SUPPLY CHAIN INTEGRITY AND SECURITY ASSURANCE FOR ICT

Mats Nilsson

THE STARTING POINT

2 B INTERNET USERS

85% POPULATION COVERAGE

5+ B MOBILE SUBSCRIPTIONS

10 YEARS OF DAILY UPLOAD

E-BOOKS SURPASSING PRINT SALES
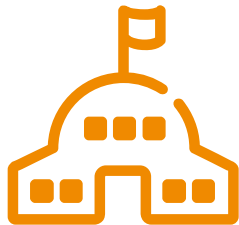
200.000 SMS EACH SECOND

CYBERSECURITY AND MOBILITY

CYBER SECURITY PERSPECTIVES

OPERATORS OF
INFRASTRUCTURE

REGULATIONS & STANDARDS

INFRASTRUCTURE VENDORS

THREATS & RISKS

THREATS AND RISKS

› User behavior

› Malicious threats

› Devices and applications

› Mobile device, application and content management

› Machine to Machine networks

› Emerging areas:
- Cloud, HetNets, Big Data

THREATS & RISKS

COMPLEX AND RAPIDLY EVOLVING ENVIRONMENT

OPERATOR OF INFRASTRUCTURE

› Business and Society is highly dependent of Mobile Networks

› Secure resilience to cyber incidents

  – Harden infrastructure

  – Improve ability to defend

  – Recover quickly – business continuity

INFRASTRUCTURE OPERATORS

MANAGE CONDITIONS AND CONSEQUENCES OF CYBER RISKS

VENDOR OF INFRASTRUCTURE

› Product Security Properties

› Security assurance in product development and supply chain

› Security in Network Deployment and Operations

› Pro-active industry Collaboration

INFRASTRUCTURE VENDORS

ENABLER

FOR

REDUCING RISKS

AND IMPROVING

RESILIENCE

SECURITY TRENDS (I)

new devices

new communication patterns

new applications

new networks

HetNet/SDN

mobile broadband

cloud

and

big data

SECURITY TRENDS (II)

NETWORK

Network evolution to mobile broadband
Network is critical infrastructure for consumers, business and public services

