Public

Owner
Telia Company
Group Security

Editor
Group Security GRC

Security in Telia Company – general description

Table of contents

Introduction

Telia Company continuously works to protect business, customer and shareholder interests. Telia Company implements security measures which aim to balance risk exposure, business value, vulnerabilities and threats.

1 Purpose

The purpose with this document is to describe the general security work within Telia Company which aims to achieve appropriate security level according to legal, contractual and business requirements. The document can be used in the communication with Telia Company's customers.

2 Scope

The document describes the general security work within the Telia Company Group.

3 Telia Company Group Policy - Security

The Telia Company "Group Policy – Security" [1] is issued by Telia Company Board of Directors stating mandatory security requirements for the group. It aims to control, facilitate and implement well-balanced security measures throughout our operation. Security measures are characterized by appropriate security and risk awareness, prevention, preparedness, and the ability to respond to, and recover from, incidents and changes in the environment.

The Group Policy applies to Telia Company AB and for its Subsidiaries and Joint Operations as their own binding policy, and is communicated on the Telia Company external website as well as on Telia Company intranet.

4 Security governance within Telia Company

Telia Company has established and implemented an Information Security Management System (ISMS) according to ISO/IEC 27001:2013 [2]. The governance of security within Telia Company is coordinated by Group Security in cooperation with all parts of the organization. The purpose with the ISMS is to preserve confidentiality, integrity and availability of information in accordance with the Group Policy - Security.

The main drivers for security are:

- Protection of shareholders' value and the company's assets and investments
- Ensuring that customers' expectations and business agreements are met
- Ensuring that the business strategies and objectives are not jeopardized due to security risks
- Ensuring that laws and regulatory security related requirements are complied with (legal compliance).

The Group Security ISMS scope includes Telia Company Group Security Governance and Enterprise Security Risk Management processes and their supporting systems, specifying requirements on information security and risk management across all organizational entities.

The ISMS is continuously maintained, evaluated and enhanced in accordance with identified needs.

The overall ISMS objectives are;

- Security risks are being adequately addressed and maintained;
- Compliance with internal and external security requirements;
- Sufficient security awareness throughout the organization; and
- Group Security Policy and Instructions current and aligned with relevant strategies.

The yearly activities performed within the scope of the ISMS aims to uphold the ISMS objectives, and include analyzing Telia Company organizational context from an information security perspective where interested parties and their expectations, issues and requirements are considered. Security risks management gives input to the main ISMS process steps.

The ISMS defines organizational roles and responsibilities for security, and its Statement of Applicability (SoA) includes the full range of ISO/IEC 27001:2013 Annex A security controls.

The SoA controls are implemented and managed as a delegated line organization responsibility i.e. all parts of Telia Company are governed under the ISMS, even if they are not included in the detailed certification scope [2]. Other key dependencies to the ISMS include supplier management, security incident management, and security design processes and procedures.

5 Security organization

Chief Security Officer, CSO

Telia Company CSO acts on behalf of the CEO by developing and maintaining security steering documents, coordinating Telia Company group security matters and by exercising central control to exploit scale advantages and synergies.

The CSO owns the security governance model and process for the Telia Company group´s 100% owned companies. For majority owned companies, certain key processes are identified and must be in place. The security governance process embraces all security areas in the group.

