

5G-TACTIC

5G Trusted And seCure network servICes

5G-TACTIC Security Assurance Methodology in 5G and beyond Ecosystems

Presenter: Ioanna Mesogiti

OTE – Hellenic Telecommunications Organization S.A.

Senior R&D Engineer

5G-TACTIC Training Workshop

“Regulatory aspects of 5G networks
Cybersecurity and Trust”

26 May 2026

What Is a Security Assessment Methodology?

A Security Assurance Methodology defines the processes, controls, and evaluation mechanisms used to assess, validate, and maintain the security and resilience of systems throughout their lifecycle.

Mobile Networks' Past and New Security Threats



- **Inherited Threat Landscape:**
 - Legacy 4G/early 5G NSA threats persist, incl. signaling attacks, IMSI catching, RAN jamming/ Denial-of-Service at the radio interface, etc.
- **Expanded Threat Landscape:**
 - **Increased Complexity:** 5G architecture with Virtualization (NFV), Software-Defined Networking (SDN) and Open-RAN, Mobile Edge Computing, significantly expands the potential attack surface compared to existing 4G/ 5G NSA networks.
 - **Multi-Stakeholder Ecosystem emerging:** Security is a shared responsibility among a diverse group of actors.

Main Existing Standards and Frameworks

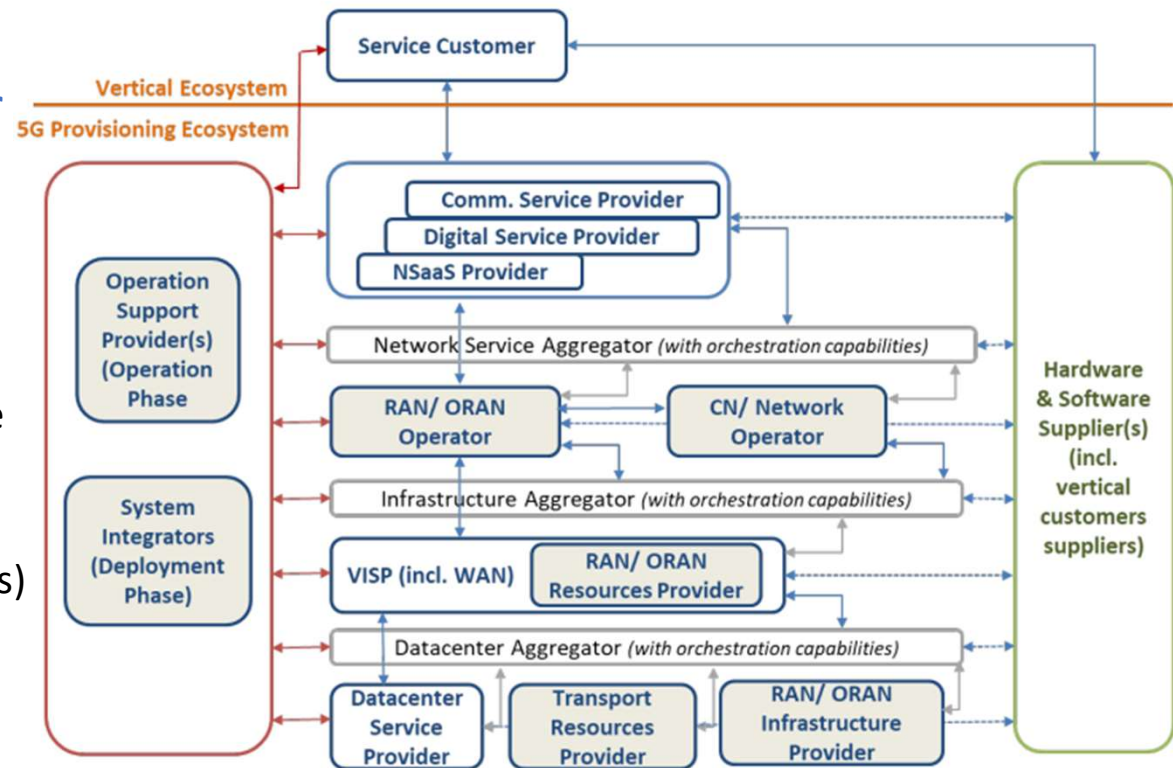


- **Existing standards and frameworks**
 - **Key 3GPP Specifications:** Especially:
 - **SECAM (TR 33.916):** The core methodology for security assurance.
 - **SCAS (TS 33.511+):** SA Specs for all major network components, incl. CN Functions (AMF, SMF, UPF) and the gNodeB.
 - **TS 33.501:** The foundational Security Architecture for the 5G System.
 - **EU Regulatory Alignment:** Key EU directives and guidelines, including **the EU 5G Toolbox, Cybersecurity Act (CSA), and NIS-2 Directive.**
 - **ENISA's recommendation for Risk Management Approach:** to follow the ISO 27005 standard for risk assessment and management, ensuring a structured and internationally recognized process.
 - **GSMA's guidelines:** especially focused on the CN domain (authentication, slicing, SBA, VAS, applications like MCX that could be integrated with Core components)

