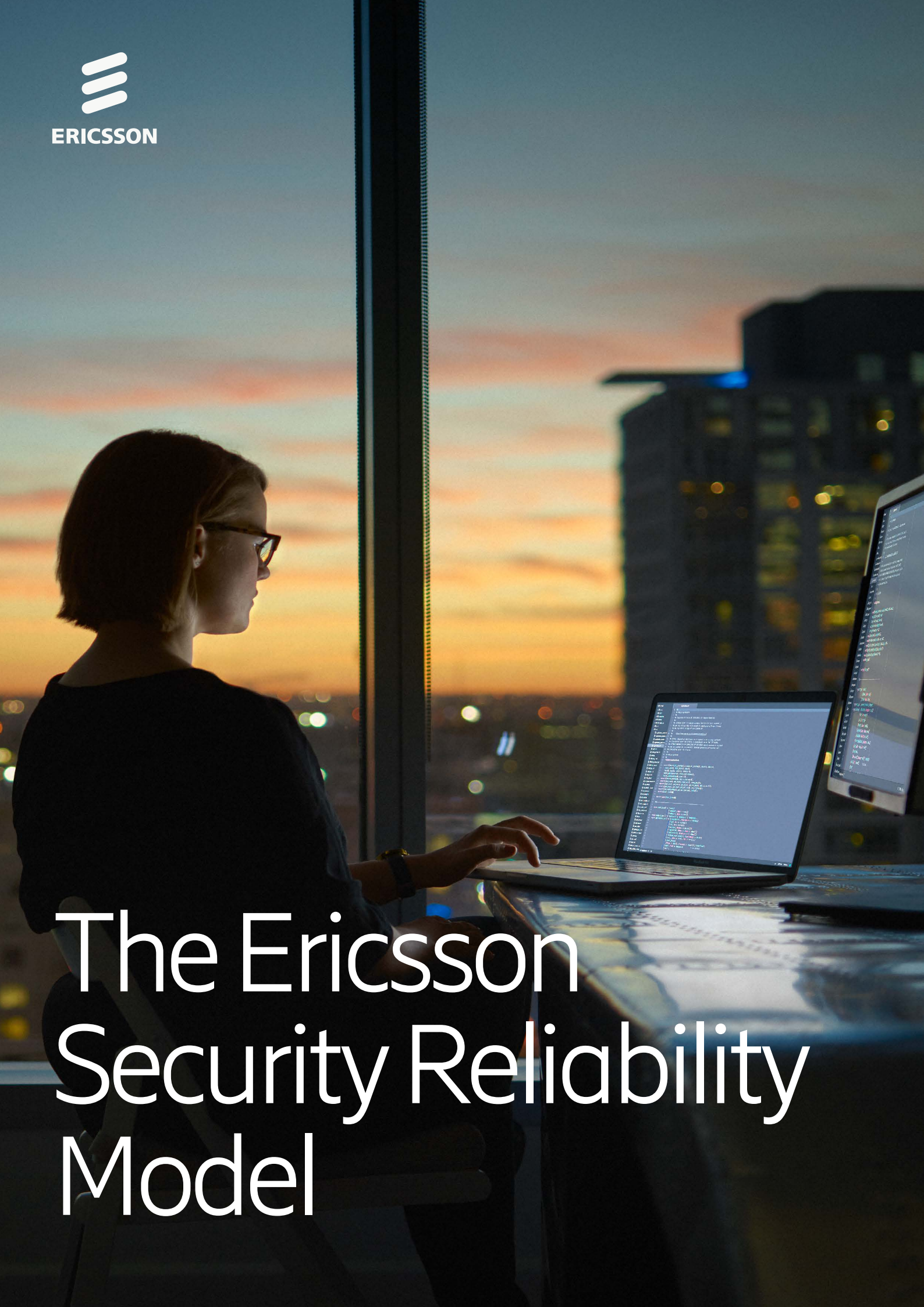


ERICSSON

The Ericsson Security Reliability Model

Ensuring product security and privacy by design and default

At Ericsson, we systematically incorporate security and privacy considerations into all relevant aspects and phases of our product value flow. Our efforts in this area follow a well-established internal control framework known as the Security Reliability Model (SRM).

