NOKIA

Nokia Cyber Security Risk Assessment

Whitepaper

NOKIA

Contents

1. Introduction	3
2. Telecom Network Security Challenges	3
2.1. Business Transformation	3
2.2. Changing Threat Landscape	4
2.3. Stringent Regulations	4
2.4. Audit and compliance management	4
2.5. IP-fication and technology convergence	4
3. Nokia Security Risk Index (SRI) Framework	5
3.1. Nokia Cyber Security Reference Architecture	7
3.2. Nokia Cyber Security Attack Use Case Library	7
3.3. Nokia Unified Compliance Framework (UCF):	8
3.4. Nokia Technology Solution Effectiveness	8
4. SRI Output	9
4.1. Quantitative	9
4.2. Qualitative	10
4.3. Strategic	11

NOKIA

1. Introduction

Organizations are responsible for handling an expansive amount of business data and to curb the countless associated threats like advanced malware, researched spear phishing, data loss, hackers, privacy violations, etc. There is an inevitable need to prioritize the risks in accordance with business initiatives and concurrently develop mitigation mechanisms, which are also mandated by some legal and regulatory requirements, to restore organization towards business prosperity.

Organisations are bound by financial constraints of investments towards cyber security imperatives and need a risk based approach to strategize the security roadmap to derive the best value of the money spent.

Surveys indicate almost all enterprises have been breached – today it is not a question of **if** you are breached but **when** you are breached. An effective Security Program forms the heart of an organization's operational defence against advanced cyber-attacks.

Threat environment is highly dynamic whereas the security controls are mostly static. Any change in the business environment will also change the threat landscape. Considering the dynamic scenario within telecom, it is imperative for the organization to carry out periodic and thorough security risk assessment covering all communication layers like network & infrastructure, applications, data, identity and access, processes across various supporting technologies. Vulnerability assessment and penetration testing considering all common and known attack use cases should be part of risk assessment framework.

2. Telecom Network Security Challenges

Telecom is one of the sectors most targeted by cyber-attacks. Telecom networks are always a lucrative target for cyber criminals as they provide the necessary backbone for information exchange such as voice, video, data, and Internet connectivity and are repositories of huge amount of sensitive data. The information stolen could be used for identity theft, spear-phishing attacks, unauthorized access to systems, attacking person or their contacts, etc. A successful cyber-attack on a telecommunication operator could also have serious implications like disruption of services for customers, covert surveillance, shut down of essential services, etc. Apart from such threats, there are other factors as well that acts as a key driver for building robust cyber-security framework for telecom operators. Some of them are:

2.1. Business Transformation

The telecom business model is transforming from 'closed' to 'open' model, mainly directed towards monetizing the existing infrastructure, exploding data traffic, improving customer experience and introducing new revenue streams. These transformations are being facilitated through the adoption of disruptive technologies like telco cloud, social media, big data mobility, etc. and telecom companies are both 'consumer' and 'enabler' of these technologies. Telecom is also moving into new consumer-centric opportunities in the Internet of Things (IoT), mobile payment systems and digital content services.

These business and technology transformations, on the flip side, also introduce few challenges – telecom companies need to have clear strategies for migration, they need to deploy apt technology infrastructure and requisite processes to leverage the technology; and, last but not the least, they have to overcome huge amount of security issues and vulnerabilities that these technologies open up. Cloud opens up issues of data confidentiality; audit and transparency; legal and regulatory compliance; and business continuity. Improper controls on business usage of Social media can lead to leakage of sensitive data; impact brand and reputation; and attract malware and spear-phishing attacks. Big data opens issues of privacy and compliance; unauthorized access and queries; and leakage of data and intelligence. Unbridled Mobility can lead to leakage of sensitive organizational data; and unauthorized access to organizational infrastructure.

2.2. Changing Threat Landscape

The current threat environment has deteriorated tremendously with nation states, hacktivists, terrorists and cyber criminals using increasingly sophisticated arsenal of advanced malware for targeted and persistent attacks (APTs), which cannot be deterred by traditional security technologies. Prevention and elementary detection methods have proved largely ineffective against increasingly advanced attacks, and many organizations don't know what to do, or don't have the resources to combat highly skilled and aggressive cybercriminals.