5G and Beyond Ecosystem & Stakeholders

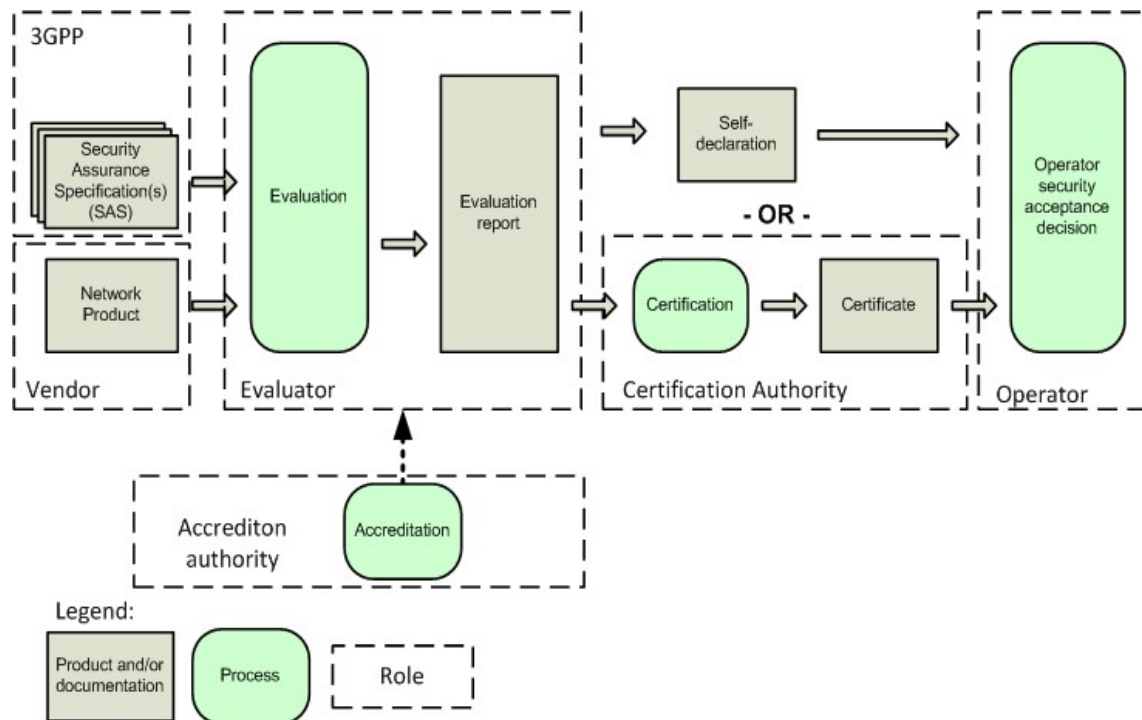
5G and beyond (5G/B5G) ecosystems can be dynamic, multi-layered environment to be shaped differently per market/ country/ area etc.

- **Shift from Hardware to Software:** Transition from closed HW-based platforms to open SW-based systems.
- **New Roles & Stakeholders** beyond traditional Mobile Network Operators (MNOs), including:
 - Infrastructure Providers
 - Virtualisation Infrastructure Service Providers (VISPs)
 - Digital Service Providers (DSPs)
- **Expanded Attack Surface:** The increased number of stakeholders and open interfaces creates more potential entry points for malicious actors.



The Security Assurance Methodology needs to take the environment into consideration and adapt to market/ country/ area 5G ecosystem formulation.

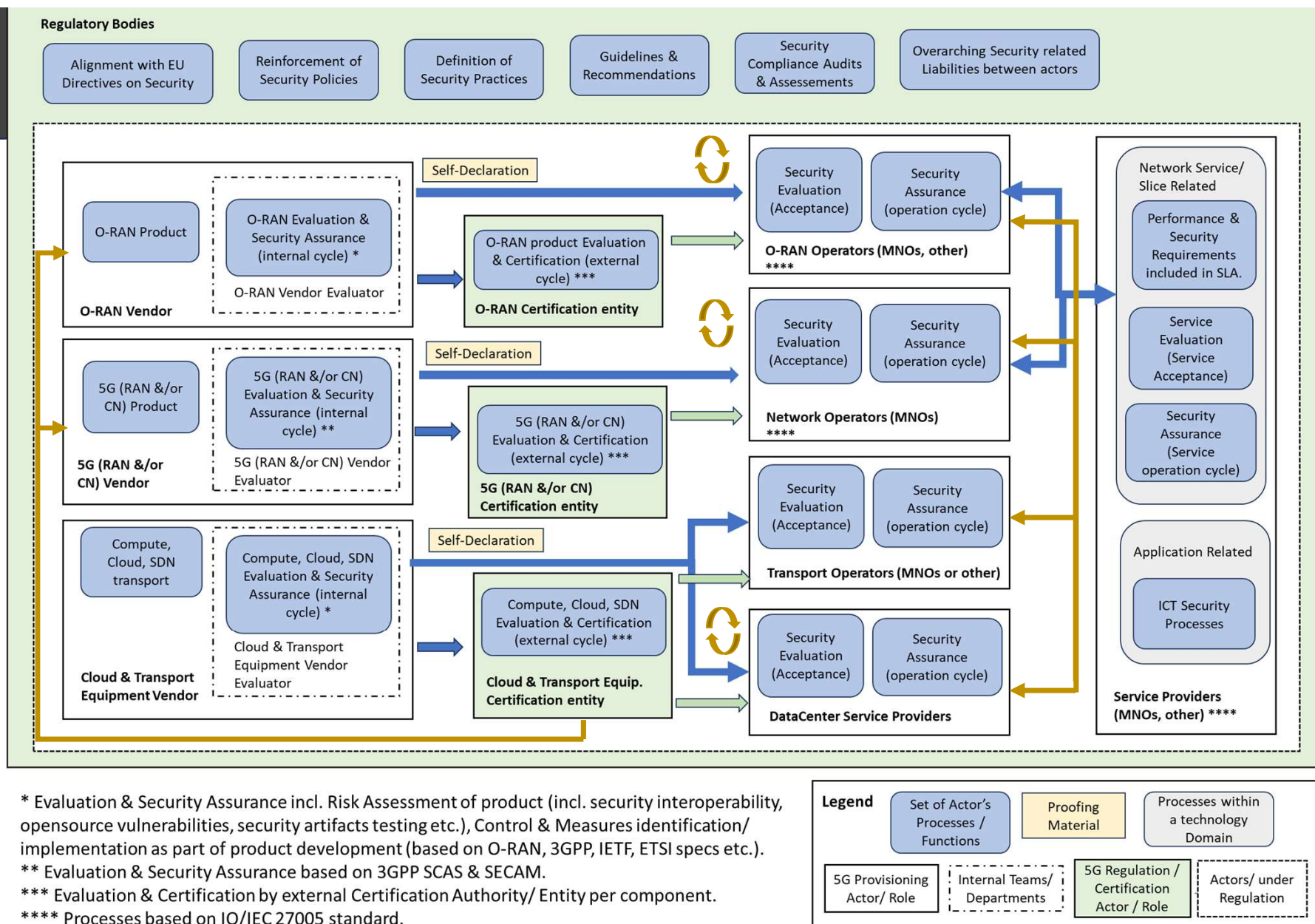
Bridging Methodologies & Future 5G/B5G Ecosystems