The SRM defines Ericsson's approach to achieving our product security and privacy by design ambitions. Its purpose is to:

- set the product security and privacy ambition levels for Ericsson's products and solutions
- specify the control framework that will enable Ericsson to fulfil the ambition levels
- outline how this control framework covers the product value flow, from the sourcing of components throughout the development activities to deployment and operations in customer networks
- demonstrate how we achieve compliance with relevant laws and regulations

How the SRM works

The SRM specifies four areas of security and privacy controls – Functions, Assurance, Compliance & Documentation, and Deployment & Operations. Functions refer to the features that we require. Assurance is about how we implement and verify products and solutions. Compliance & Documentation is about providing guidance for security and privacy in use. Deployment & Operations refers to our practices to ensure that security and privacy are maintained.

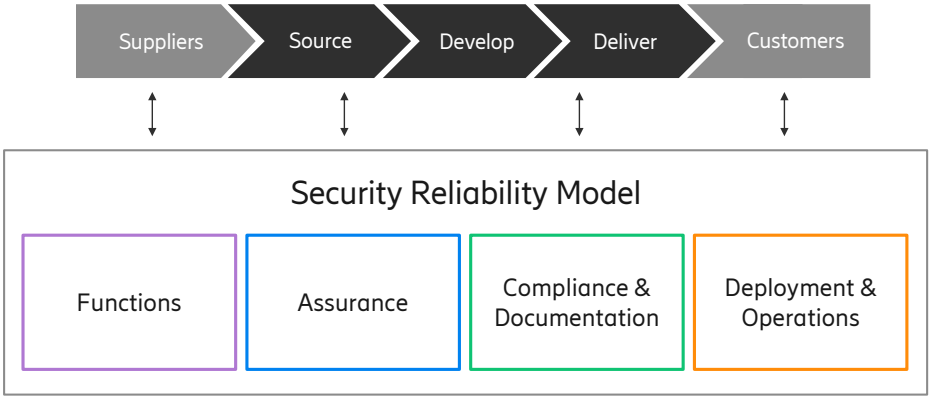


Figure 1: How the SRM interacts with Ericsson's value flow

As shown in Figure 1, the four areas of security and privacy controls apply across Ericsson's value flow, spanning from our demands on suppliers through to activities in the areas of sourcing, developing, and delivering, to ensure that we meet the demands of our customers.

The SRM is an integral part of how we work. Therefore, we provide training to our workforce about the SRM and the tasks and activities that are associated with it.

Throughout the value flow, Ericsson's ISO27001 certified Information Security Management System (ISMS) supports SRM activities with controls for information and IT security.

Supporting customer compliance

Our commitment to supporting Ericsson customers to achieve compliance with relevant laws and regulations is one purpose of SRM. When the relevant features and functions are implemented correctly, our products and technologies ensure the execution of the assurance activities that enable our customers to achieve and maintain compliance. The continuous application and evolution of the SRM is crucial for Ericsson to deliver on the expectations of customers, regulators and society around the issues of security and privacy.

Managing risks

The SRM enables a managed, risk-based approach to security and privacy implementation where requirements are tailored to the target environment and demands. As shown in Figure 2, the SRM's risk management procedures consists of four core tasks: assessment, treatment, documentation and sign off. This approach helps us meet stakeholders' expectations and cater for the rapid evolution of technology and the continuous changes in legislation globally.

While all of our products are subject to baseline SRM assurance requirements and activities, products with higher sensitivity are subject to additional assurance requirements and activities.

Figure 2: Risk management in the SRM

From Source to Deliver: the SRM and the ISMS

The SRM is centered on product security and sets the ambitions for the portfolio, but it also identifies controls to maintain integrity throughout delivery jointly with the ISMS. The purpose of the ISMS, throughout the entire value flow in the SRM, is as a baseline support, answering for information and IT security related controls in development and handling of a product in each stage. The ISMS is built on Ericsson interpretation of ISO/IEC 27001:2022 and certified for the very same standard.

Any dependencies that the SRM has on the ISMS have been reviewed and aligned to identify where SRM controls are related to ISMS. Such controls span everything from how to perform and document security training, product management and development; to how to perform and store audits; to how to tackle incidents.

