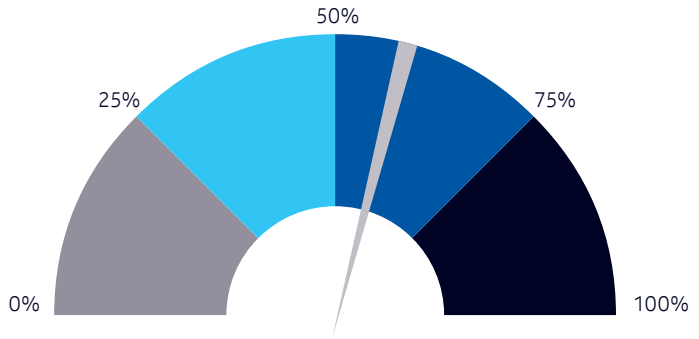
Security Risk Index (SRI)

Security Risk Index (SRI) is a unique security assessment framework to measure the organization's readiness against relevant security threats (both internal and external) and meeting legal, regulatory and compliance mandates attributable to information security in the 5G and Industry 4.0 era. It has been designed to support organizations in their journey of security governance, risk and compliance management.



OVERALL SRI SCORE

Compliance%	<=25%	26%-50%	51%-75%	76%-100%
	Negligible	Low	Medium	High

Security concerns prior 5G service introduction?

Nokia's SRI provides clear, quantified inputs for decisions necessary for adapting existing security posture to 5G requirements

Product overview

Digital transformation in the 5G and Industry 4.0 era has led to significant cybersecurity implications in Operational Technology (OT) and IT environment of CSPs and verticals. It is thus essential for them to carry out periodic security risk assessments of their telecom infrastructure and cover all critical layers such as network and infrastructure, applications, data, identity and access, and processes. The risk assessment must also cover the core telecom technologies including 2G, 3G, 4G/LTE and 5G, Fixed line for example and the associated layers such as Radio Access Network, Transmission Network, 5G NG Core, Evolved Packet Core, IMS, Management and Orchestration, etc. The risk assessment methodology should include security maturity assessment. 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 Security Risk Index (SRI) has been designed 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.

Organization benefits

Holistic risk assessment for both enterprise and telecom infrastructure against Nokia's exhaustive cyber-attack use case library

Continuous awareness on key security gaps related to processes, technologies and skill-sets.

Effective compliance to legal, regulatory and privacy requirements

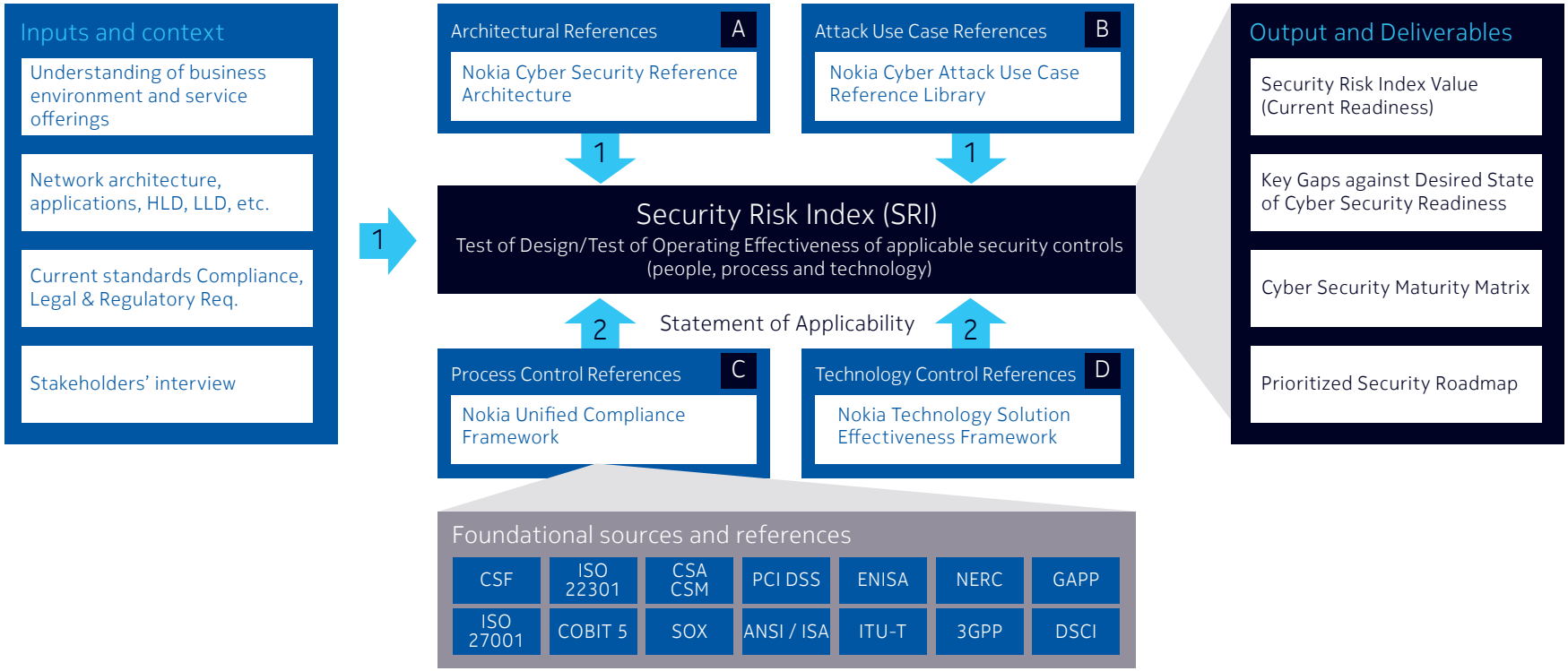
Complete visibility on operating effectiveness of security controls within the organization