2.3. Stringent Regulations

The legal, regulatory and compliance mandates are becoming more and more stringent for Telecom operators. In many regions, it holds the telecom operator directly accountable for ensuring effective information security environment and data privacy controls.

Regulators are exercising their right of governance on Telecom networks, since it is a key critical infrastructure. The EU has proposed a cyber-security strategy outlining its vision in the domain and clarifies roles, responsibilities and defines actions required to protect citizens'. EU General Data Protection Regulation (GDPR) contains a definition of "personal data breach," and notification requirements to both the supervisory authority and affected data subjects. In the US, cyber security is seen as a serious economic and national security threat and involves stringent procedures around it. In Asia, some governments have established national cyber security policies.

Regulators are also specifying minimal requirements of compliance that are verifiable before a network element can be used in the telecom network of any carrier. To safeguard the privacy of their citizens, some governments are proposing legislation requiring their citizens' data be stored within the boundaries of their country and governed by their privacy laws. The collective implication is that networks will need to meet minimum security requirements, operators will need to monitor and report compliance to these requirements, proactively assess the potential business impact of a breach and report breaches of the networks and business systems that process user-identifiable data.

2.4. Audit and compliance management

Several international standard development organisations like ITU, ISO/IEC, 3GPP, 3GPP2, etc. have prescribed standards that are applicable to telecom networks. Different countries have legislations and regulations that mandate the telecom operators to adopt specific security standards. Many operators also provide varied services to non-telco customers and as a service provider they also need to demonstrate compliance against various other standards like HIPPA, PCI DSS, SSAE 16, SOX, etc. The operators have to undergo different audits (both internal and external) against different standards and have to regularly demonstrate operating effectiveness of various security controls emanating from these various standards. The internal processes need to be designed considering 5 Ws - 'who', 'what', 'when', 'where' and 'why' – for various activities performed.

2.5. IP-fication and technology convergence

Telecommunication network worldwide is a mix of both circuit and packet based technologies. The Public Switched Telephone Network (PSTN) makes use of circuit-switched technology and is rapidly being replaced by mobile wireless network (packet-switched) technology. Packet-based switching technology used in Next Generation Networks is usually implemented through the use of the Internet Protocol (IP) suite. The IP was based on open standards and not originally designed for security implementations. The weaknesses in the IP have been exploited since long, and add to the risks of adopting an IP-based network.

Telecommunication networks also present a convergence of several technologies – PSTN, 2G, 3G, 4G/LTE and 5G with vital network components. These components are Access network, Transmission network, Core network (circuit-switched and packet switched), Application and Management Network, Internal and External Networks.

The interconnection interface due to this convergence of different technologies exposes the entire network to intruders and increases the potential for attacks caused by advanced malwares and exploits. Such attacks may be from either internal or external sources. In such cases, any part of the telecommunication network is vulnerable including the radio and core networks.

Attacks on telecommunication operator's network could also scale up to other networks through the interconnection interfaces. The intruders can, therefore, gain access to their targets irrespective of the geographical location. They use highly sophisticated arsenals, not leading to physical destruction, but stealing organizational and personal sensitive information for financial benefits, competitive advantage, and state sponsored attacks, etc. Some of the attack examples are

- Creating malicious codes
- Cyber terrorism
- Denial of Service Attack
- Espionage
- Identity Theft
- Fraud
- Spamming
- Intellectual property theft
- Wiretapping
- Phishing
- Spoofing, etc.

3. Nokia Security Risk Index (SRI) Framework

Business cases for security require cost-benefit balance and these related questions:

- What are our industry peers doing, and how are we placed in relation to them?
- What is acceptable industry good practice, and how are we placed with regard to these practices?
- Based upon these comparisons, can we be said to be doing enough?
- How do we identify what is required to be done to reach an adequate level of management and control over our security processes?

It can be difficult to supply meaningful answers to these questions. Security organization is constantly on the lookout for benchmarking and self-assessment tools in response to the need to know what to do in an efficient manner. The security head should be able to incrementally benchmark against that control objective. This responds to three needs:

- A relative measure of where the organization is
- A manner to efficiently decide where to go
- A tool for measuring progress against the goal

Nokia has developed a framework for cyber security risk assessment - Security Risk Index (SRI) to address the above needs. It is designed to evaluate and identify risks associated with applicable threats and inherent security weaknesses, and to provide a basis for management to establish a value-based security program.