Risk assessments and privacy impact assessments

According to the SRM, a product release or new feature is analyzed through both a risk assessment and a privacy impact assessment. By following the activities outlined in Figure 3, we build an understanding of the assets that comprise the release or feature (interfaces, data or capabilities) as well as their criticality, threats, controls and assumptions. We look at risk from several perspectives in a customer network context and define appropriate mitigations to minimize exposure. These treatments may be in the form of functional requirements, assurance activities or both.

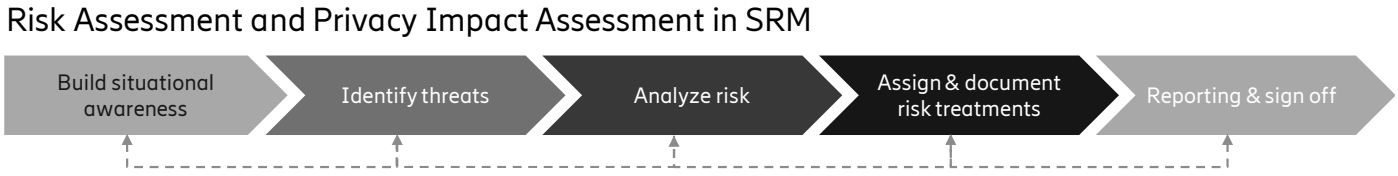


Figure 3: Process for assessing risks and privacy impacts in the SRM

Treatments are agreed upon by the relevant parties, documented and followed up on so that we can always determine what we are working toward and what progress has been made. We are transparent in our practices and examine how well we fulfill our own strict requirements through methodical assurance activities. We are also clear about responsibilities and accountability and have robust exemption evaluation processes in place to ensure the highest level of conformance as our standard from the start.

SRM area #1: Functions

The Generic Product Requirements (GPRs) defines a set of generic security and privacy functions for Ericsson products. The SRM mandates that each product organization shall analyze, decide and document the applicability and compliance to our GPRs for security and privacy.

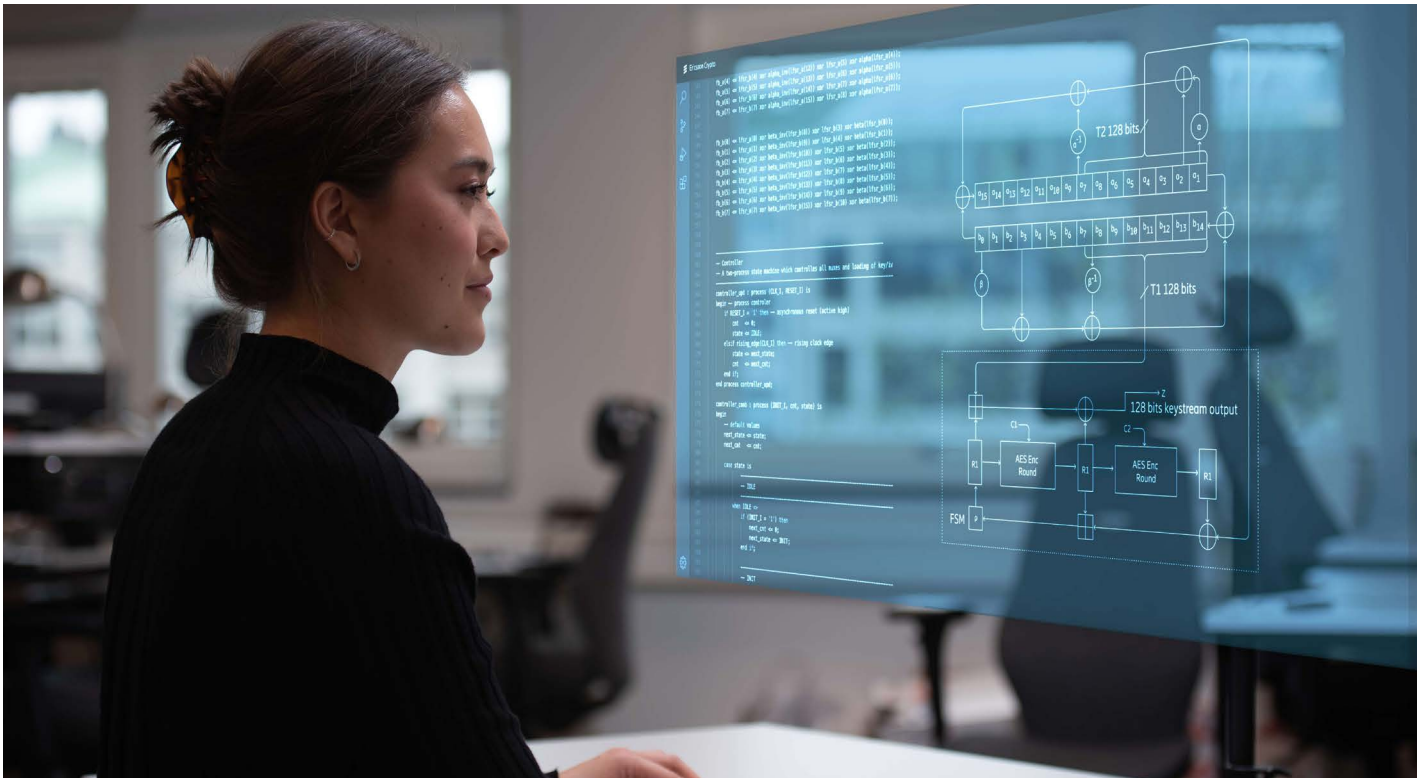
The generic security functions are divided into the following categories:

