system or application, and the related changes, are identified and assessed during the development idea stage.
- The planning phase must take account of functional and non-functional information security requirements, and risk- and threat assessment based information security controls.
- All requirements are fulfilled during development.
- Internal information security testing or external auditing is done prior to the release of a system/software or major change to an existing system/software. Information security testing can also be done automatically, as part of the development release process.
- Post-development:
  - Regular system vulnerability scans are performed to monitor information security vulnerabilities.
  - An invitation only Bug Bounty program is running for vulnerability monitoring of designated customer services.
  - Web application firewalls and DDoS protection are used to protect customer services.

13. Infrastructure security

- OP's information system infrastructure is protected by a layered information security architecture. If one or more technical controls fail, other technical solutions work to prevent or limit any problems caused. The layered structure begins with devices and extends, via data communications networks and devices, to servers and services.
- OP's intranet is segmented into data networks — such as production networks, development networks and workstation networks — depending on the segment's purpose and the related regulatory requirements. Segmentation ensures that information security problems in one environment do not spread throughout OP's internal network. Data communications between segments are filtered and monitored. They are also encrypted in accordance with the related risks and regulatory requirements.
- Servers and workstations are hardened, equipped with information security software, regularly updated and covered by access control and log-management solutions, and their information security level are continuously monitored and violations countered.

14. Third party and cloud services security

- To a growing extent, OP's infrastructure extends to third-party and cloud services. Infrastructure, platforms or software can be procured as a service. When software or platforms are procured in this form, cyber security management is based on contractually agreed matters and third party risk management.
- Before moving to a third party or cloud service, the related information security risk-level in accordance with OP's procurement processes is assessed. The risk-level specify the related information security requirements that must be in the agreement made with the third party or cloud service.
- The third party and cloud services security requirements are identical with the infrastructure security requirements.

15. Detecting cyber threats

- OP follows news and developments in information security and gather threat information and technical Indicator of Compromise (IOC) descriptions from multiple sources.
- OP has multiple Security Operations Centres continuously monitoring the information security of OP's infrastructure for internal and external threats. Detected incidents are investigated and managed in accordance with agreed and documented procedures. Such incidents can include malware alerts, online scams targeting staff, and attacks on information systems or data networks.
- A security technology stack which includes analytics, is used to detect information security incidents in the networks and systems.

16. Business continuity and recovery management

- OP has a framework of reference for high-quality business continuity management. Every business and OP cooperative bank is responsible for ensuring uninterrupted operations through its own business continuity plan and system-based recovery plans. Business continuity plans include preparation for cyber threats. OP's contingency plan is based on OP's business continuity plans.
- OP actively trains for cyber security incidents through the year.
- OP performs annual red or purple team testing to ensure that the protection, detection and response capabilities perform as expected.

OP Financial Group