It provides 'Quantitative', 'Qualitative' and 'Strategic' output to measure the effectiveness of their security program along with tactical and strategic security roadmap for the organization.

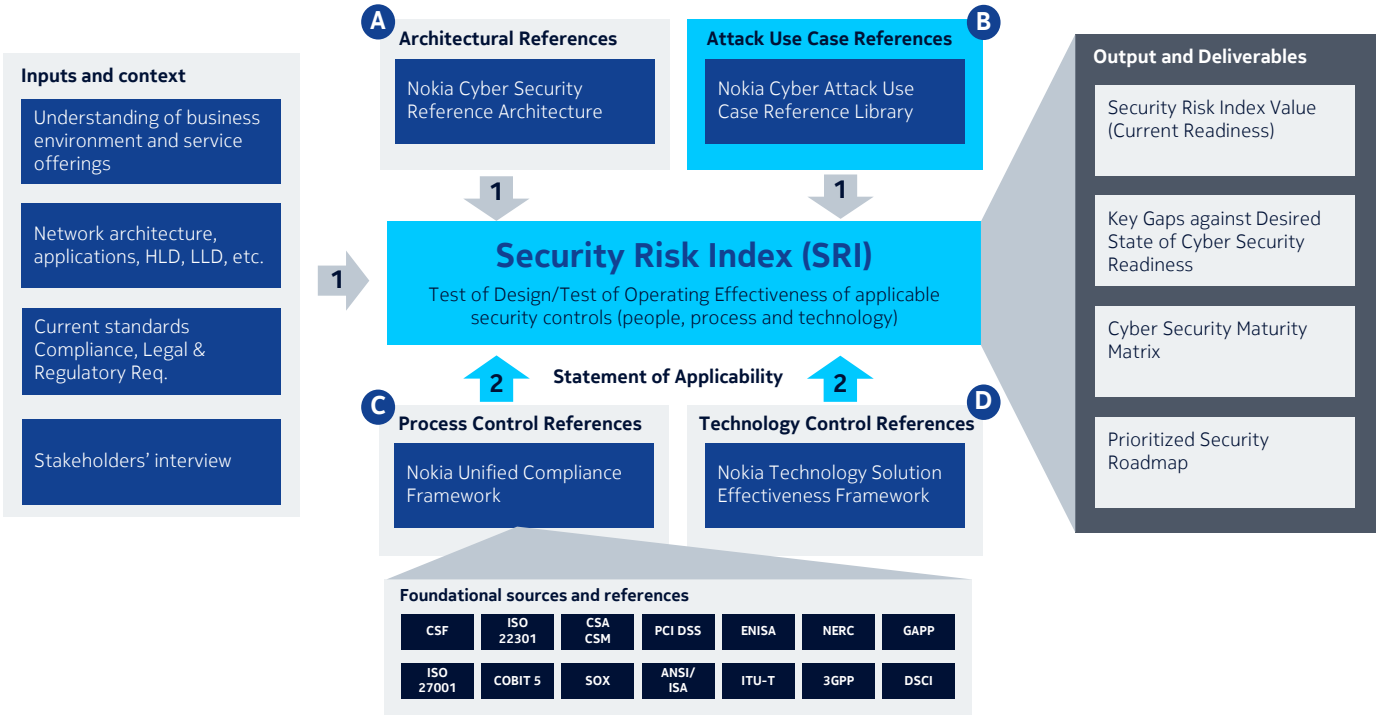

Figure 1. SRI Framework

SRI has three layers – input, processing and output. It starts with the understanding of security requirements in light of business context, study of the existing capabilities and the compliance mandates. It then uses the enabling tools (as stated below) to identify the 'statement of applicability' to do the test of design of applicable controls and test of their operating effectiveness.

3.1. Nokia Cyber Security Reference Architecture: This covers the different building blocks of cyber security framework.

3.2. Nokia Cyber Security Attack Use Case Library: This constitutes the library of cyber-attack use cases at different layers of communication stack.

3.3. Nokia Unified Compliance Framework (UCF): This is the aggregation of various information security standards which are applicable globally. It combines all the standards and converts the same into unique set of security controls.

3.4. Nokia Technology Solution Effectiveness: This covers the baseline technology features and the associated processes/services, which are required to make any technology solution complete.