- SECAM is primarily **product-centric** and **network-function** focused.
- Not fully addressing **complex multi-stakeholder responsibilities** (e.g., cloud providers, transport operators, service providers).
- Limited support for **continuous, real-time assurance in dynamic cloud-native and virtualized environments**.
- Insufficient coverage of **multi-vendor interoperability risks and open architectures** (e.g., O-RAN, NFV, SDN).
- Strong integration needed with **operational risk management that includes lifecycle coordination across actors**.

5G-TACTIC view on 5G/B5G Ecosystem Roles in Security Assurance

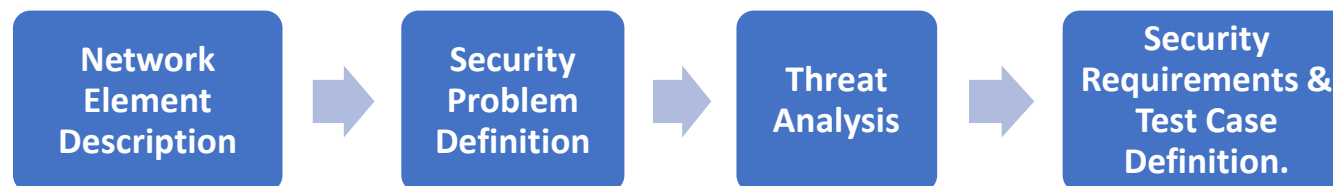
Distinct security assurance roles/duties for Equipment Manufacturers, Network Operators (MNOs), Service Providers, and Regulatory Bodies throughout the entire product and service lifecycle.



Implementation of 5G-TACTIC Security Assurance Methodology



- The 5G-TACTIC high-level security assurance methodology can be further defined in terms of phases and processes.
- Phases of the security assurance processes implementation:
 - **Planning**
 - **Risk assessment**
 - **Security controls and measures implementation**
 - **Assurance activities including Compliance and Certification**
 - **Continuous monitoring and improvement**
- The methodology implementation processes **envelop the technical processes of the SCAS approach:**



5G-TACTIC Security Assurance Methodology – Planning



- **5G-TACTIC-defined Planning processes:**

- **Establishment of a security assurance governance team**, with representatives from various actors and individuals with diverse background and roles; such as network operations, compliance, risk management, and information security experts **from various actors** (i.e. DCSPs, MNOs, Vendors, Regulatory bodies etc).
- **Definition of the security assurance implementation plan**, aligning them with actor roles, regulatory requirements, and industry standards, 5G ecosystem formulations and sharing of accountabilities across the network segments/ assets etc.
- **Identification and clear communication of accountabilities** at various network/ service development, deployment and operation phases; and at various security assurance processes.

- **5G-TACTIC-defined Risk Assessment processes** are related to identifying, analyzing, and evaluating risks to 5G network components.
 - **Identification and categorization of assets** (HW/SW/data/ functionalities etc.) within the specific 5G network deployment.
 - **Conduction of a threat and vulnerability analysis specific to the 5G deployment under analysis; operated by the 5G Ecosystem under analysis; addressing given SLAs.**
 - Evaluation of risk impact and probability to be materialized.

5G-TACTIC Security Assurance Methodology – Control



- **5G-TACTIC-defined Control Implementation processes** are related to:
 - Definition of **security controls tailored to** the unique risks associated with **5G networks, deployment, ecosystem structure**.
 - **Implementation** of the selected controls. This may involve working with vendors and service providers to configure security features.