Access to industry and domain experts for risk assessment

Tactical and strategic roadmap for cyber-security

Bridging design gaps at process and technology layers

Security Risk Index (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.

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

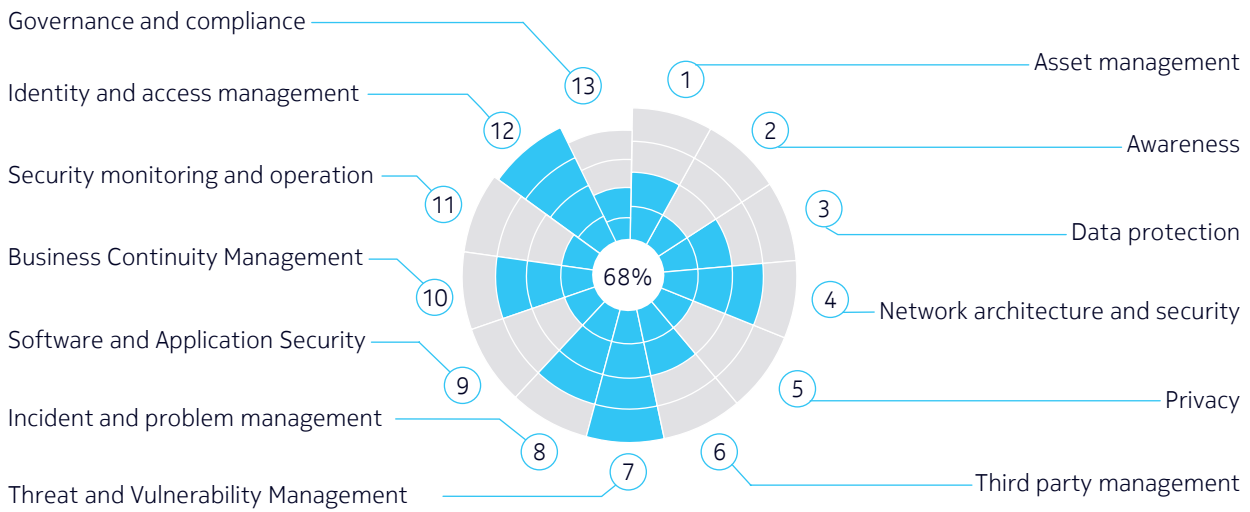
B. **Nokia Cyber Security Attack Use Case Library:** This constitutes the library of security-attack use cases applicable to an organization.