3.1. Nokia Cyber Security Reference Architecture

Nokia cyber security reference architecture is a cohesive security design comprising of different building blocks, which are required to build an effective defense against cyber-security and data privacy threats. It covers strategic alignment of security program with business objectives and also focuses on processes and technologies to help the organization build the defense across multiple layers like network & infrastructure, application, data, identity and access management for applicable attack use cases. It defines the requirement for detection, prevention, response and recovery controls at each layer. It also touches the requirement of safe adoption of disruptive technologies like cloud, big data, etc.

The architecture also talks about data privacy requirements of the ways an organization gathers, uses, discloses, and manages a customer or client's data. It mandates to fulfil legal requirements (wherever applicable) to protect a customer or client's privacy. Security is one of the key components of data privacy controls.

Cyber security and privacy awareness intends to create informed employees who make better data security and privacy protection decisions, both in and out of the office, that lower information security risks to the organization and protect the privacy of clients and customers.

3.2. Nokia Cyber Security Attack Use Case Library

Telecommunication attack cases library covers the security threats which are possible across different telecom technologies –PSTN, 2G, 3G, 4G, LTE and 5G with vital network components. These technologies are broken into various layers like – User, Access, Transmission, Core (circuit-switched and packet switched), Application and Management layers, etc. These layers are further broken into components and are mapped with ITU-T 805.x framework for threat modelling.

Threat modelling process consists, of four phases, as shown below.

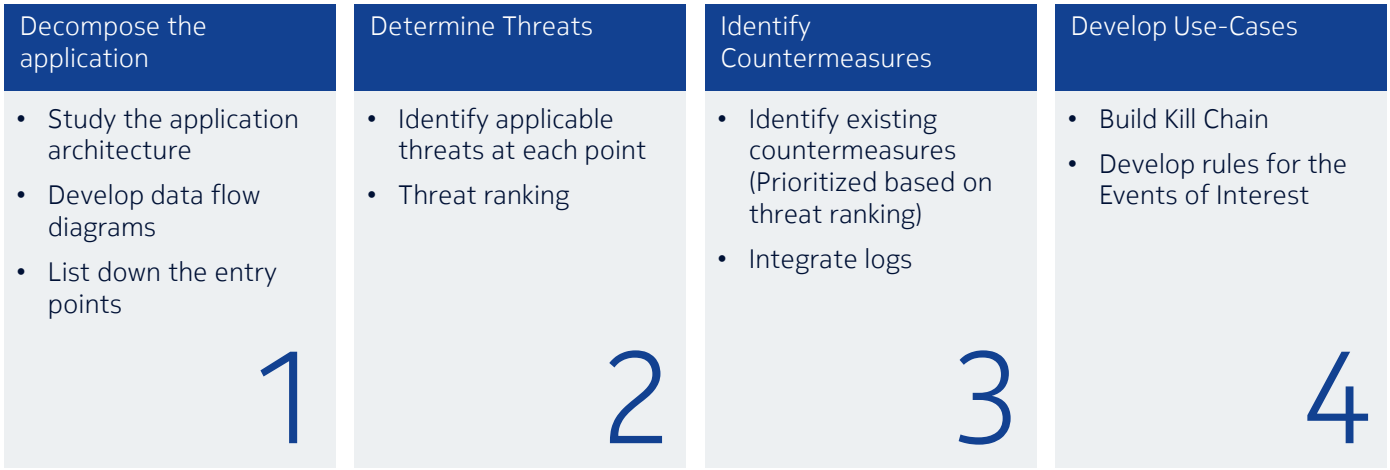

Figure 2. Threat Modelling

1. Decomposing the application – This phase includes the breaking down of the architecture of application/system, including the underlying network and host infrastructure design to create a security profile for it. The security profile is built to uncover vulnerabilities in the design, implementation, or deployment configuration of the application.

2. Determine threats – In this phase, the goals of an attacker are considered, and with knowledge of the architecture and potential vulnerabilities of the application/system, threats that could affect the same are identified.
3. Identify counter measures – Every organization has security controls in place. However, the level and coverage of these controls vary. This phase aims to discover these controls. Any risk assessment performed on this application are taken into account, and also a questionnaire based approach is used to identify what preventive and detective controls have been implemented to counter the threats.
4. Develop Content (Rules, Reports or Dashboards) – Based on the outcome of the previous three phases, EoIs (Event of Interest) are identified, correlation scenarios are developed, chaining of events across the 'Kill Chain' is performed, and the resulting use cases are documented.