- network protection
- identity and access management
- logging
- data protection
- application security
- platform security

The generic privacy functions are similarly divided into the following categories:

- identity and access management
- logging
- data protection
- personal data identification
- fair data processing
- personal data management

Risk assessment and privacy impact assessment processes are used to identify and prioritize the applicable security and privacy functions from the set of GPRs. In other words, not all functions listed in the GPRs are necessarily compulsory, or applicable, for a specific product. The network context or target deployment will determine the applicability of GPRs and any additional functions beyond these.



Source – Develop – Deliver

The functions specified for product security and privacy will be addressed in different ways in the Source – Develop – Deliver product value flow illustrated in Figure 1.

When sourcing products or components from external suppliers for our portfolio and offerings, we consider the GPRs for product security and privacy. This also applies to third-party products that form part of a customer-specific system integration project.

In the development stage of the value flow, a set of security and privacy design rules provides guidance to the development teams about how to implement the security and privacy features. This enables the security-by-default approach that enforces the use of secure protocols, for example.

All the products Ericsson delivers to customers need to fulfill applicable GPRs. The scope of this includes sourced components, our own development and solutions that comprise several products. In addition to using a common set of generic requirements as a base, our products also often include security functions that are context and deployment-scenario dependent.

SRM area #2: Assurance

Assurance refers to the activities conducted with the intention to ensure that the final product is secure when it is running in its target environment.

We have grouped our assurance activities into five main categories:

- risk assessment
- privacy impact assessment
- secure coding
- vulnerability analysis
- hardening

Additionally, our assurance work includes activities for continual improvement and adherence evaluation.

The SRM specifies the relevant assurance activities for each category in every phase of the product value flow: Source, Develop and Deliver. Depending on the characteristics of the product, the appropriate level of assurance activities – basic, advanced or tailored – is set for each category. Refer to the 'Assurance levels in the SRM' box for details.

Source

With respect to sourcing, the SRM defines the assurance activities done at the time when either free and open source software (FOSS) or commercial off-the-shelf software (COTS) is used in a product.

For FOSS, the introduction to Ericsson includes a risk assessment that evaluates factors such as the amount of commits (when a new version of code is made available) into the version control system, the number of active members in that particular FOSS community, and the country of origin. The identified risks are fed into the risk assessments of products that use the FOSS.

For COTS, we perform a product security sensitivity segmentation and select the appropriate activities based on the results. As a counterpart to FOSS community evaluation, we assess COTS suppliers. Based on these and other facts, we conduct a risk assessment, allocate appropriate risk mitigations and carry them out. For COTS, we also gather information about the product components and their provenance.

For both FOSS and COTS, the sourced components are registered in our vulnerability management service for prompt indication and management of any known vulnerabilities. For more information on vulnerability management and Ericsson's Product Security Incident Response Team (PSIRT).

