ENISA and European Standardization Organizations Event Feb.2nd-Feb.4th 2021

Day 3 – Panel 5
Situation on the standardization of 5G cybersecurity

Francois Zamora, Orange,

Afnor's France Head of Delegation at the ISO/IEC JTC1 SC27

Topics

- 5G security: is this topic addressed within ISO/IEC JTC 1 SC 27?

- What are the current and future considerations? Is there a need to cooperate with other SDOs in that respect?

- From a telecom company perspective, what would be the benefit of having a certification schemes on 5G security?

5G, 5G operation, 5G use cases imply complex systems

Figure 3: Generic 5G Architecture

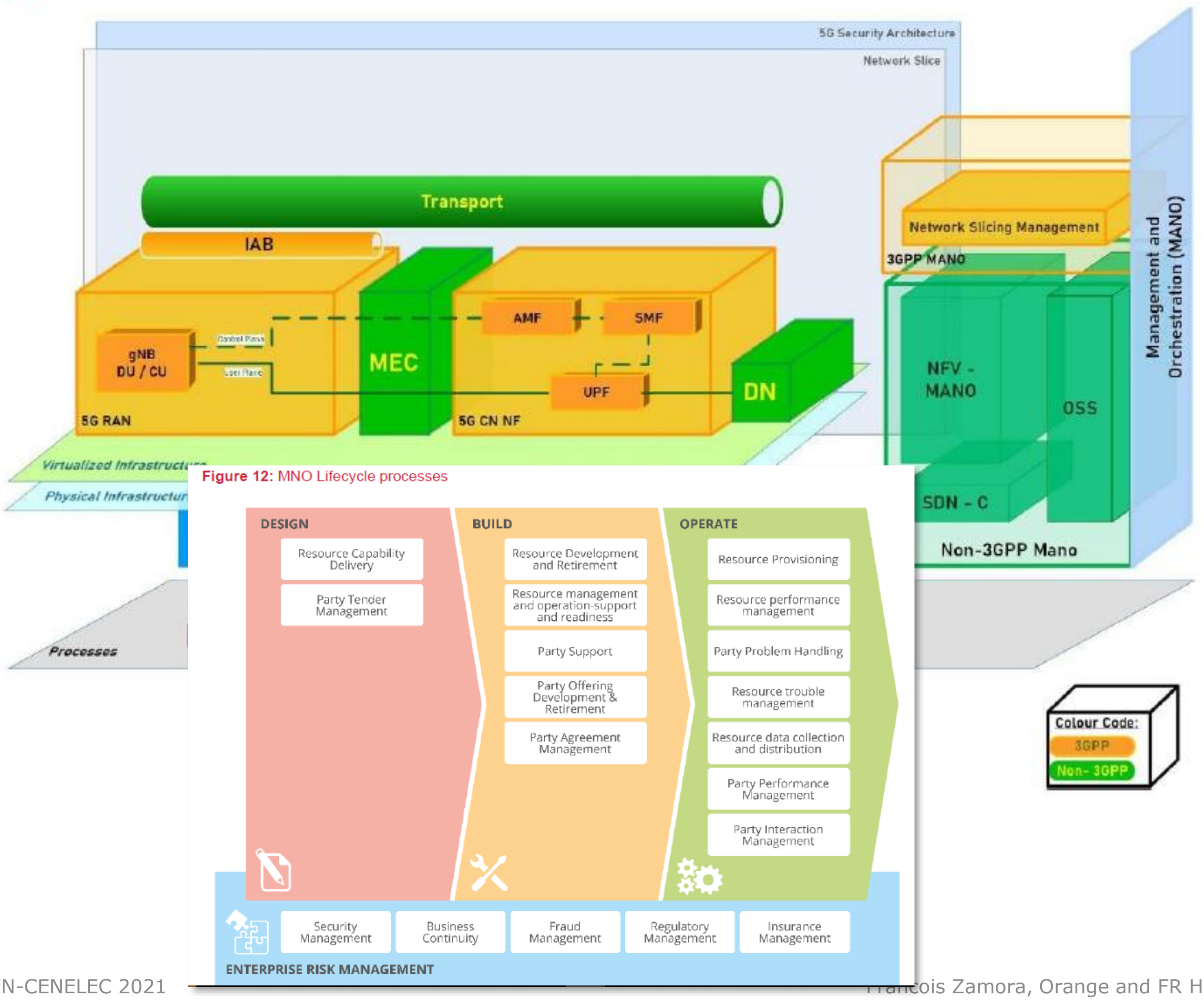


Figure 12: MNO Lifecycle processes

DESIGN
- Resource Capability Delivery
- Party Tender Management

BUILD
- Resource Development and Retirement
- Resource management and operation-support and readiness
- Party Support
- Party Offering Development & Retirement
- Party Agreement Management