- **5G-TACTIC-defined Security Assurance Activities, including Continuous Monitoring and Improvement processes** are related to:
 - **Regular testing and validation** of security controls to ensure they function as intended, including iterative loops of penetration testing, vulnerability assessments, simulation of potential attacks etc.
 - Implementation of **continuous monitoring solutions** to track the performance of security controls and identify any anomalies or potential threats in real-time.
 - **Analyses of the results** of the aforementioned assurance activities, towards identifying weaknesses in running security controls and measures and re-defining/ improving them.
 - **Assessment and review of the overall performance of the security assurance methodology**, against the target objectives, and improvement steps towards more secure, available and high performant networks.

Regulatory Bodies

Alignment with EU Directives on Security

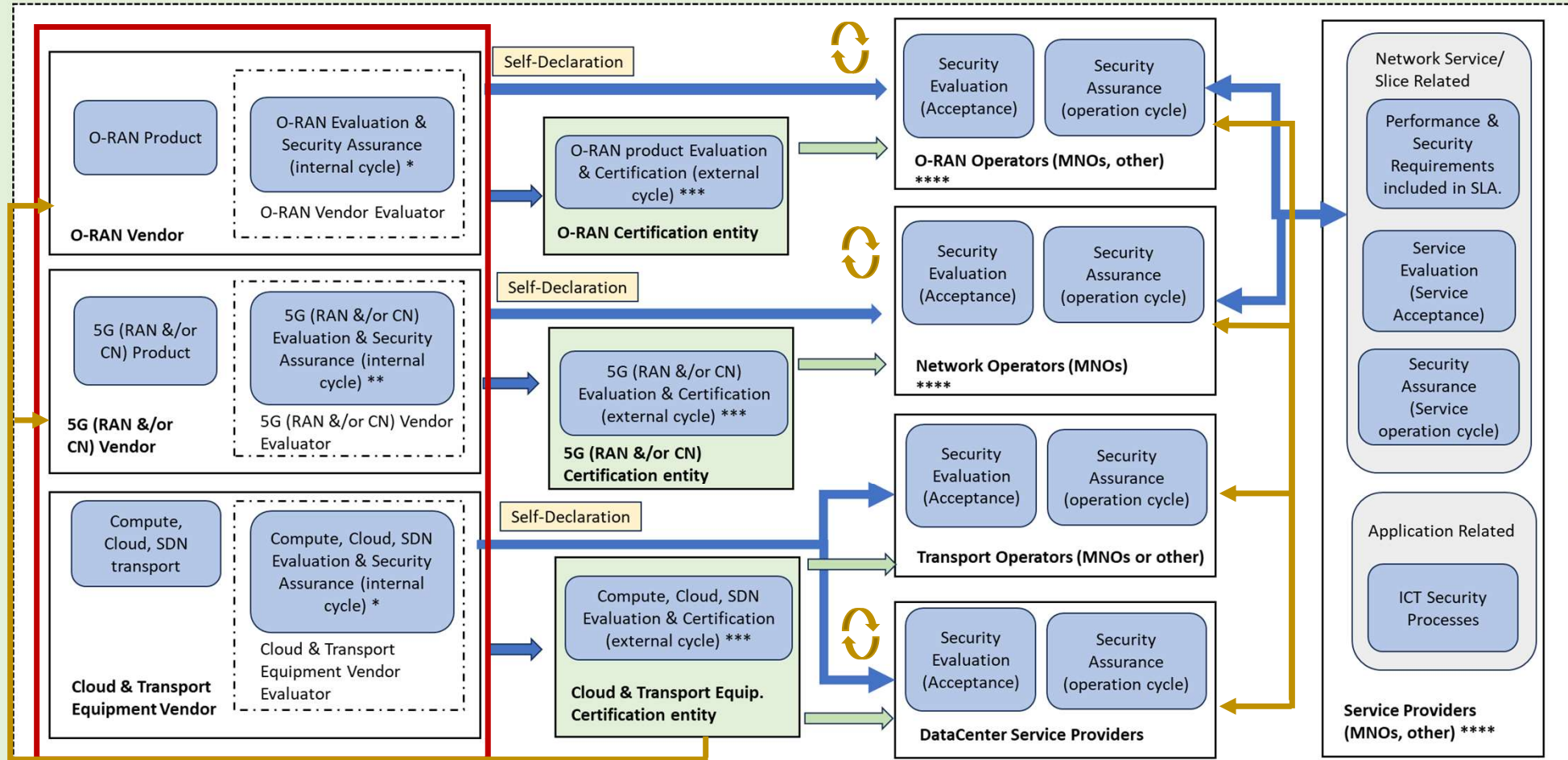
Reinforcement of Security Policies

Definition of Security Practices

Guidelines & Recommendations

Security Compliance Audits & Assessments

Overarching Security related Liabilities between actors



Equipment Manufacturers (Vendors)



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**

- Equipment manufacturers must **integrate 3GPP security specifications into product design** and align with relevant security standards and certifications.
- A structured **product-level security assurance lifecycle** must be defined and implemented prior to commercialization.
- **Comprehensive risk assessment** is required for both **in-house developed** components and **third-party/Open Source HW/SW dependencies**.
- **Continuous vulnerability monitoring and patch management** is essential, especially when leveraging Open Source components, including timely notification to operators.
- **Strong risk management and mitigation strategies** must be maintained across production, deployment, and operational phases in close collaboration with customers and operators.