We are dedicated to ensuring the integrity of our supply chain and security of our products, which extends to software and hardware development, testing, implementation and operation, and incorporating risk management as a key part of our end-to-end lifecycle process.

As highlighted in Figure 4, it is the risk management procedure that identifies which products have higher sensitivity.

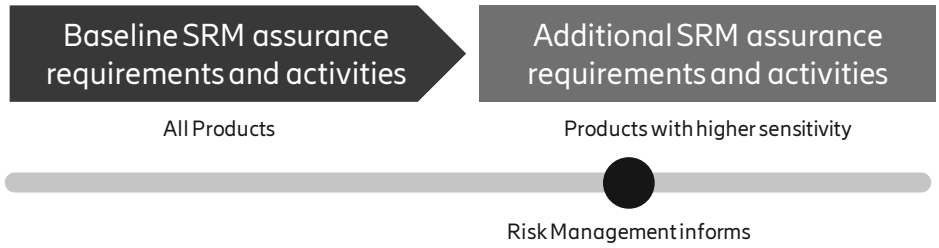


Figure 4: Identifying products with higher sensitivity as part of the risk-based approach

Assurance levels in the SRM

Different levels of security and privacy assurance are needed depending on the risk level and the sensitivity of the product. The SRM defines a set of security-assurance activities, dividing them in three levels: basic, advanced and tailored. Each level assumes fulfillment of the previous ones.

Basic-level activities apply to most products and represent industry best practice. They require a limited amount of manual work or can be automated. Basic-level activities go beyond a simple hygienic level of assurance, defining a basis for world-class security and privacy assurance.

Advanced-level activities are also based on industry best practice. For practical reasons, however, these activities cannot be executed as frequently as basic-level activities. The purpose of advanced-level activities is to further strengthen security assurance for specific parts of the product.

Tailored-level activities comprise highly product-specific activities that are not applicable for a wide range of products.

While basic-level activities are performed by all areas of product development, advanced and tailored-level activities may be performed for parts of products with a higher security or privacy assurance level, or in cases where specific assurance requirements exist. Risk assessments and privacy impact assessments can determine which advanced and tailored level activities need to be done, when cases are directly linked to specified security or privacy risk mitigation.

Develop

The security and privacy assurance areas described in this section are valid for both software and hardware. Depending on the risk assessment findings, it may be necessary to complement them with other security and privacy assurance methods.

Risk assessment

A risk assessment uses systematic methodologies such as threat modeling with STRIDE to identify risks related to the product when used in the customer's network. Based on the risks identified and their evaluation, a risk mitigation plan is created. It mitigates the identified risks by introducing security controls or by suggesting other alternative means such as specific configuration to reduce the customer's risk exposure. One option to reduce a risk is to select an advanced level of security assurance activities to be performed during product development. A set of advanced and tailored activities are defined in the assurance areas: secure coding and vulnerability analysis. Examples of such activities are extended secure coding review and penetration testing performed by an external team.

Privacy impact assessment

A privacy impact assessment is a risk management activity that examines privacy threats based on the type of personal data processed and the sensitivity of the processing activity within a given context. The assessment outputs residual privacy risks after treatment and forms the basis for implementation decisions that carry accountability. To identify privacy threats, we apply the appropriate threat modelling methodologies (TRIM or LINDDUN). Based on the threats, privacy risks are identified and evaluated, and treated according to the mitigation plan.

Secure coding

By following secure coding practices, we are able to reduce both design flaws and implementation bugs during the software development. The SRM follows the SEI CERT secure coding standard together with the OWASP top 10 and SANS CWE top 25 lists. SRM standards are enforced by tools like static and dynamic code analysis, and with secure coding reviews. Tools are configured for the optimal coverage of these rules, and a manual review of the code enforces the rules that can't be verified with the tools. Code quality may have an impact on security – for example, when the code is modified. Thus, tools are used also for tasks such as measuring code complexity, detecting the use of unsafe functions and finding duplicate code.

Vulnerability analysis

A vulnerability analysis comprises the testing and verification of activities that are designed to identify weaknesses and vulnerabilities in the product or solution. The vulnerability analysis verifies the security characteristics and security configuration of the product/solution and identifies new vulnerabilities through both black-box and white-box testing. Multiple tools and techniques are

used, such as port scanning, vulnerability scanning, fuzzing and dynamic web-application testing. Manual penetration testing is also performed. The verification of the security controls' functionality is done in the product's functional verification.