OPERATE
- Resource Provisioning
- Resource performance management
- Party Problem Handling
- Resource trouble management
- Resource data collection and distribution
- Party Performance Management
- Party Interaction Management

ENTERPRISE RISK MANAGEMENT
- Security Management
- Business Continuity
- Fraud Management
- Regulatory Management
- Insurance Management

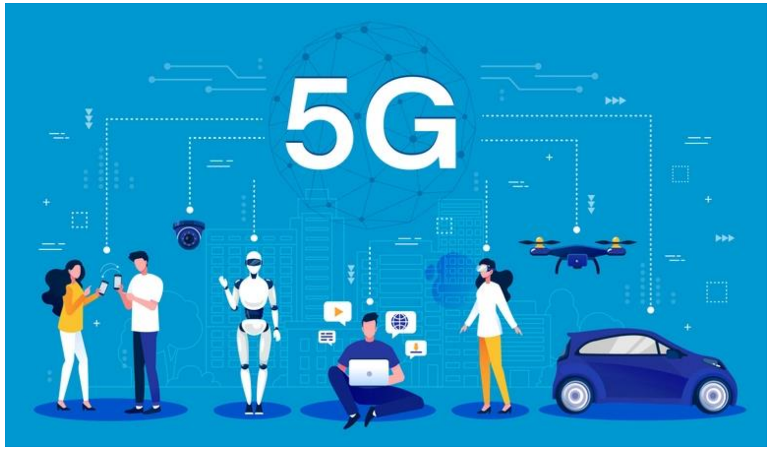


Figure 4: Core network architecture Zoom-in

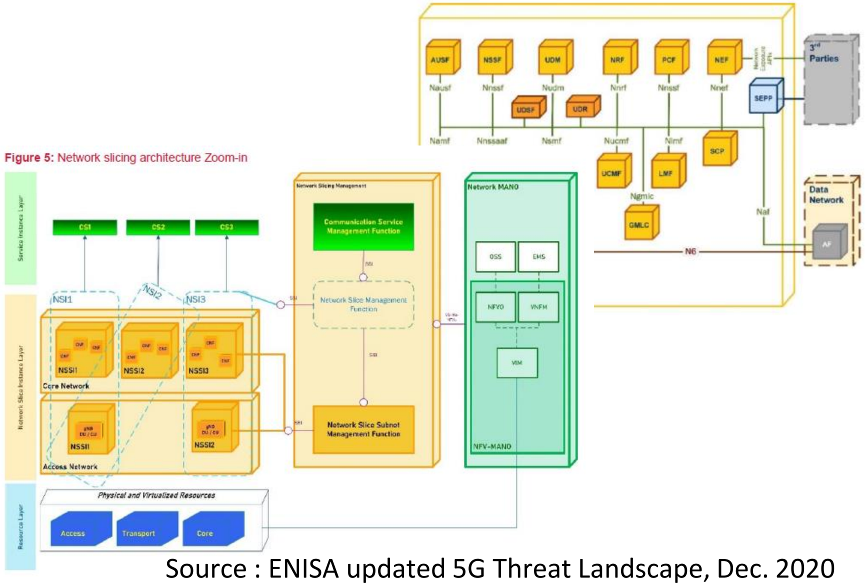
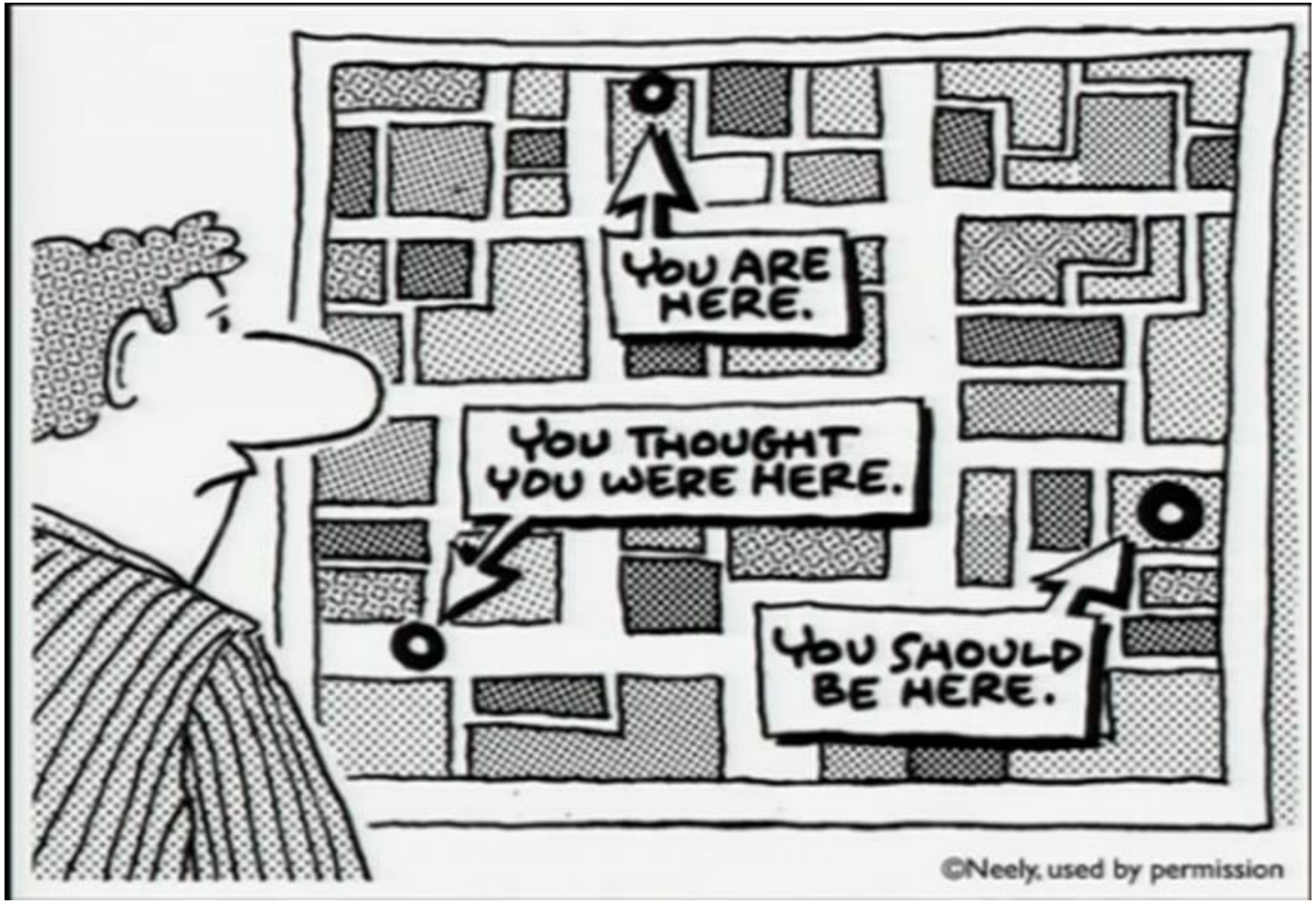


Figure 5: Network slicing architecture Zoom-in

Source : ENISA updated 5G Threat Landscape, Dec. 2020

How to deal with 5G security complexity? Any relevant options for 5G cybersecurity certification?



Takeways 1/2

- A sound basis to address 5G security keeps valid from ISO/IEC JTC 1 SC 27 frameworks
  1. Risk management framework keeps with ISO/IEC 27005
  2. Continuous improvement should rely on ISO/IEC 27001
  3. State-of-art of Statements of Applicability must include Security Monitoring and Response (ISO/IEC 27035)
  4. Mapping to ISO/IEC 27033-7 of VNF security capabilities should be explored

- 5G sub-domains Cybersecurity Certification should consider 2 schemes:
  1. Pan-European 5G cybersecurity risk homologation “Substantial” to match Industries needs, at “High” to match Member States needs (on specific sub-domains),
  2. Pan-European 5G Vendors cybersecurity certification with “Basic” to enable a first-level of system hardening and integration