Regulatory Bodies

Alignment with EU Directives on Security

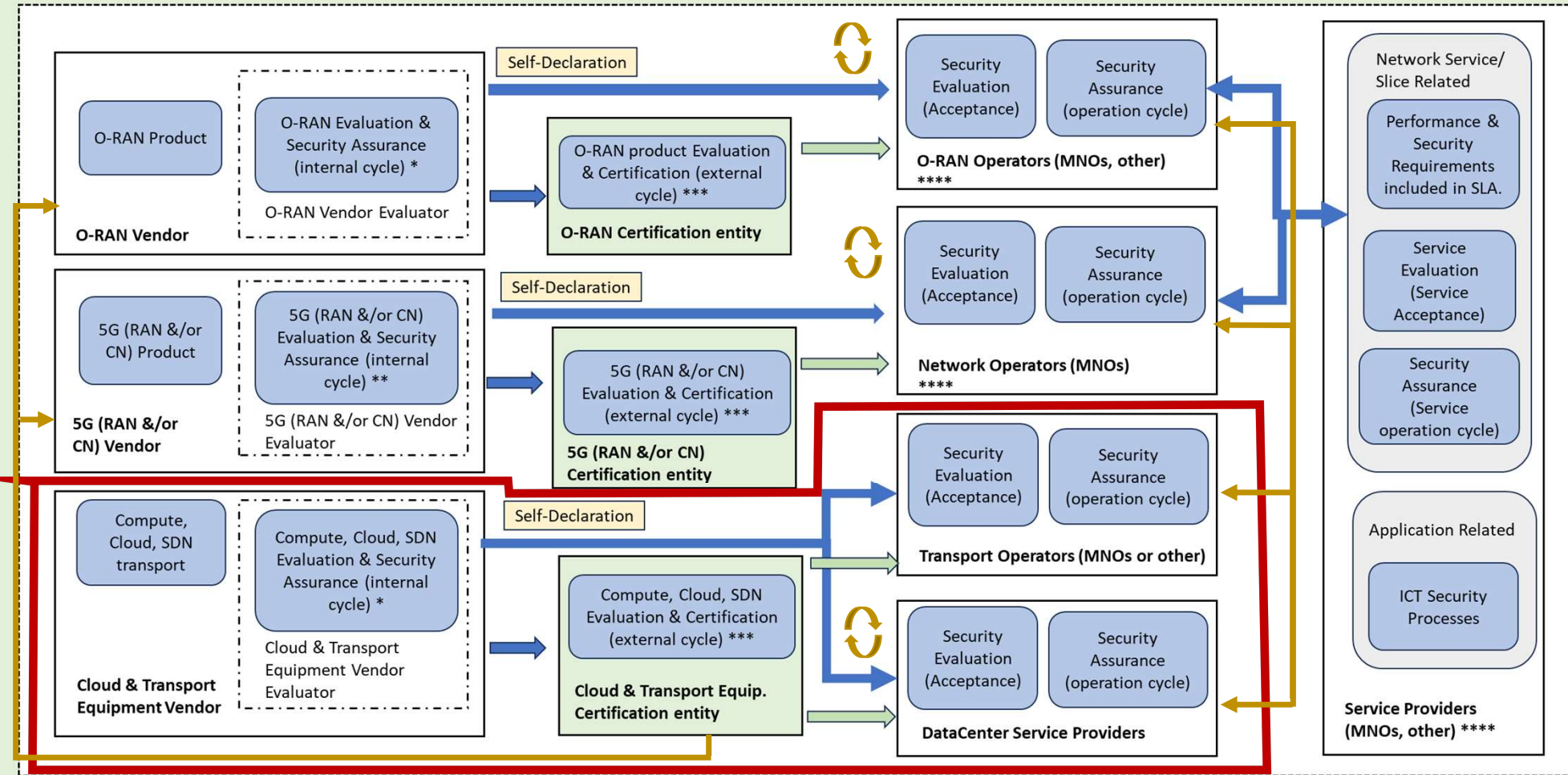
Reinforcement of Security Policies

Definition of Security Practices

Guidelines & Recommendations

Security Compliance Audits & Assessments

Overarching Security related Liabilities between actors



Data Center Service Providers



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**
 - DCSP must **implement strong security controls** such as encryption, secure access management, and continuous security assessments, **especially for 5G-hosted environments**.
 - They must ensure compliance with relevant security standards and regulations, maintaining secure cloud infrastructures for hosting 5G network functions and applications.
 - **A dedicated cloud-specific risk assessment process** must be applied to identify and manage threats in virtualized and cloud-native environments.
 - **A clear shared responsibility model must be defined with network operators**, specifying roles and obligations for security management and incident response across the service lifecycle.

Transport Network Operators



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**

- Transport Network Operators are responsible for end-to-end security of transport segments, applying relevant standards (e.g., ITU, IETF, NIS, alongside 3GPP where applicable).
- Continuous risk assessment and security management must be applied to transport network infrastructure to address evolving threats and vulnerabilities.
- Transport operators **are required to maintain close coordination with overlay Mobile Network Operators (MNOs)** to ensure secure integration within the overall 5G architecture.
- **Security requirements must be embedded into SLAs** covering operational security obligations across the service lifecycle.