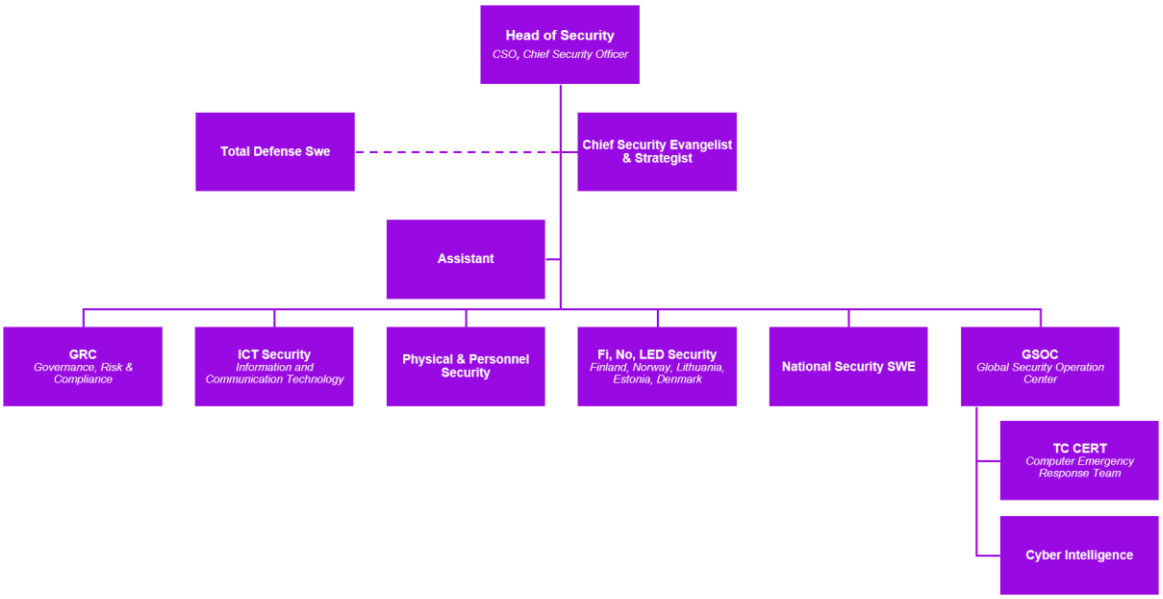

Figure 1: Telia Company Group Security organization. The Group Chief Security Officer (CSO) has the overall responsibility for the security governance in the Telia Company group.

6 Risk assessment and treatment

Telia Company Group Policy for Risk Management provides directions on how to work with risk at Telia Company. The policy emphasizes the management of risk within the daily operations; the work with identifying and managing both risks and opportunities shall be fully integrated in the business planning, control and working processes. The line organization has the primary responsibility for managing risks. The Chief Risk Officer is responsible for coordinating and monitoring the process and compliance as well as reporting to Group Management and Board of Directors.

The risk management process is process based on the principles in the ISO standard 31 000 for risk management. Basic steps in the process are:

- Risk assessment
- Risk treatment
- Continuous monitoring

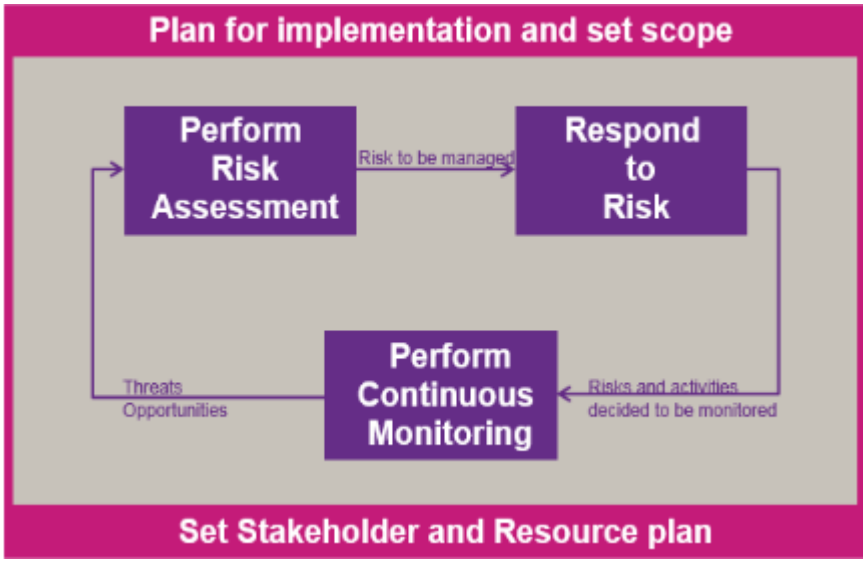

Figure 2: Telia Company Risk management process

7 Asset management and information security

Telia Company protects its assets such as personnel, information, IT infrastructure, internal and public networks, as well as office buildings and technical facilities. Special attention is given to information affecting user privacy. Information security is vital for Telia Company in ensuring appropriate protection of information during its whole lifecycle. Telia Company has measures to set appropriate level of protection of its assets and to prevent and detect disclosure of sensitive information to unauthorized parties.

