ERICSSON

OUR ENTERPRISE SECURITY

EMPOWERING BUSINESS

INTRODUCTION

Communication is changing the way we live and work. Ericsson plays a key role in this evolution, using innovation to empower people, business and society.

This document is intended to provide the reader an overview of how Ericsson addresses the different aspects of our Enterprise Security, i.e. Personal Security, Asset Protection and Product Security. Any additional questions after reading this document on our Enterprise Security should be sent to Ericsson via http://www.ericsson.com/contact

Ericsson manufactures and supplies products on the basis of international standards such as 3GPP (wireless) and best architecture practices such as ITU-T recommendation X.805. Business operations including managed services are carried out in line with the ISO/IEC 27001 Information Security Management standard. Ericsson believes that security is crucial for maintaining and enhancing stakeholder confidence by:

- **Personal Security**
Doing all that can be done to ensure the wellbeing and safety of Ericsson's personnel and disaster response efforts

- **Asset Protection**
Protecting the information and physical assets for which Ericsson are custodian (our own, our customers' and partners')

- **Product Security**
Providing products which are resilient to serious threats presented by the evolving telecom landscape and assisting with security services to ensure our customers' assets are well defended

Ericsson's business is driven by speed and simplicity. Our growth and success lies in our ability to collaborate and build partnership, while knowing and acting on inherent security risks. Security should provide the right balance of risk taking versus risk mitigations.

Due to the ongoing evolution of the worsening threat landscape, it is important to align security mechanisms through proper risk management processes, instead of relying on isolated security controls.

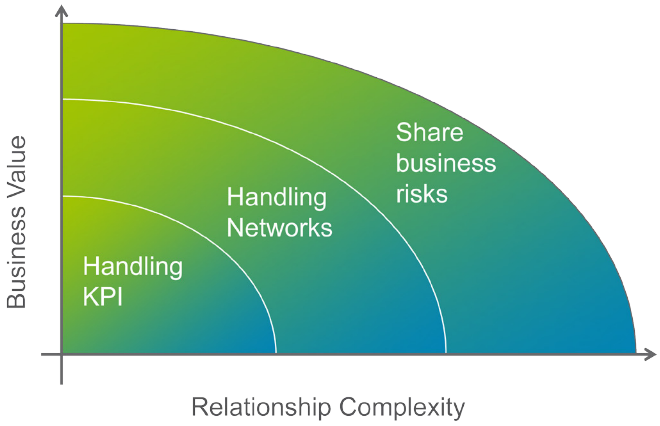
Security risk management in daily operations is always under improvement and regular reviews take place to ensure the effectiveness of controls, including assessing any new threats and vulnerabilities.

Ericsson is in a leadership position today, but we have to evolve to meet our customers' expectations.

We are evolving from a mainly transactional relationship of managing security KPIs into truly becoming a part of the customer's business.

Customers should rest assured that Ericsson treats their business as we do our own. This leads us to increased customer collaboration and greater complexity in our customer relationships.

Today Ericsson has the telecom industry's most comprehensive managed services offering. Activities range across designing, building, operating and managing day-to-day operations of a customer's network. We manage networks that serve more than 750 million subscribers in more than 100 countries.



SECURITY SHOULD PROVIDE THE RIGHT BALANCE OF RISK TAKING VERSUS RISK MITIGATIONS.

Respect, including respect for the privacy of individuals, is one of our core values to be complied with by all employees in their work for Ericsson.

We are committed to protecting the privacy and confidentiality of personal information, including, but not limited to employees, contingent workforce, customers, and end-users.

As the relationship with customers is becoming more complex we are proud of having a world-wide organization of security professionals supporting account managers in dealing with whatever security concerns our customers may have.

PERSONAL SECURITY

We are committed to ensure a safe working environment and healthy workplaces around the world. We have a comprehensive organization and supporting tools to assist personnel in our business activities should an emergency occur. All personnel have access to a dedicated 24/7 emergency number and the latest travel advisories for all countries which we operate in.