C. **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.

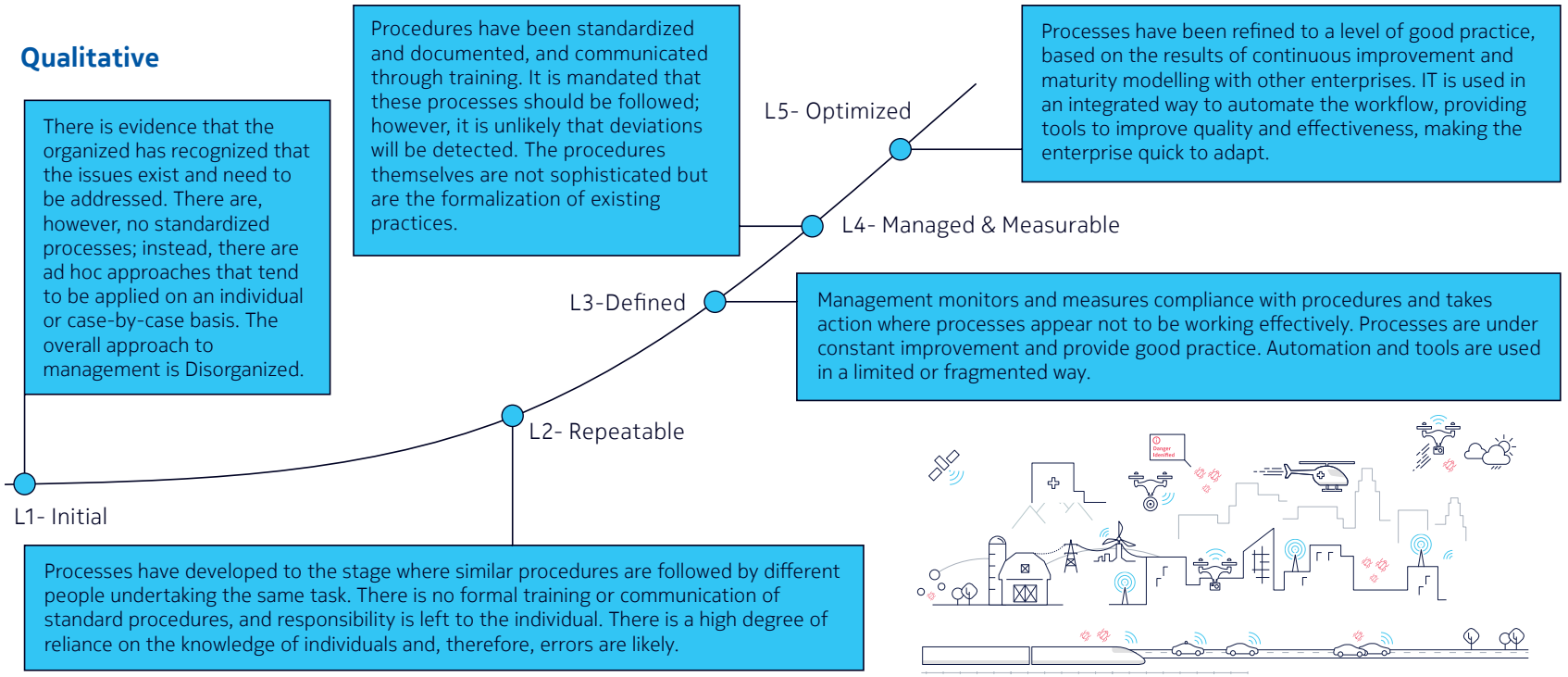
D. **Nokia Technology Solution Effectiveness:** This covers the baseline technology features and the associated processes/ services, which are required to make any technology solution complete.