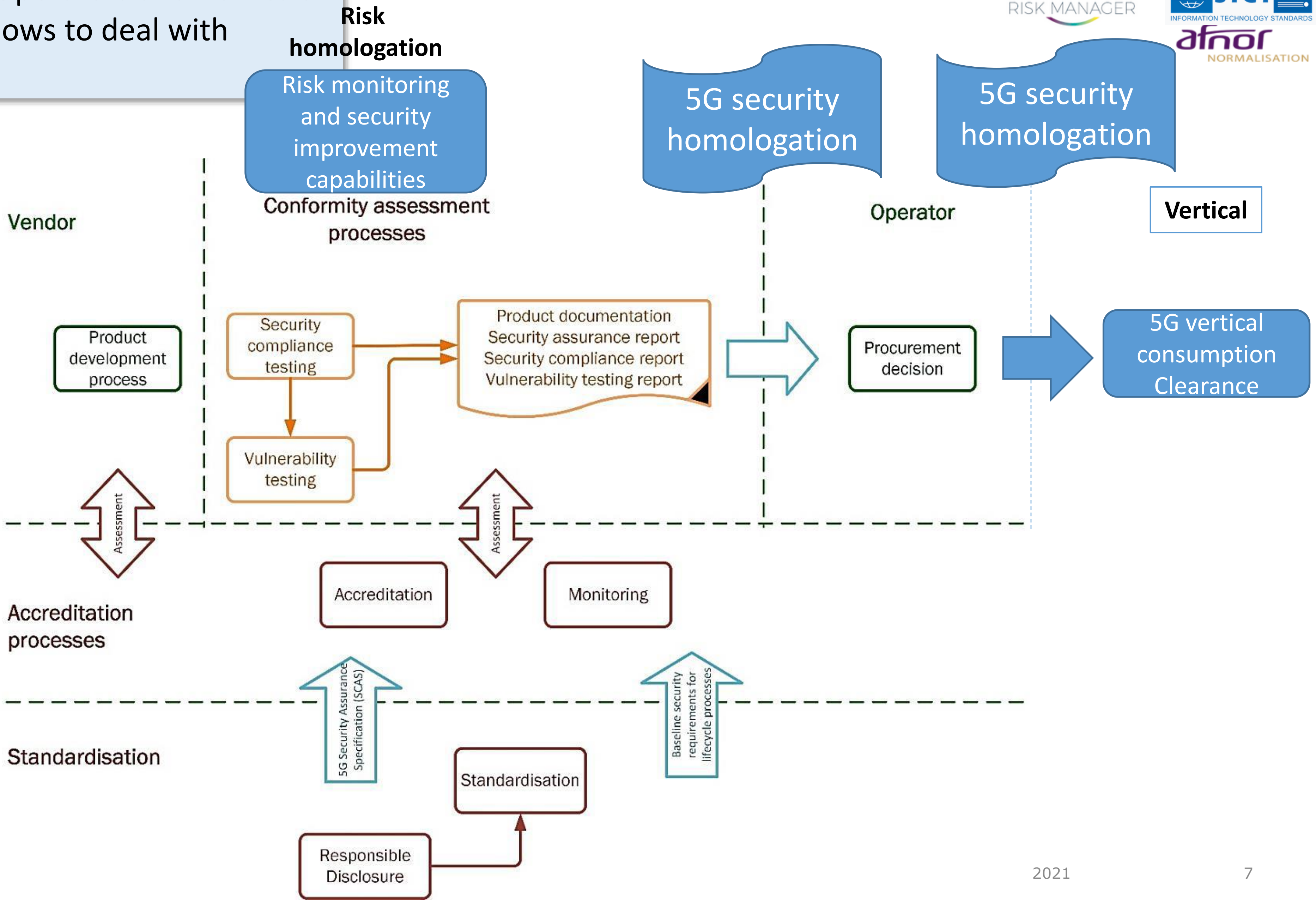
Takeways 2/2

- What role for ISO, IEC, CEN and CENELEC with regards to 5G standardization?