Hardening

The term hardening refers to increasing the security of an application by reducing its attack surface. Hardening affects not only design, but also configuration and deployment. It ensures that the product is configured in a manner that minimizes the risk of unauthorized access and system compromise. Development-time hardening includes, for example, ensuring that processes are run with least privileges, removing unnecessary software components, updating to the latest patch level of the components, disabling insecure services and replacing default passwords.

Continual improvement

Our continual improvement process for development and product lifecycle includes a root-cause analysis of the security flaws. The resulting improvements are incorporated into the relevant design or processes.

Adherence evaluation

Adherence evaluation refers to the monitoring and documentation of adherence to security and privacy assurance activities, functional requirements, and design rules that describe how a functional requirement is to be implemented. In the adherence evaluation, we ensure that the actual implementation was done according to the rules.

Automation

Ericsson uses the DevSecOps approach. We integrate security into a CI/CD (Continuous Integration/Continuous Deployment) pipeline to make sure all security tests have been performed through the pipeline with minimum human interaction. We automate as much as we can and introduce security as early in the process as possible in order to catch and mitigate vulnerabilities efficiently. Automation includes different types of security tests including static code analysis, software composition analysis and dynamic application security testing.

Artificial Intelligence (AI)

We leverage the benefits of Artificial Intelligence (AI). These technologies play a key role in the creation, testing, and evaluation of our products, as well as being integrated into the products themselves. We are committed to ensuring the security and protect the privacy of these systems, while working to make sure they are trustworthy.

In development environments, we only use AI systems that have been thoroughly evaluated and approved. For our products, we apply specific security assurance methods to mitigate potential vulnerabilities and weaknesses in the AI. Furthermore, our products strictly adhere to privacy and data protection principles. To ensure these principles have been followed, we have methodologies and processes in place to assess the adherence.

We continuously monitor the latest technological updates and trends, adopting them when they are deemed beneficial and secure.

API Security

Network exposure via Application Programming Interfaces (APIs) is driving a major transformation of the telecom industry. APIs are used more and more to utilize the capabilities of telecoms networks in building new business and novel services. The extended availability of the APIs as well as the new features provided by them introduce a lucrative target for malicious actors. Naturally, this development implies that the APIs delivered will have high requirements on security, both as security features and the security assurance.

SRM adopts the API security related requirements by requiring the compliance towards the OWASP top 10 for API and for Web Applications. This implies the need to mitigate the risks listed in the OWASP top 10 lists while not forgetting the other security requirements having implications to API design and implementation. We have carefully analysed all OWASP proposed mitigations and ensure that SRM includes all needed requirements.

Deliver

To ensure the security and integrity of the products we deliver to our customers we also include assurance activities in the Deliver phase of the value flow.

Software is delivered using defined delivery flows such as Ericsson's Software Gateway. This approach ensures the integrity of the software through secure delivery channels and with actions such as software signing. Security assurance for hardware includes performing risk assessments, checking of the integrity of the components and the products, signing of the hardware where possible, loading of software using the promoted delivery flows, and integrity-checking the outbound supply chain.

Configuration management

Configuration management is a key component of providing assurance across the value flow. Ericsson uses a version-control system on hardware, source code, compilers, build tools and environment, binary software, third-party components and customer documentation that ensures accountability, authorization and the integrity of all changes during the complete product lifecycle. This ensures that all the binaries can be reproduced and that there is a clear audit trail for changes.

To ensure that we have reproducible, deterministic builds, we use automated build environments with minimum manual intervention when compiling the source code and building the binaries. We have procedures in place to ensure that we track all requirements and design changes that impact the product in a systematic and timely manner. Extra care is taken to ensure that only authorized developers have access to the source code.

Ericsson embraces the approach to minimize the amount of released product versions supported. This enables rapid development with frequent releases of new product functionality.

SRM area #3: Compliance & Documentation

The Compliance & Documentation area defines the information that demonstrates the security and privacy status at product release and in the customer documentation. This area also defines applicable certificates and statements of conformance for external stakeholders, as well as providing necessary guidelines to maintain security and privacy in customer environments.