3.3. Nokia Unified Compliance Framework (UCF):

Nokia UCF is aggregation of different security standards to form a unique set of security controls, which are mapped with Nokia Cyber Security Reference Architecture. It defines the requirements for control design (ToD) effectiveness and methods to test the operating effectiveness (ToOEf) of each security controls. It also models the maturity state of each security domain based on CoBIT framework.

- Test of design (ToD) effectiveness includes a mix of interviews with personnel, identification of organizations' information security needs, and review of all relevant security documentations to ascertain if the security controls are operated as prescribed, satisfy the company's control objectives and can effectively prevent or detect errors attributable to information security. Process walkthroughs with at least one sample is performed to evaluate design effectiveness;
- Test of operating effectiveness (ToOEf) includes re-performance of the control to determine whether the control is operating as designed and whether the person performing the control possesses the necessary authority and competence to perform the control effectively. Process walkthroughs are performed to evaluate design effectiveness. Collection and assessment of evidences are performed to evaluate operational effectiveness.
- Maturity modelling processes is based on a method of evaluating the organization, so it can be rated from a maturity level among ad-hoc (1), repeatable (2), defined (3), managed & measurable (4) and optimized (5). The maturity levels are designed as profiles of security processes that an organization would recognize as descriptions of possible current and future states.

The statement of applicability of security controls is derived from UCF and it may differ from organization to organization.

3.4. Nokia Technology Solution Effectiveness

Nokia Technology Solution Effectiveness module primarily focuses on three things:

- Technology architecture effectiveness covering different communication layers to cover up the applicable use cases
- Minimum baseline features that the technology architecture shall cover
- Identification and stitching of required services around security products or the technology layer

4. SRI Output

SRI provides 'Quantitative', 'Qualitative' and 'Strategic' output to measure the effectiveness of their security program along with tactical and strategic security roadmap for the organization.

4.1. Quantitative

The unique security controls under Nokia Unified Compliance Framework are categorized under 13 domains. These domains are

1. Security organization and governance
2. Information asset management
3. Security and privacy awareness
4. Data protection
5. Identity and access management
6. Network architecture and security
7. Data privacy
8. Software and application security
9. Third party security
10. Threat and vulnerability management
11. Incident and problem management
12. Security operations and monitoring
13. Security aspect of business continuity planning and disaster recovery

SRI provides domain-wise and overall score to reflect the level of compliance.