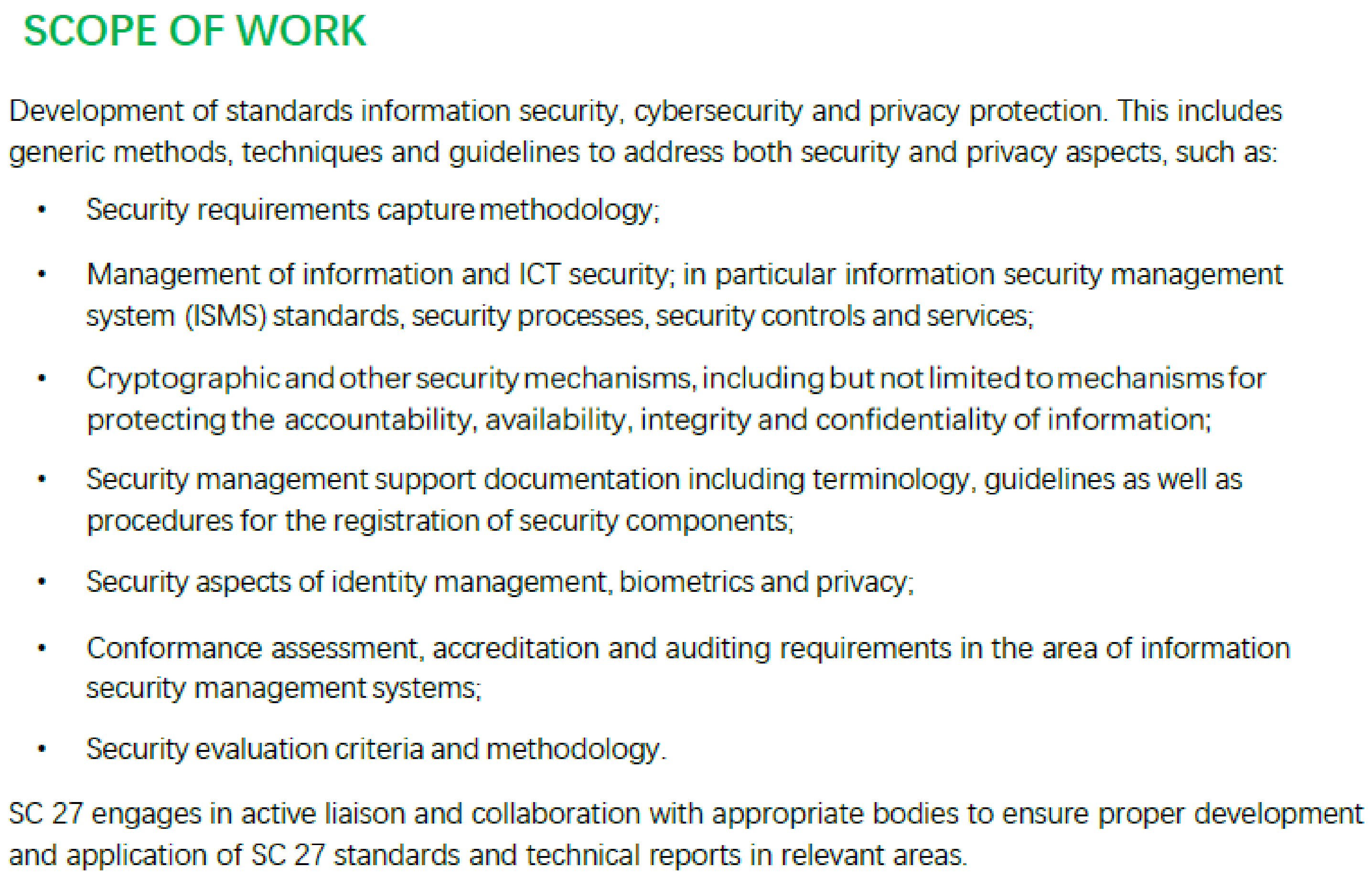
1. ENISA's 5G Threat Landscape could be transferred in a European Standard
2. 5G risk likelihood evaluation should rely on EBIOS Risk Manager and Kill Chain™ knowledge bases relying on technical works from 3GPP and ETSI
3. Foster an homologation approach of 5G cybersecurity risks
4. Coordinate with Member States to define a pan-European « High » for relevant 5G sub-domains
5. Coordinate with industries to make NIS2-compliant « Substantial »
6. Standardize methodologies for real-time risk likelyhood evaluation leveraging on Big data and AI
7. Standardize knowledge bases of threats and threat detection techniques leveraging on CERTs observations

Proposal 1 :
5G cybersecurity certification for Operators and Verticals based on 5G risk homologation allows to deal with systems complexity

Proposal 2 :
5G cybersecurity certification for Vendors :
« Basic » based on 3GPP Approach NESAS/SCAS


Risk homologation
Risk monitoring and security improvement capabilities
5G security homologation
5G security homologation
Vertical
Vendor
Conformity assessment processes
Operator
Product development process
Security compliance testing
Vulnerability testing
Product documentation
Security assurance report
Security compliance report
Vulnerability testing report
Procurement decision
5G vertical consumption Clearance
Assessment
Assessment
Accreditation
Monitoring
Accreditation processes
5G Security Assurance Specification (SCAS)
Baseline security requirements for lifecycle processes
Standardisation
Standardisation
Responsible Disclosure

Annex - ISO/IEC JTC 1 SC 27 areas



SCOPE OF WORK

Development of standards information security, cybersecurity and privacy protection. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management system (ISMS) standards, security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure proper development and application of SC 27 standards and technical reports in relevant areas.

Source: SC27, Standing Document 11, 2020