Information classification is the basis for security related work. By knowing the criticality of information and its security class it is possible to define the protection level needed for the information and design appropriate protection mechanisms in an economic and efficient way. Information assets are to be classified based on legal, contractual and business requirements by using Telia Company' s security classification model and protected accordingly taking into account also threats and risks.

Three security characteristics described below are to be considered when classifying information and when defining the protection level for the corresponding IT solution:

- **Confidentiality**: Providing protection of the information in such a way that it is not available for or disclosed to unauthorized or unintended users/parties.
- **Integrity**: Defining necessary protection against unauthorized modification, deletion, repetition or loss of information. It also provides functionality to verify or trace modifications.
- **Availability**: Defining the necessary protection for making Information and Services accessible and usable upon demand by an authorized entity, within an agreed maximum duration of unavailability.

Telia Company uses four confidentiality levels: Public, Internal, Confidential and Secret, in order of increasing security level, providing the required security objectives for the corresponding classes.

8 Human resource security

Telia Company has an internal baseline to set the security levels for TC employees and contractors. Prioritized measures are:

- Safeguards to prevent employees from threats and harm.
- Ensure that employees, contractors and third-party users understand their responsibilities.
- Ensure that employees, contractors and third-party users are suitable for the roles they are considered for.
- Reduce the risk of theft, fraud or misuse of facilities, resources or information.

Performing pre-employment background controls is a vital part in the recruitment process and helps TC to hire with confidence. A more detailed personal screening is carried out when Telia Company is recruiting employees to fill key positions. The director who has decided to recruit is responsible for ensuring that necessary background checks / personal screening is initiated for these categories.

Group Security is responsible for performing the detailed screenings and delivering feedback regarding the results to the recruiting unit.

Telia Company continuously works to mitigate the risks for employees that may be exposed to threatening situations. Necessary protective measures are taken to reduce the risk exposure as much as possible. A structured emergency alert model is in use so employees are always (24h/7) able to call and receive support if threats occur on business trips.

All employees sign appropriate confidentiality agreements.

Improving security awareness is a continuous process. It is targeted at all levels of the organization, including subcontractors and other third parties working for Telia Company. The aim is that all employees, and others working for Telia Company, understand and are familiar with the laws and regulations governing Telia Company's operations, internal and contractual requirements, implemented protection mechanisms and related incident reporting methods. Security steering documents (e.g. policies, instructions, guidelines and best practices) are available on the company's intranet. Telia Company runs a security awareness program that consists of mandatory and more specific e-learnings covering different areas of security, combined with tailor-made trainings arranged for specific target groups (e.g. customer support, shops, project managers, product managers).

9 Physical security

Appropriate security levels in offices, stores, technical sites and data operation centers according to business demands is essential for maintaining Telia Company businesses and personnel security.

Threats against Telia Company assets (products, operations and facilities) are analyzed to assess the need for and degree of access protection. In assessing and designing protection, the location of the facility, the availability of guards and the frequency of crime in the area are taken into consideration.

Planning and establishment of sites or operations is evaluated to avoid unnecessary risks. Before establishing an operation, risks related to natural and human caused hazards at the site and the surrounding area are identified and evaluated by the business responsible in consultation with facility management.

To achieve appropriate security level Telia Company has internal requirements such as:

- Security areas in all offices, stores, technical sites and data operation centers shall be defined and classified in different security levels. Each level is defined according to what security measurements needs to be fulfilled. The zone concept for offices is divided in three levels and technical facilities are divided into five levels to be able to adapt the protection for the specific requirements.
- Ownership for each security area shall be defined and documented.
- Access control arrangement must be in place in all types of security areas.
- Access rights shall be documented and regularly revoked.
- Protection against burglary, fire and other threats must be in place according to security area type.