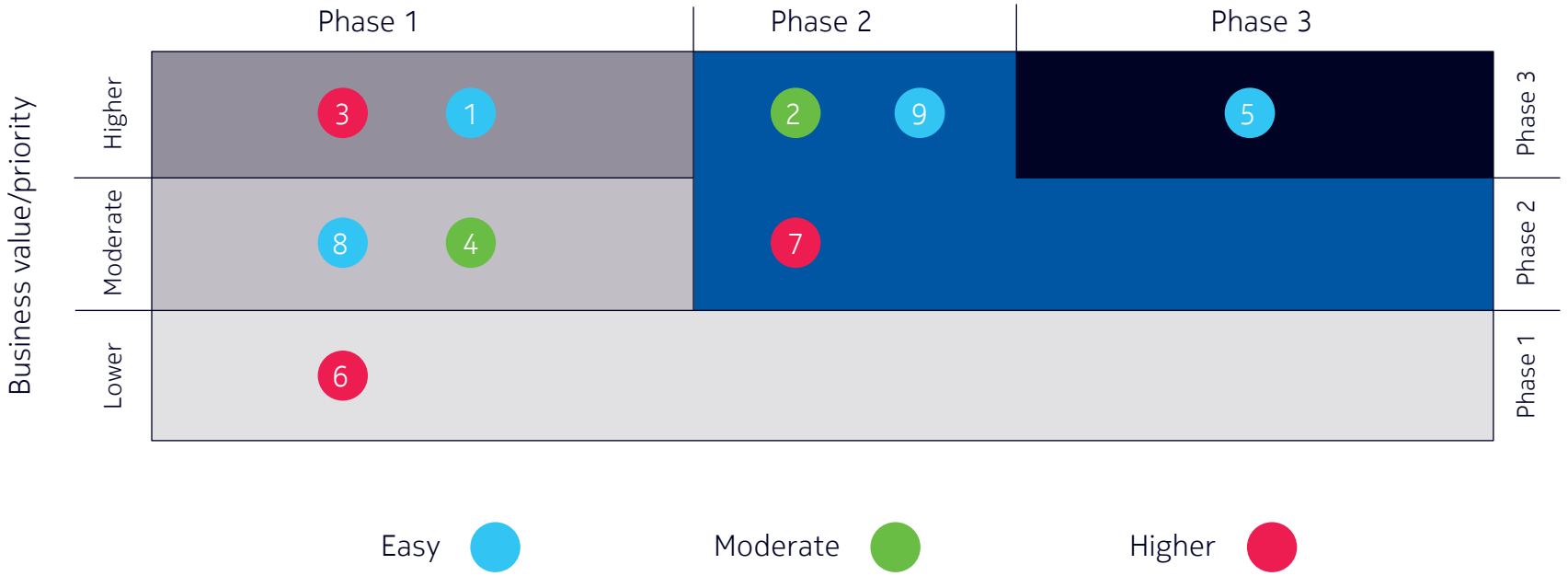
SRI provides 'Quantitative', 'Qualitative' and 'Strategic' output to measure the effectiveness of their security program along with tactical and strategic security roadmap for the organization.

Quantitative



Qualitative





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'

SRI Execution Models

1. Test of design effectiveness (Basic Model): Review of all information security management system across all 13 domains to ascertain if the security controls are designed effectively, satisfy the company's control objectives and can effectively prevent or detect errors attributable to information security. Process walkthroughs with at least one sample will be performed to evaluate design effectiveness. This includes limited vulnerability assessment and security configuration testing.
2. Test of operating effectiveness (Advanced Model): Re-performance of the control to determine whether the control is operating as designed and whether the security architecture is being designed and managed effectively to meet the desired objectives. Process walkthroughs are performed to evaluate design effectiveness. Collection and assessment of evidences from significant samples are performed to evaluate operational effectiveness. This includes exhaustive vulnerability assessment, penetration testing and security configuration testing.

SRI – Key Features

a. Understanding of environment:
   i. Network architecture
   ii. Existing security infrastructure across all communication layers – network, infrastructure, application, data, identity & access management, monitoring & response, etc.
   iii. Existing security control framework
   iv. Legal, regulatory and compliance mandates attributable to security
   v. Functional security requirements

b. 'Statement of Applicability' of security controls
   i. Identification of unique set of security controls applicable to an organization
   ii. Aligning security controls with global best practises

c. Threat modelling for critical information assets

d. Test of design and Test of Operating Effectiveness of applicable security controls in line with applicable threats and use cases

e. Identification of cyber-attack/ security attack use cases

f. Vulnerability assessment/ penetration testing

g. Cyber-security readiness score (AS-IS status)