> PERSONNEL WHO ARE EXPOSED TO THREATS SHALL BE GIVEN ADEQUATE PERSONAL PROTECTION.

Following the 9/11 attack and the Thailand Tsunami 2004, the need to instantly know who is where became evident. On Group level we have access to travel details for most of the business travelers. We are proud to say that today we are able to reach almost all staff with immediate warning SMS or request travelers to confirm health status and location.

However, even with the current high level of Ericsson knowledge relating to travelers whereabouts, we are constantly seeking to improve by increasing coverage, both in terms of the number of travelers and also geographical area.

When an incident is perceived as crisis, Ericsson's crisis management organization takes action. Regions within Ericsson all have a Crisis Management Task Force (CMTF) to deal with severe incidents not managed by normal incident management procedures.

Crisis Management

We manage a crisis situation in accordance with applicable steering documents and actions are prioritized to remove or minimize threats to life and safety. Our priorities in a crisis are:

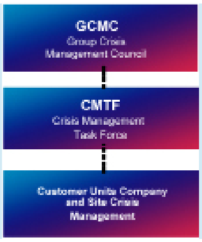
1. Removing threats to life or safety
2. Protecting the commercial interest of Ericsson
3. Protecting the brand
4. Ensuring that Ericsson is acting as a responsible corporate citizen

The following diagram outlines our crisis management organization.

> Group Crisis Management Council (GCMC) – Manages crisis on Group level

> Crisis Management Task Force (CMTF) – Manages crisis on Regional and Business Unit level

> Customer Units, Company/site crisis teams – Manage crisis in the country or on the site


GCMC
Group Crisis Management Council
CMTF
Crisis Management Task Force
Customer Units Company and Site Crisis Management

We strongly believe that a crisis situation is best handled locally by the affected organization's CMTF. At Group level the Group Crisis Management Council (GCMC) is the supervisory body which monitors and supports CMTF actions.

Many successful tasks have been carried out including evacuation of staff from places of unrest, rescue operations from earthquake-hit areas, etc. We are taking every opportunity to improve by reviewing lessons learned following all major crisis situations that have occurred.

Disaster Response Efforts

While we as individuals cannot do much about specific events, we can do something about the aftermath.

When there is a human need to communicate Ericsson is there.

The Ericsson Response program is based on Ericsson's previous involvement and experience in various disaster response efforts throughout the world and is run in collaboration with several United Nations organizations, the International Federation of the Red Cross and the Red Crescent (IFRC), Save the Children and other partners.

Ericsson Response was founded in April 2000 at the request of company employees who wanted to use their experience and skills in disaster relief situations on a voluntary basis. Since then hundreds of Ericsson employees from all global regions have volunteered, been trained and deployed in various disaster relief operations.

ASSET PROTECTION

We provide support for networks with over 2 billion subscribers and we manage networks serving more than 750 million subscribers. In addition, we handle many trade secrets in our daily operations. This responsibility, entrusted to us by our customers and partners, has led Ericsson to cultivate strong capabilities in the area of asset protection.

Ericsson is convinced that meeting the challenging business demands to protect assets that we own, or have been entrusted with, involves the implementation of security frameworks which augment our day to day operations.

These frameworks are supported by top level management and are clear on roles and responsibilities. Information Security, Physical Security and Business Continuity are all in scope for such frameworks, resulting in consistent, efficient and cost effective Enterprise Security.

Information Security

The Information Security Management (ISM) framework defines how we manage information security in alignment with the international information security management standard ISO/IEC 27001. However, when there is a clear business value and/or a customer request, Ericsson will proactively acquire ISO/IEC 27001 certification within defined and prioritized scope.

CORRECT ACCESS TO CORRECT INFORMATION AT THE RIGHT TIME IS AT THE CORE OF ERICSSON'S BUSINESS.

The human factor plays an important role in protecting information. All staff is regularly trained in basic security practices and Ericsson utilizes ongoing information campaigns to keep everyone informed and up to date.