DEVICES

Devices:
Phones transforming into computers and entertainment

APPLICATIONS

Applications:
Mobile malware, e-payment attacks, botnets

CONTENT
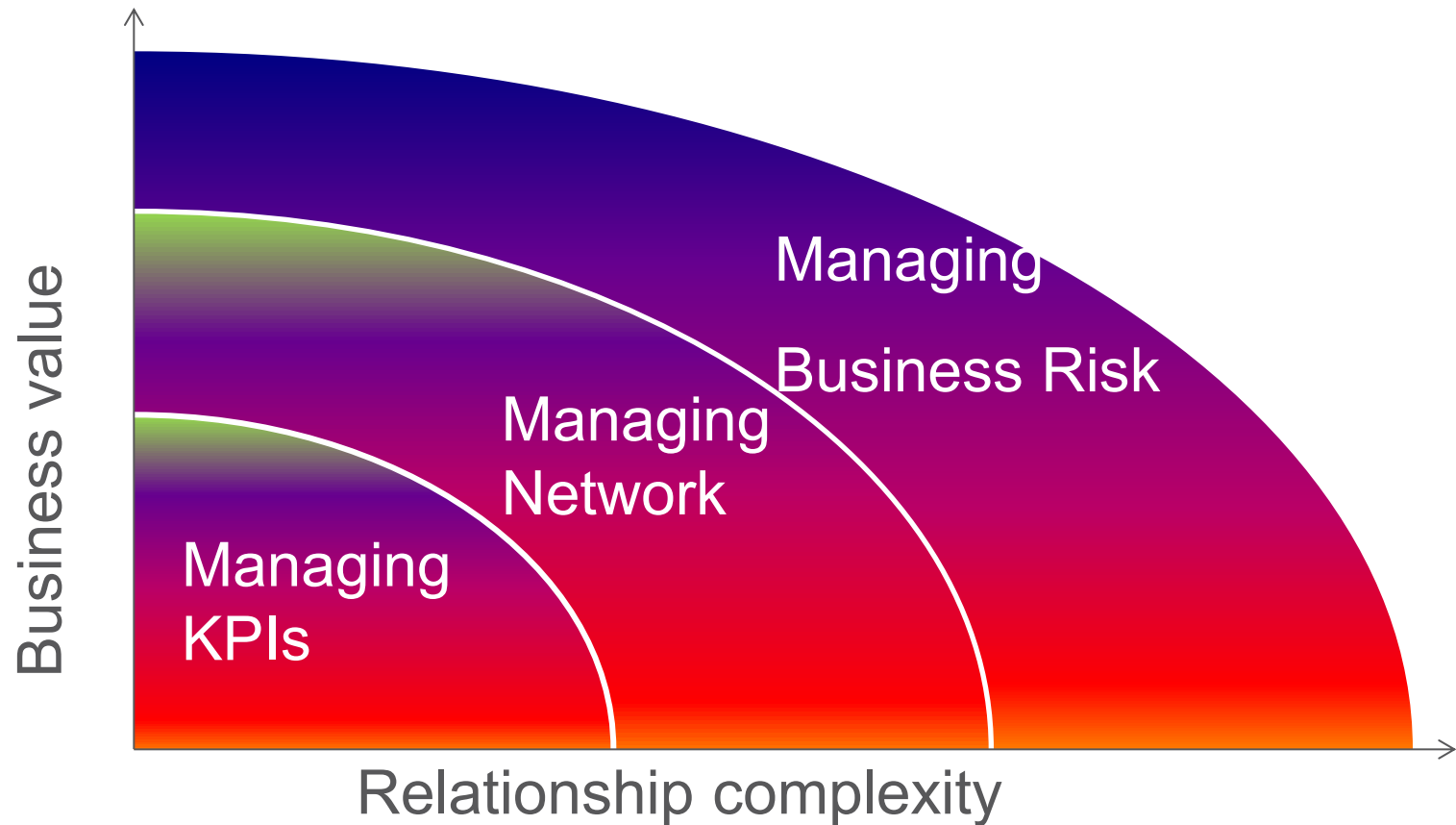
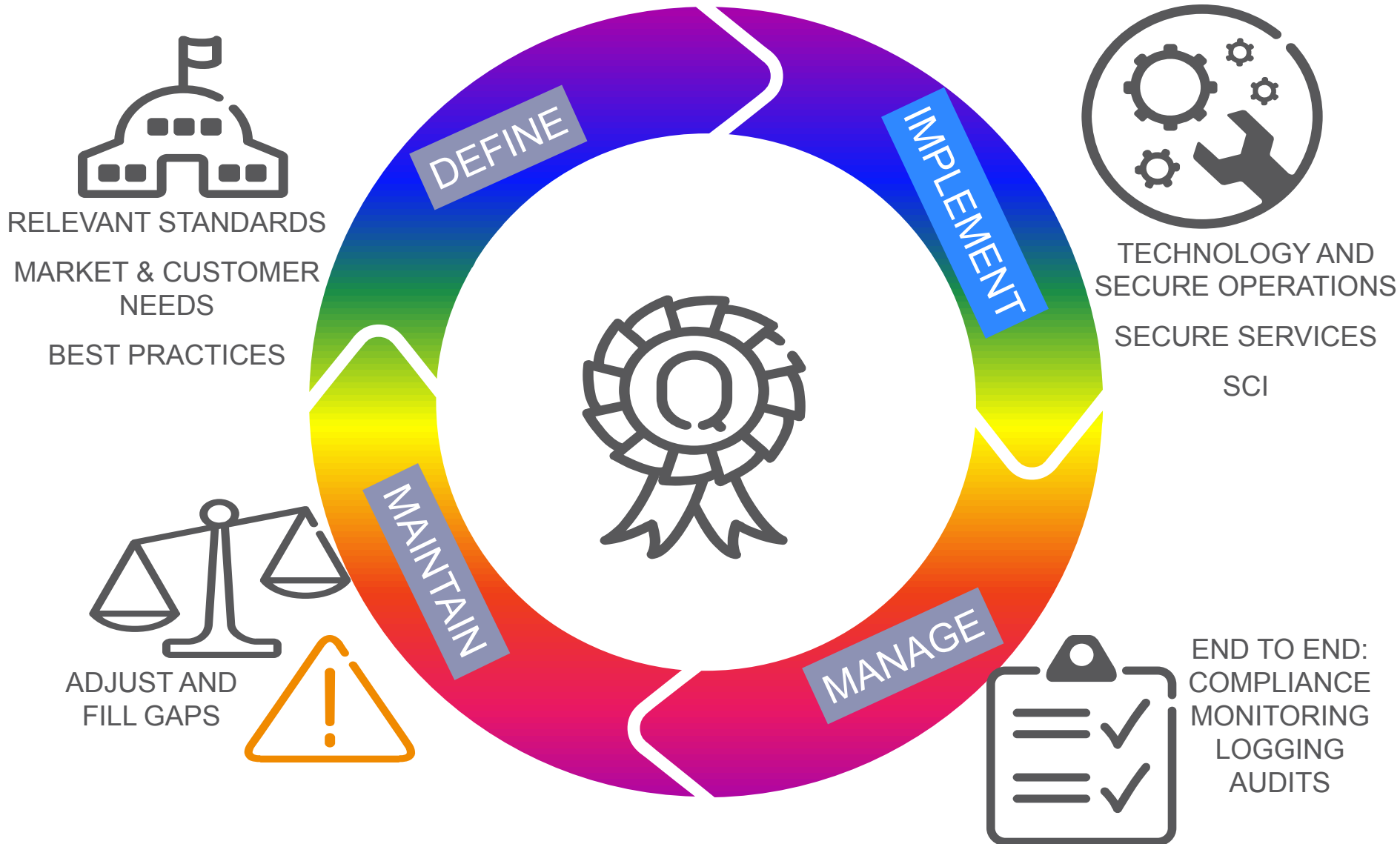Content:
Secure storage, transmission and sharing