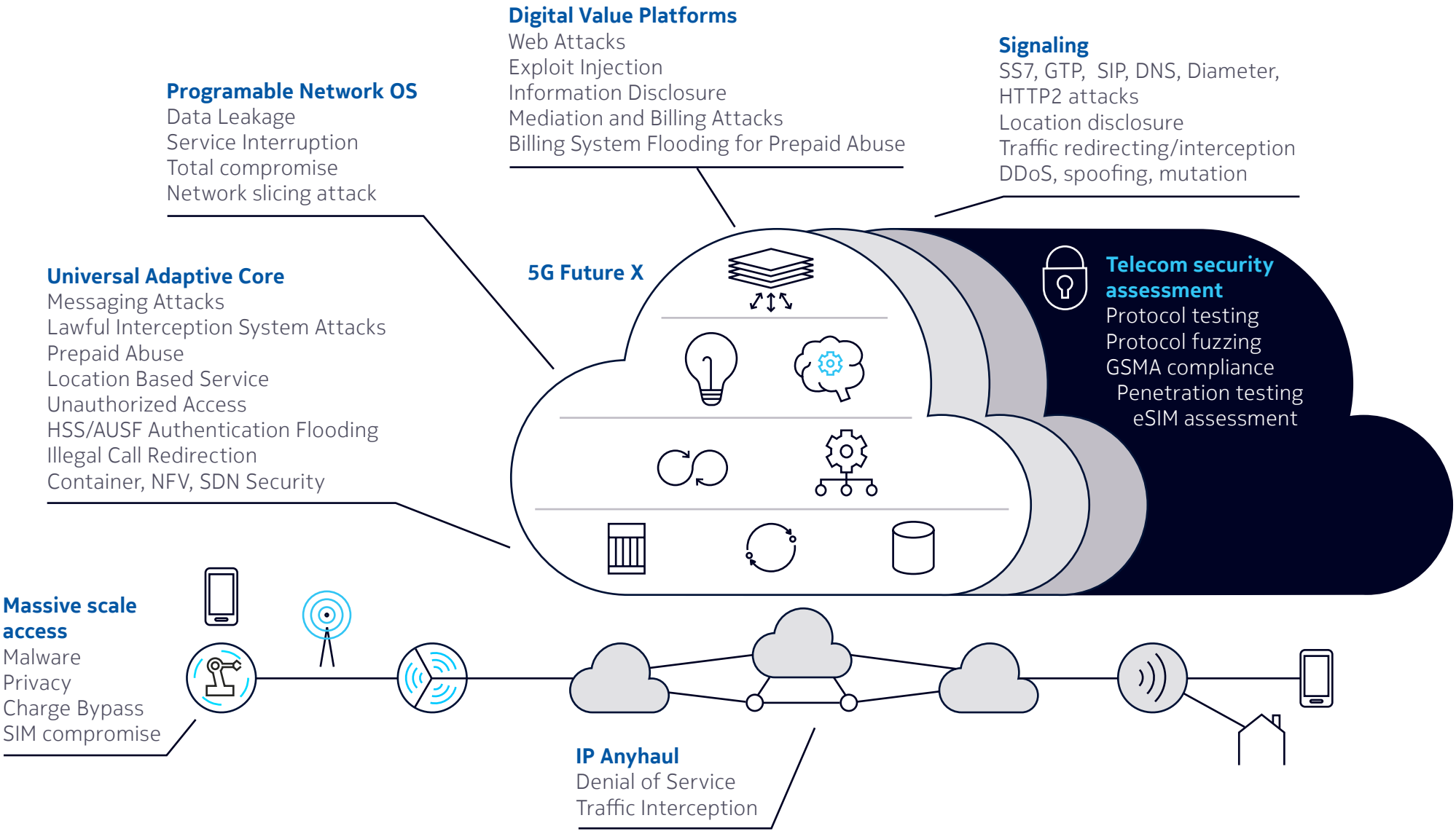
h. Identification of key gaps with respect to processes, technology and skill-sets

i. Cyber security maturity score (current state and desired state)

j. Top 10 recommendations to move from current state to desired state (TO-BE status)

k. Continuous risk governance

Advanced Telecom Security Assessment



Nokia Oyj
Karaportti 3
02610 Espoo
Finland

CID: 201993
Product code SR2007045390EN

www.nokia.com
www.nokia.com/networks/services/managed-security-services/

About Nokia
Nokia is a global leader in the technologies that connect people and things. Powered by the innovation of Bell Labs and Nokia Technologies, the company is at the forefront of creating and licensing the technologies that are increasingly at the heart of our connected lives.

With state-of-the-art software, hardware and services for any type of network, Nokia is uniquely positioned to help communication service providers, governments, and large enterprises deliver on the promise of 5G, the Cloud and the Internet of Things. **http://nokia.com**