One important contributor to achieving an advanced level of information security is IT-security – ensuring that IT systems perform as expected and have the sufficient capability to protect information. Security controls that we have implemented are based on industry best practices and general standards, such as CobiT (used for the SOX ITGC controls), ISO 27001, NIST 800-53, privacy laws, and other applicable regulations. Experience to date has proven their effectiveness, attested to by various activities including penetration testing and external audits.

Purpose of this session

- > Raise awareness on Information Leakage.
- > Understand connection between risk of information leakage and your position.
- > Become more risk conscious and know how to act.

TWO CAN KEEP A SECRET – IF ONE OF THEM IS DEAD

Confucius 500BC

Information security awareness training is an essential part of the ISM framework.

All leadership teams, employees and external workforce are targeted for regular awareness activities.

Physical Security

The Physical Security Management framework defines how we manage physical security. As a global organization we have a long tradition of defining and implementing physical security controls to counter the wide and varied array of threats.

PHYSICAL SECURITY INCLUDES PROTECTION AGAINST UNAUTHORIZED ACCESS, FIRE AND OTHER HAZARDS.

Now we are in a phase of aligning physical security management with information security management in order to satisfy requirements set out by ISO/IEC 27001.

The physical security framework is executed locally to achieve cost effectiveness taking local threats and vulnerabilities into account.

Business Continuity

We feel that there is a high sense of urgency for Business Continuity Management (BCM) due to events such as pandemics, ash-clouds, severe storms and acts of violence. We have seen an increase in awareness and demands for BCM from customers and other stakeholders which we address by Ericsson's BCM framework.

We are proud to announce that our external auditors, DNV, PWC and E&Y are supporting this BCM framework approach and that it has been deployed throughout the organization.

PRODUCT SECURITY

Product Security is the capability embedded in our products to support secure network operation by preventing damage from threats such as denial-of service attacks, theft or manipulation of network data.

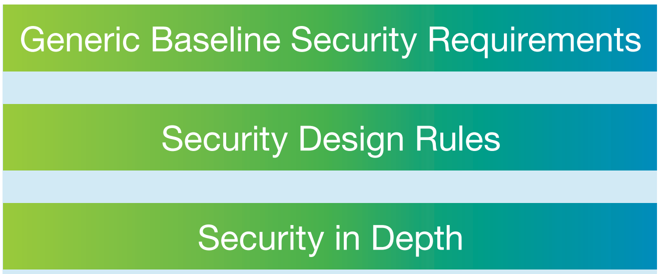
We manufacture and supply our products on the basis of international standards for the management of telecommunication products, such as 3GPP and best architecture practices such as ITU-T X.805 recommendation.

Network operators and service providers must adapt to a continuously changing risk landscape and vendors must provide appropriate security in their products, solutions and services. We are actively adapting our products as networks evolve, based on best practices and our own experience of network operations. Thus “best of breed” products and operational experience are embedded into Ericsson’s offerings.

PRODUCT SECURITY IS THE CAPABILITY OF THE PRODUCTS TO SUPPORT SECURE NETWORK OPERATION.

The evolving networks and changing threat scenarios demand appropriate measures to be taken during the product development process. These measures enable us to ensure the required level of product security.

Although the required level of product security shall always be determined in a business context we also have to provide a basic security level that is in balance with the risks faced and our customers’ explicit and implicit expectations. Apart from security functionality implemented in the product itself, hardening and vulnerability analysis is part of the development process.



The Generic Baseline Security Requirements are based on existing best practices in the industry and what is normally expected as the inherent level of security in telecom products.

In achieving the required level of product security, Ericsson is using well defined Generic Baseline Security Requirements and Security Design Rules that are regularly updated to match the changes in technology, regulations and business.

The Security in Depth principle, which can be summed up by the term “belt and braces”, is fundamental for the Generic Baseline Security Requirements. It is considered a fundamental security principle for products supplied by Ericsson and is based on many complementary security mechanisms arranged to support each other.

Telefonaktiebolaget LM Ericsson
SE-126 25 Stockholm, Sweden
Telephone +46 8 719 0000
Fax +46 8 18 40 85
www.ericsson.com