Access to the Telia Company Group's property, plants, buildings and locations is controlled. Access for authorized persons is limited to the demands of their particular tasks or assignments. In addition, access to installations of a sensitive nature requires approval by the director in charge or the owner of the room/ area. Access rights are handled in a common way in order to ensure efficiency and security. Security is achieved by having good processes in place.

Telia Company business operations are located in controlled areas, which are physically protected by a defined and documented security perimeter. A controlled area is designated as a zone which represent Telia Company physical zone concept.

Workplaces that are regularly visited by customers and other business contacts have issued clear-cut routines for handling visits, besides providing the necessary technical security solutions.

Employees can prove their identity with an ID card issued by Telia Company. Anyone who visits an access-protected Telia Company area must wear his or her ID badge so that it can readily be seen. The general exception to this rule is in public locations to which the public or customers have access.

Contracted personnel and service personnel must be able to confirm their identity. It is up to each Region (or country) to decide if contractors etc. shall use an ID card issued to them by Telia Company or with an ID card issued by own employers. If they have not received an ID card from either their own employers or Telia Company, they will be registered as visitors and provided with visitor's ID badges.

10 Operations security and communications security

During the entire life cycle of products, services, and key strategic and operational processes Telia Company works to identify and mitigate risks and threats affecting the operations and services. Analysis aims to guide decision making and ensure proper implementation of security measures to meet compliance and balance risk exposure.

To ensure that Telia Company conducts its operations and delivers according to expected quality there are group common requirements that must be fulfilled. Examples of such requirements are in the areas of: change management, logging, using third party services, IT and network management. It is the responsibility of the line organization to implement and comply with the governing documents and procedures that Telia Company has adopted, according to the Telia Company security governance model. To ensure compliance, security delegation agreements are defined and delegated to the line

organization clarifying their role, mandate and responsibility within the security area. Risk analysis and risk assessment is used for making decisions and to ensure proper implementation of security measures to meet compliance and balance risk exposure.

11 Access control

Telia Company maintains control of the access to information, premises, IT Solutions, network elements and other assets, based on business, security, legal and contractual needs. Telia Company makes great efforts to ensure that access rights are granted only on personal “need to have” basis and connected to staff according to responsibilities and duties. Regular updates and controls are implemented for the access control systems. The user´s access rights are reviewed after change of duties and/or responsibility. Access is controlled to prevent unauthorized access or trespass.

Telia Company has internal requirements to ensure that groups of information processing facilities and users are segregated in the IT solutions and networks to support legal, contractual and business requirements and protect Telia Company against major service disruptions, incidents or fraud. The line organization is responsible for implementing access control in ordinary operations as well as managing and follow up procedures.

12 Information systems acquisition, development and maintenance

Telia Company uses projects as a form to conduct business critical work and to allocate resources to investments. A common project model framework for project management is used which aims to provide support for the control, management and execution of projects. The common model enables measuring project progress and results in a unified way. The model provides a common project decision-making framework and supports the management of projects with common instructions and templates.

Within the project models there are security activities that will help the project to identify and implement necessary measures to fulfil legal, contractual and business requirements. These measures are a combination of physical and logical security measures for assuring integrity, confidentiality, availability and accountability which together will assure the required security level. In the end of the project there is a formal handover to the receiver organization. The purpose with the formal handover is to assure that all the necessary information is transferred to the maintenance organization and that they have the ability to manage and ensure the required security level through the entire life cycle.

Telia Company use third party services for some parts of the operations. In these cases, Telia Company follow established procedures and routines for ensuring required security level is fulfilled by the third part. These procedures include analyses to identify and setting the requirements as well as follow up that the required security level set by Telia Company is achieved.

13 Information security incident management

Telia Company Global Security Operation Center (GSOC) enables the company to prevent, detect, investigate and respond to security incidents and frauds. The GSOC organization is divided into two group level functional teams: Cyber Intelligence and TC CERT.