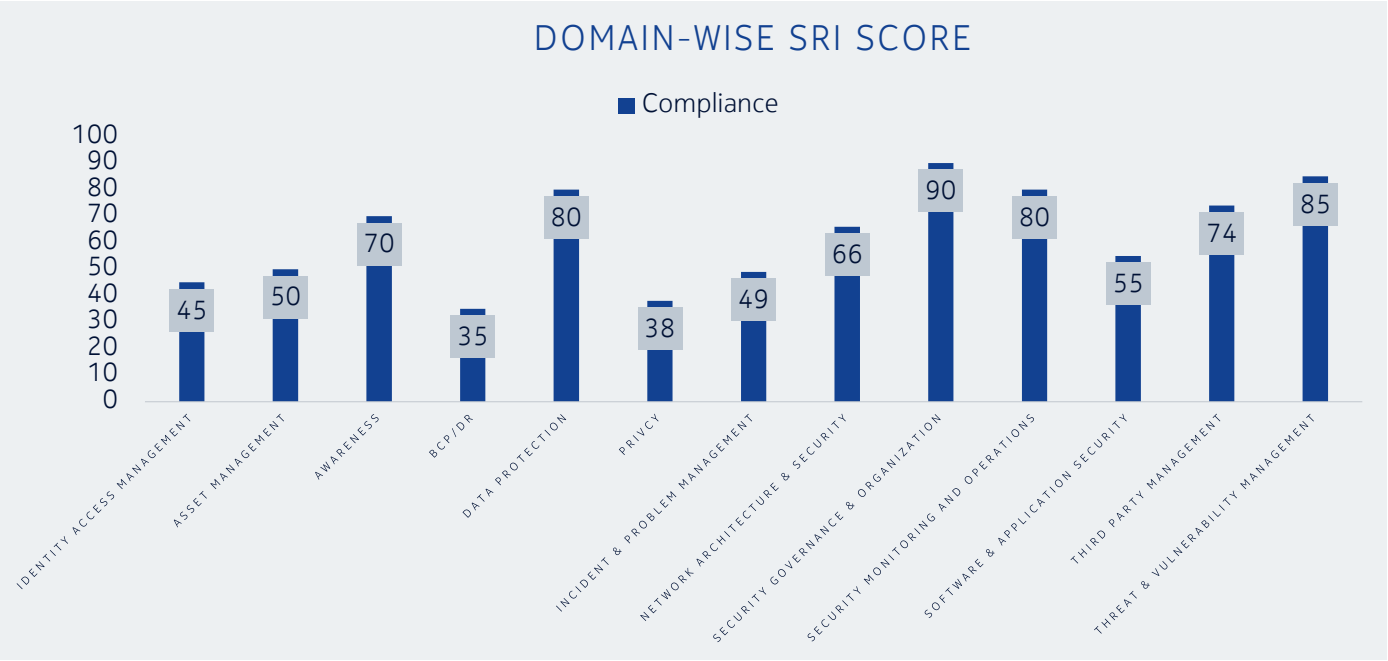

Figure 3. SRI Score – Domain-wise

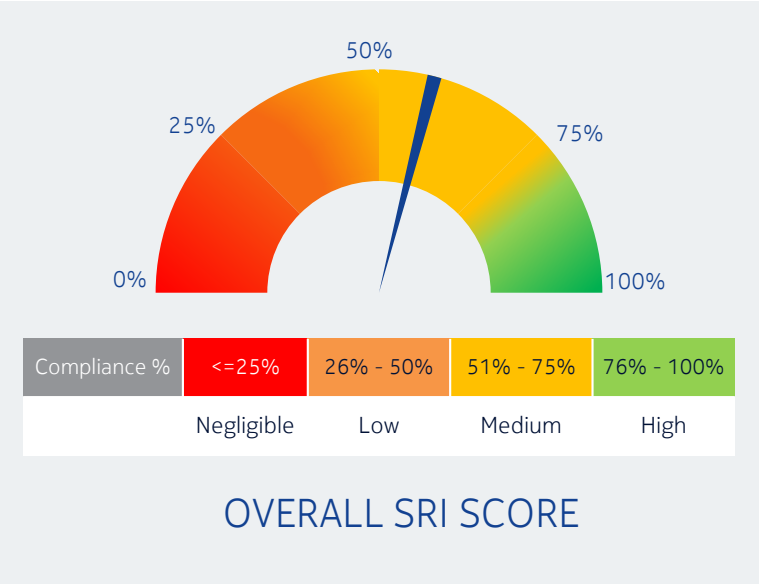

Figure 4. SRI Score – Overall

4.2. Qualitative

Maturity modelling for management and control over security processes is based on a method of evaluating the organization, so it can be rated from a maturity level of ad-hoc (1) to optimized (5). The maturity assessment model has been derived from CoBIT framework. The maturity levels are designed as profiles of security processes that an organization would recognize as descriptions of current and future states.

Using the maturity models developed for each security domain, management can identify:

- The actual performance of the organization—Where the organization is today
- The current status of the industry—The comparison
- The organization's target for improvement—Where the organization wants to be
- The required growth path between 'as-is' and 'to-be'

This will help to make the results easily usable in management briefings, where it is presented as a means to support the business case for future plans. The advantage of a maturity model approach is that it is relatively easy for management to place itself on the scale and appreciate what is involved if improved performance is needed.

The 1-5 scale is based on a simple maturity scale showing how a process evolves from a non-existent/ ad-hoc capability to an optimized capability.

L1- Initial

There is evidence that the organized has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

L2- Repeatable

Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

L3-Defined

Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.

L4- Managed & Measurable

Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

L5- Optimized

Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Figure 5. Maturity Levels

4.3. Strategic

Although a properly applied capability already reduces risks, an organization still needs to analyze the controls necessary to ensure that risk is mitigated and value is obtained in line with the risk appetite and business objectives. The continued analysis introduces new actions. The strategic output consolidates these actions to define a roadmap for an organization to move from the ‘current state’ to the ‘desired state’.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code SR1706012949EN