2. Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government. **This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers.**

A secure software development lifecycle (SDLC) systematically incorporates security and privacy considerations into all relevant aspects of product value flow and follow a well-established internal control framework. The Ericsson Security Reliability Model (SRM) defines Ericsson's approach to achieving product security and privacy by design ambitions. The SRM specifies four areas of security and privacy controls – Functions, Assurance, Compliance & Documentation, and Deployment & Operations.

1. Functions refer to the required features.
2. Assurance addresses implementation and verification of products and solutions.
3. Compliance & Documentation is about providing guidance for security and privacy in use.
4. Deployment & Operations refers to our practices to ensure that security and privacy are maintained.

The four areas of security and privacy controls apply across the end to end lifecycle, spanning from demands on suppliers through to activities in the areas of sourcing, developing, and delivering, to ensuring customer demands are met. Throughout our organizational and development workflow, Ericsson's ISO/IEC 27001 certified Information Security Management System (ISMS) supports SRM activities with controls for information and IT security.

The SRM enables a managed, risk-based approach to security and privacy implementation where requirements are tailored to the target environment and demands. This approach helps meet stakeholders' expectations and cater for the rapid evolution of technology and the continuous changes in legislation globally. While all products are subject to baseline SRM assurance requirements and activities, products with higher sensitivity are subject to additional assurance requirements and activities. A product release or new feature is analyzed through both a risk assessment and a privacy impact assessment.

SRM area 1: Functions
The SRM mandates that each product organization shall analyze, decide, and document the applicability and compliance to requirements for security and privacy. It also defines a set of generic security and privacy functions. Risk assessment and privacy impact assessment processes are used to identify and prioritize the applicable security and privacy functions.

SRM area 2: Assurance
Assurance refers to the activities conducted to ensure that the final product is secure when it is running in its target environment. These activities include risk assessments, privacy impact assessments, secure coding, vulnerability analysis and hardening. 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.

SRM area 3: Compliance & Documentation

The Compliance & Documentation area covers all the information that demonstrates the security and privacy status at product release and in the customer documentation. It 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. Security test reports and security standard conformance all play a key role in this area.

SRM area 4: Deployment & Operations

The Deployment & Operations area groups together the operational aspects of product security that arise in the product value flow, including security in system integration, guidance that operators require to operate their network in a secure way and customer support to resolve any incidents that arise.

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. By ensuring that deployed products are free from unacceptable risks, we can avoid many potential security and privacy incidents. Security and privacy assurance assessments are documented, and the outcome is used for improvements in subsequent releases, as part of the product roadmap. Vulnerabilities are managed throughout the lifecycle of the product, not just on initial build. A single process or technology does not define a secure development methodology; it requires a combination of techniques and operational maturity, transparency, traceability and trust throughout an organization to represent the best practices required to secure critical infrastructure.