Customer Product Information

The Customer Product Information (CPI) for a specific product covers all of its features and commands. For each commercial release, the following product security and privacy related information is provided for the product on the CPI extranet:

- a hardening guideline that contains the information needed to harden the product at deployment before commencing operation
- a security user guide that describes how to operate the product in a secure way and documents the product's security features and their intended use
- a privacy user guide that describes the privacy operation and maintenance activities that can be performed for the product and documents the product's privacy-related features and their intended use (may be combined with the security user guide)

When relevant, the CPI also includes additional documentation such as update procedures.

In addition, release notes are provided, containing information about fixes to vulnerabilities in the product since the previous release.

Security test reports

Our security test reports document information that is relevant for the customer regarding the security of the product. These reports provide information about the security test tools and their versions used during development and remaining findings. They include information about any false-positive findings, such as vulnerabilities that are identified by standard security scanning tools but that are not applicable for the product in question.

Security standard conformance

Ericsson aligns our organization, processes and systems to industry and regulatory standards. We use conformance statements for selected products to demonstrate our security compliance to external stakeholders such as regulators and customers. Our approach is aligned with the GSMA's Network Equipment Security Assurance Scheme (NESAS). It includes:

- NESAS conformance claims, which are based on self-assessment and used for a specific product or group of products sharing the same development and product lifecycle processes
- NESAS audit summary reports, which document the results of NESAS audits
- SCAS (Security Assurance Specifications) evaluation reports, which must be performed by an ISO 17025 accredited NESAS test lab

Privacy compliance

The SRM privacy by design approach ensures consistent compliance with technical and administrative requirements for the entire portfolio. The requirements specify the expected level of privacy functions, privacy assurance activities, and documentation for products. This approach enables customers to achieve compliance with various regulations and standards. The privacy by design requirements are derived from various sources, such as regulatory obligations, customer requirements, and company policy and strategy. They are aligned with European Union's General Data Protection Regulation (GDPR), which serves as a global blueprint for data protection and privacy compliance.

SRM area #4: Deployment & Operations

The Deployment & Operations area focuses on the integration of any product or solution into a customer network, ensuring that it is ready for live operation. Ericsson handles different sets of activities for deployments and operations depending on the deployment model for each customer, based on their requirements.

The Deployment & Operations area groups together the operational aspects of product security that arise in the product value flow, including:

- security in system integration (SI)
- security in network rollout and deployment
- customer support

Security in system integration

Our deployment teams follow secure deployment processes and procedures for SI, where we further develop and deliver the solution architecture and tailor the implementation to fit the customer's specific context. We follow the SRM model by applying SRM activities as they are defined for functions, assurance and documentation. SI work starts with selecting released products and ends when the customer solution is activated in the production environment.

At the very beginning of each SI project we perform a security review of the solution architecture to catch any design weaknesses and inform the deployment team of any risks that need to be addressed.

We manage the risks of the customer solution by performing threat modeling and risk assessment, assessing the privacy impacts and by treatment of the identified risks. We also assess the security risks of the selected FOSS and third-party products. Before we deliver the solution to the customer, we assure the risks have been mitigated to an acceptable level.

If the solution requires the development of any additional code, our integration and deployment engineers develop it according to security design rules and secure coding practices.

Customized solutions require system hardening. Our hardening process takes into account the hardening guidelines for the solution components and the specific hardening needs for the integrated solution.

Security testing is tailored to the scope of the customer project. Depending on the contractual obligations, it may be performed by Ericsson security experts, customer security teams or third-party companies.

Where applicable, we create and supply solution security and privacy user guides and other customer-oriented documentation.

Security in network rollout and deployment

The security of telecommunication networks depends on their ability to withstand both physical attacks and cyberattacks. To support our customers in mitigating these types of risks as they relate to Ericsson products, we provide guidelines and recommendations for countermeasures. It is important to note, however, that we intend for our guidelines and recommendations to serve as a complement to local market legislation and regulations. They do not replace or override local regulations or legislation in any territory.

To ensure the integrity of network and radio sites, we recommend field activities in four key areas: physical security, site hardening, secure access and security management.

Physical security measures are designed to deny unauthorized access to facilities, equipment and resources.