Regulatory Bodies

Alignment with EU Directives on Security

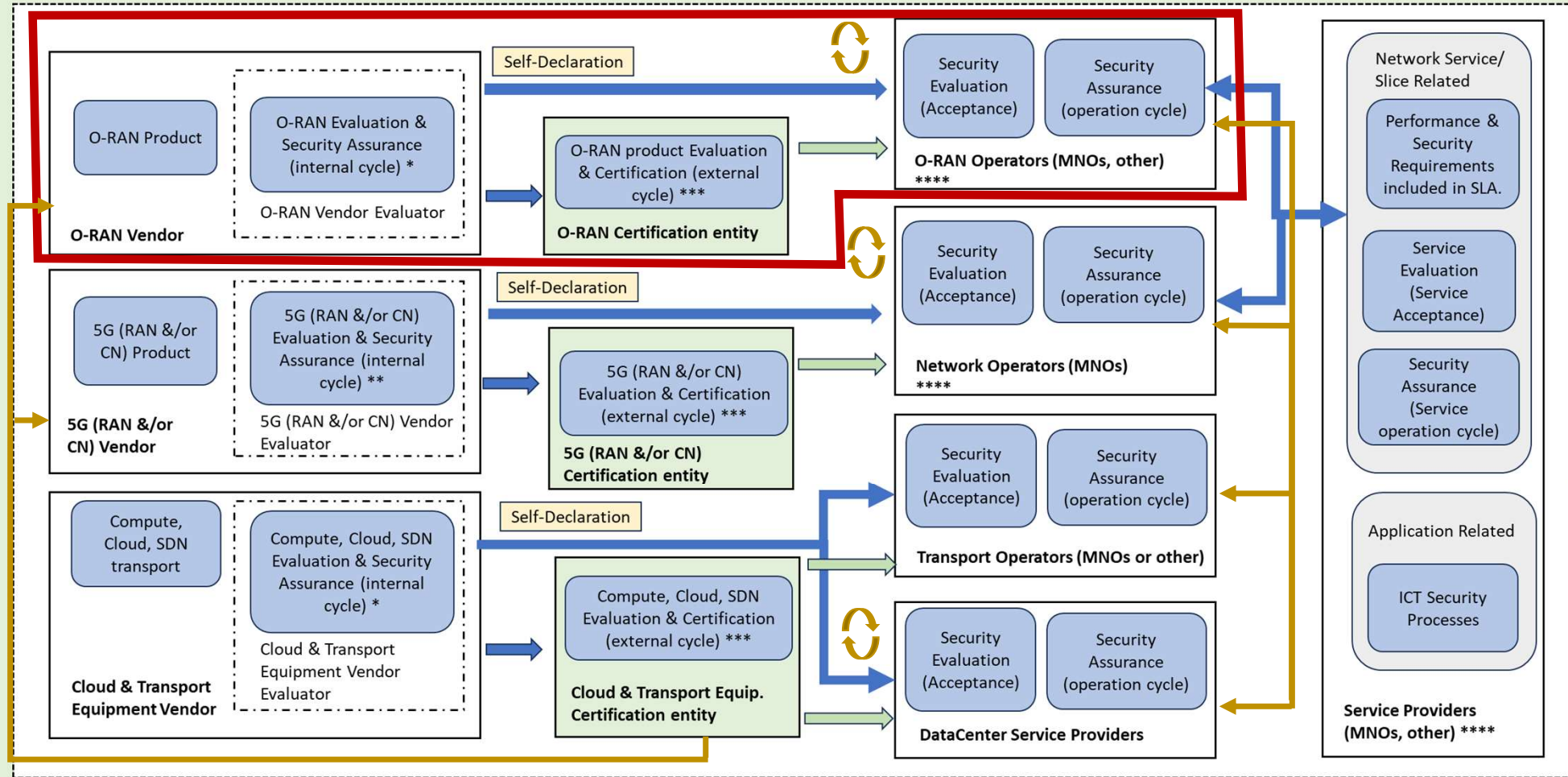
Reinforcement of Security Policies

Definition of Security Practices

Guidelines & Recommendations

Security Compliance Audits & Assessments

Overarching Security related Liabilities between actors



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**

- O-RAN vendors must integrate 3GPP and O-RAN Alliance security specifications into product development to ensure standards compliance.
- A formal security assurance lifecycle per product must be defined and implemented prior to commercialization, including structured risk assessment and validation.
- **Special attention is required for open-source dependencies and multi-vendor interoperability,** ensuring consistent security levels across disaggregated deployments.
- During deployment and operation, **O-RAN vendors need to provide security guidance and consulting,** supporting operators in secure configuration and usage of their solutions.
- **Robust risk management strategies and lifecycle security processes** must be maintained in close collaboration with network operators **across production, deployment, and operational phases.**

O-RAN Providers - Operators



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**
 - **O-RAN operators must implement security controls tailored to open and disaggregated RAN architectures**, ensuring protection across multi-vendor environments.
 - Regular risk assessments and vulnerability analysis must be performed across RAN elements, including multi-vendor and open-source components.
 - Continuous security monitoring and adaptive mitigation strategies are required to respond to evolving threats in O-RAN deployments.
 - O-RAN operators must maintain close collaboration with O-RAN vendors to ensure security is embedded in both design and operational phases of the network.