The Security Incidents team manages variety of services and processes, which concentrate on IT security in both customer networks and in Telia Company’s own corporate network.

The Security Support team provides operational support in relevant security areas, mostly providing guidance and best practice but also operative tasks if agreed upon but also awareness activities and security training. The team is also responsible for managing all internal investigations.

Telia Company maintains zero tolerance towards criminal activities. Measures are in place to detect and promptly respond to security incidents. All Telia Company employees and line managers are obligated to report security incidents according to established routines. As a rule, the police are notified of crime or suspected crime. Telia Company only discloses information to authorities to the extent required by local laws

14 Business continuity management

Business continuity management assures the resilience of Telia Company' s critical processes, functions, services and products in the event of disruptions which may significantly impact upon Telia Company' s ability to deliver its' key services and products to customers and other stakeholders.

Potential threats and impacts to the business are identified and whenever possible, mitigated before they occur. Continuity plans are in place to ensure the appropriate response to and recovery, according to business, legal and regulatory demands, from events that disrupt the continuity of the business.

Business continuity management is incorporated in Telia Company' s product life cycle and infrastructure life cycle processes to further ensure resilience. Business continuity management is managed according to best practices and international standards.

Telia Company' s Crisis Management organization handles critical incidents/situations and is in place at Group level as well as country level. Crisis management plans enable the Crisis teams to efficiently manage and communicate the appropriate information during a crisis. The crisis team provides an interface to customer support.

Telia Company's operations are continuously monitored by the Service Assurance & Operations (SA & Ops) control center.

Service Assurance & Operations control center monitors the status of the production environments and focuses on preventing incidents by proactive monitoring and actions, resolving incidents with minimal outage time for the customer and managing information to customers. The SA & Ops control center also analyses production quality impact on customer experience, identify improvements needed, and inform stakeholders to ensure high level services.

15 Compliance

Telia Company continuously works to comply with relevant laws and regulations as well as with contractual demands. To ensure compliance with laws, contractual demands and Telia Company' s internal steering documents, security requirements and reviews are defined and delegated to the line organization clarifying their role, mandate and responsibility within the security area. Security awareness activities are arranged to facilitate the compliance within the organization.

It is the responsibility of the line organization to implement and comply with the governing documents and procedures that Telia Company has adopted, according to the Telia Company security governance model. Telia Company has whistle-blowing procedures to give possibility to employees or other stakeholders raise concerns about perceived

misconduct in the company or how the company conducts business with customers or suppliers.

Security audits (reviews) are decided by Group Internal Audit. Security audits are conducted to ensure implementation of corrective actions and compliance with the Group Security Policy, instructions and legal/regulatory demands.

Non-compliance to the Telia Company Group Security Policy is reported to the Chief Security Officer (CSO).

16 References

[1] Group Policy - Security https://www.teliacompany.com/en/about-the-company/public-policy/

[2] The Telia Company Group level ISO/IEC 27001:2013 Certificate No. C463-ISMS143-08-18 valid from 2018-08-11 to 2021-08-21 (subject to annual surveillance audits). *Certification scope: Telia Company Group's ISMS covering the Group Information Security Governance and Enterprise Information Security Risk Management processes and their supporting systems, specifying requirements on information security and risk management across all organizational entities in accordance with the Statement of Applicability (SoA), Ver. 1.0.* This certificate can be validated by email request at ms@pecb.com (UIC: MSCB-111-96452).

17 Version history

Versions	Status	Date	Modified by	Comments
1.0	Approved	2012-12-10	Andreas Rappe	
2.0	Approved	2013-09-30	Andreas Rappe	Text updated
3.0	Approved	2014-09-05	Andreas Rappe	Updated text in chapter: 3,4,6,7,13,14
4.0	Approved	2016-09-28	Fiona McPheat	Updated text, organization and template with new logo
4.1	Approved	2018-07-02	Peter Björkman	Text updated
5.0	Approved	2018-11-12	Peter Björkman	Organization & text updated