TECHNOLOGY

Technology:
Open source software
Cloud and Big Data analytics

EVOLVING TO MEET CUSTOMER EXPECTATIONS

Managing Business Risk

Managing Network

Managing KPIs

Business value

Relationship complexity

Trust is gained by a systematic approach to threats across the whole environment, including SCI

ERICSSON APPROACH ON SECURITY

RELEVANT STANDARDS

MARKET & CUSTOMER NEEDS

BEST PRACTICES

DEFINE

IMPLEMENT

TECHNOLOGY AND SECURE OPERATIONS

SECURE SERVICES

SCI

MAINTAIN

ADJUST AND FILL GAPS

MANAGE

END TO END: COMPLIANCE MONITORING LOGGING AUDITS

OUR PERSPECTIVE

IMPROVE RESILIENCE

› Secure network infrastructure to be more resilient

› Work with operators to maintain business optimal security in their networks

› Industry guidance through standards and best practices

› SCI part of risk assessment and mitigation through appropriate controls (similar to own R&D)

REDUCE CYBER SECURITY RISK

› Daily co-operation and collaboration via CERT community to improve ability to defend and recover

FUTURE DIRECTIONS

REDUCE CYBERSECURITY RISK

➢ Leadership in the industry ecosystem: networks, devices, applications
➢ Collaboration in regulations, standards and industry bodies

IMPROVE NETWORK RESILIENCE

➢ Secure network infrastructure for resilience
➢ Work with operators to maintain security in their networks

EDUCATION & COMMUNICATION

➢ Educate and communicate with users
➢ Anticipate threats and develop innovative solutions