Regulatory Bodies

Alignment with EU Directives on Security

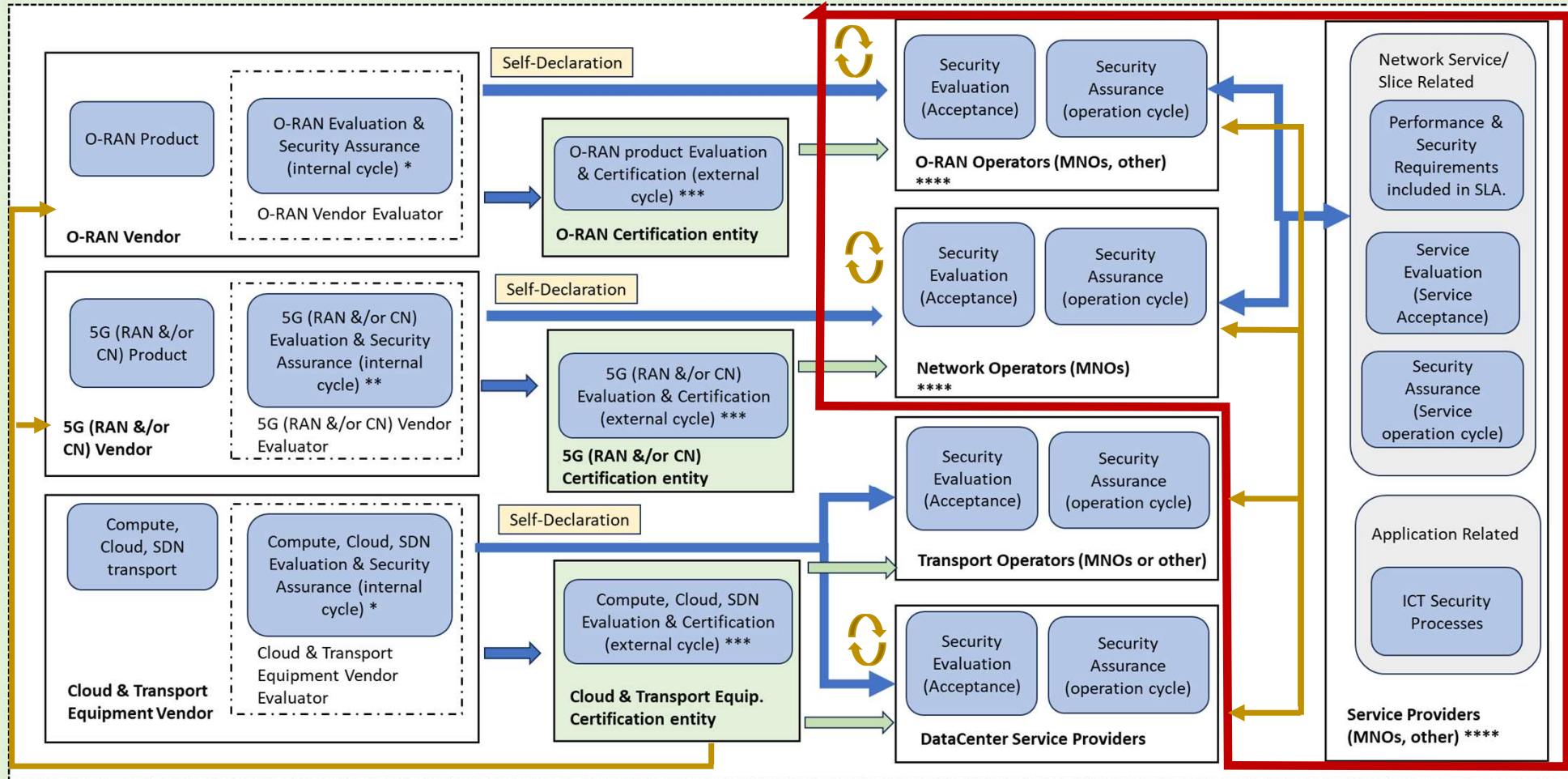
Reinforcement of Security Policies

Definition of Security Practices

Guidelines & Recommendations

Security Compliance Audits & Assessments

Overarching Security related Liabilities between actors



Mobile Network Operators



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**

- Mobile Network Operators (MNOs) must implement core security controls across all network elements under their control and shall perform structured risk assessments aligned with 3GPP SCAS/SECAM and ENISA guidelines, ensuring compliance with established security standards.
- They need to establish robust security monitoring, incident response, auditing, and penetration testing processes to detect and mitigate vulnerabilities.
- **They may need to engage in cross-industry collaboration and threat intelligence sharing with cybersecurity stakeholders to strengthen overall network resilience.**

- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**

- Service Providers are responsible for securing application and services, including secure coding practices, vulnerability assessments, and timely patch management.
- They **can be asked to ensure service-level security accountability, embedding security requirements into SLAs.**
- Security incidents and performance impacts must feed into continuous risk assessment and service assurance processes, enabling proactive mitigation.
- **Service Providers** can be required **to collaborate closely with network operators** to ensure alignment with underlying security controls and policies.