Site-hardening activities include ensuring that sites are securely configured and that equipment is protected from disruptions caused by failures in supporting utilities. We encourage our customers to follow public-safety-grade guidelines and comply with recommended site requirements.

To ensure secure access, we recommend the use of an Identity, Credential and Access Management framework that consists of tools, policies and systems that enable the right individual to access the right resource at the right time and for the right reason.

Security-management activities establish, maintain and terminate the security aspects of the network. They ensure that sites are securely configured and that run-time hardening is implemented. We recommend following standard procedures for random vulnerability assessment of installed sites and ensuring hardware integrity.

The protection of our intellectual property rights (IPR), our customers' networks and their customers' data are top priorities for us, governed by the Ericsson Group Management System (EGMS) and our Information Security Management System (ISMS) policies, and certified by ISO/IEC 27001. All our personnel and suppliers follow Ericsson's Code of Conduct and Code of Business Ethics.

Customer support

When we deliver a solution to a customer, we hand over control to the customer's operations team. The key security aspects for our customer support include addressing security questions and concerns, analyzing security scan results and handling security incidents.

From an Ericsson perspective, security operations are generally about making it easy for operators to use the protection and detection functionality in the products so that they can efficiently respond to the changing security landscape in production networks.

Ericsson customer support responds to customer requests primarily by engaging in three types of activities:

- working together with PSIRT to resolve questions and concerns, security scans findings, general security tickets and incidents in a timely manner
- doing root-cause analysis of incidents, identifying actions to correct the incident and ensuring they are implemented appropriately
- identifying lessons learned and implementing the necessary organizational, process and system improvements to prevent similar future incidents in any Ericsson products

Our ISMS controls ensure that information security risks are considered. For example, when logging into our customers' networks, we log all actions and store them according to the security policy. After we have carried out the agreed activities in the customer network, we conduct security tests, preserve local hardening, and close any open ports/surfaces. Security-related tickets are routed to a special team consisting of top security experts.

Vulnerability management

Vulnerability management is important throughout the value flow, but is of greatest significance in the Deployment & Operations area.

The work to avoid vulnerabilities includes product and feature risk assessments and secure design, secure coding principles and use of analysis tools, and supply-chain security considerations. Thorough testing is performed to ensure high product quality. Security testing involves crafting input that lies outside what is expected in normal operations and may cause the system to misbehave in a way that an attacker could exploit.

One enabler for building very complex systems is the utilization of high-performing third-party components and libraries. The reuse of proven code, both open source and commercially licensed, enables most software companies to concentrate on creating added value, rather than reinventing the wheel. Unfortunately, however, including third-party functionality comes at the price of third-party vulnerabilities. To address this challenge, Ericsson maintains a catalogue of third-party components used in our products.

The PSIRT continuously monitors both public and subscription-based sources for alerts on discovered vulnerabilities in third-party software. This allows external vulnerability notifications to be mapped to Ericsson products. Where there is a match, an alert is sent internally to the affected product development organization that provides an analysis of how the reported fault impacts the Ericsson product in question. The alert analysis provides information of the severity and potential impact of the vulnerability.

If a product is affected by a vulnerability, a trouble ticket will be created. Appropriate remediation will be implemented and provided through standard support channels. Ericsson embraces the approach to minimize the amount of released product versions supported. New revisions of software contain both new features and corrections. Releases are pre-scheduled, but if urgently needed, unplanned emergency corrections can be made.

Conclusion

Ericsson's Security Reliability Model ensures that product security and privacy gaps are identified as early as possible – ideally during the conception phase of a new feature, product, service and solution. This allows us to control the direction of product development towards secure implementation. Considering relevant security and privacy requirements during the product design phase enables a secure implementation based on a risk-based approach.

Our customers are informed about the security and privacy aspects of our products via appropriate CPI documentation. This allows Ericsson customers to operate our products in a secure way and ensure better compliance to relevant privacy laws and regulations, such as the European Union's General Data Protection Regulation.

By ensuring that deployed products are free from unacceptable risks, we can avoid many potential security and privacy incidents. The security and privacy assurance is documented and the outcome is known and used for improvements in subsequent releases, as part of the product roadmap. Vulnerabilities are managed through the lifecycle of the product.

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

3/287-01 FGB 101 0955 Rev B