Regulatory Bodies

Alignment with EU Directives on Security

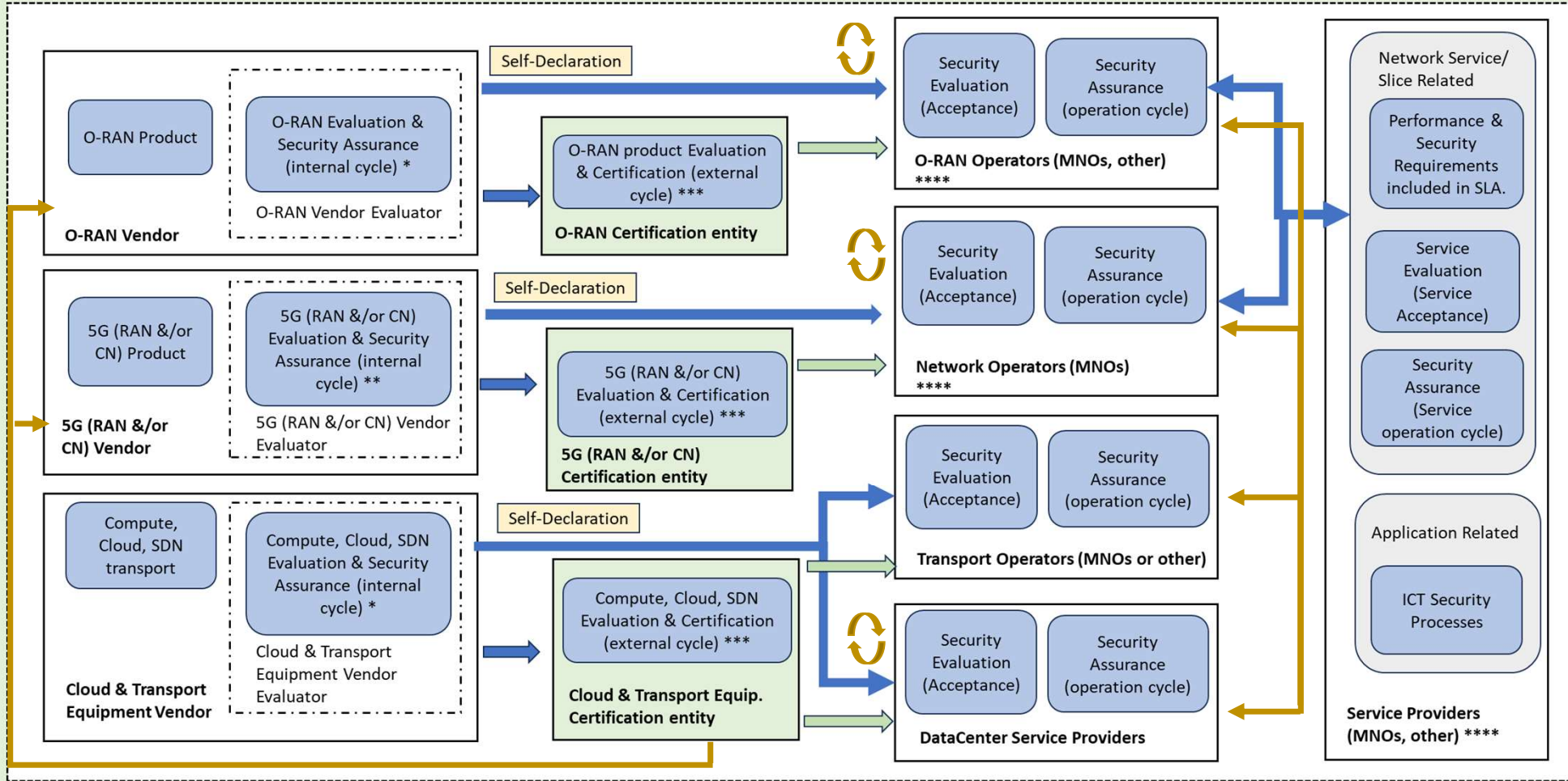
Reinforcement of Security Policies

Definition of Security Practices

Guidelines & Recommendations

Security Compliance Audits & Assessments

Overarching Security related Liabilities between actors



Regulatory Bodies



- **5G-TACTIC-defined Security Assurance Role Overview in future 5G/B5G Ecosystems**

- Regulatory bodies are responsible for defining, developing, and enforcing security policies and standards governing 5G/B5G network operations across the ecosystem.
- They establish a regulatory framework for security assurance, covering both role-specific responsibilities and end-to-end system security requirements.
- Regulatory authorities promote the adoption of best practices, guidelines, and recommendations to ensure consistent security assurance across all ecosystem stakeholders.
- At deployment and operational stages, they may need to conduct audits, assessments, and compliance checks to verify adherence to security regulations and standards.
- They will play a key role in enabling ecosystem-wide coordination and continuous improvement, fostering collaboration among stakeholders to address emerging cybersecurity threats.

Conclusions



- 5G/B5G deployments may introduce a broader and more complex security landscape driven by virtualization, open architectures, and multi-stakeholder ecosystems.
- Traditional SECAM approaches may be rendered insufficient for dynamic, cloud-native, and multi-vendor mobile network environments.
- Effective 5G/B5G network assurance may require clearly defined responsibilities across all ecosystem actors.
- A lifecycle-based methodology is essential, covering planning, risk assessment, assurance, and continuous monitoring.

5G-TACTIC proposes a comprehensive security assurance methodology that defines lifecycle phases, processes, and role-specific responsibilities across the future 5G/B5G ecosystems.

Thank you for Your Attention!