SAND5G

https://sand5g-project.eu/

Course on risk assessment methodologies for national 5G security oversight

D3.1: Security training, knowledge and capacity building report
Dedicated Courses from National Authorities

This project has received funding from the DIGITAL EUROPE (DIGITAL) programme under Grant Agreement No 101127979

Course Roadmap : Scope and Objectives

The purpose of this course on national 5G security oversight is to:

- **Focus** on risk assessment methodologies for public authorities (legal and strategic framing)
- **Combine** regulatory, technical, and operational perspectives (ENISA 5G threat landscape)
- **Cover** national risk procedures, supply-chain assessment, high-risk vendors, and Integration with SAND5G platform capabilities
- **Place emphasis** on actionable outputs for oversight and supervision (Reporting, governance and controls)
- **Target** audience that includes analysts, inspectors, authority teams, and policy advisors

5G versus 4G: Why Traditional Risk Assessment Fails

Traditional risk assessment models serving 4G networks are insufficient for 5G due to **fundamental shift from hardware-centric to software-defined architecture**:

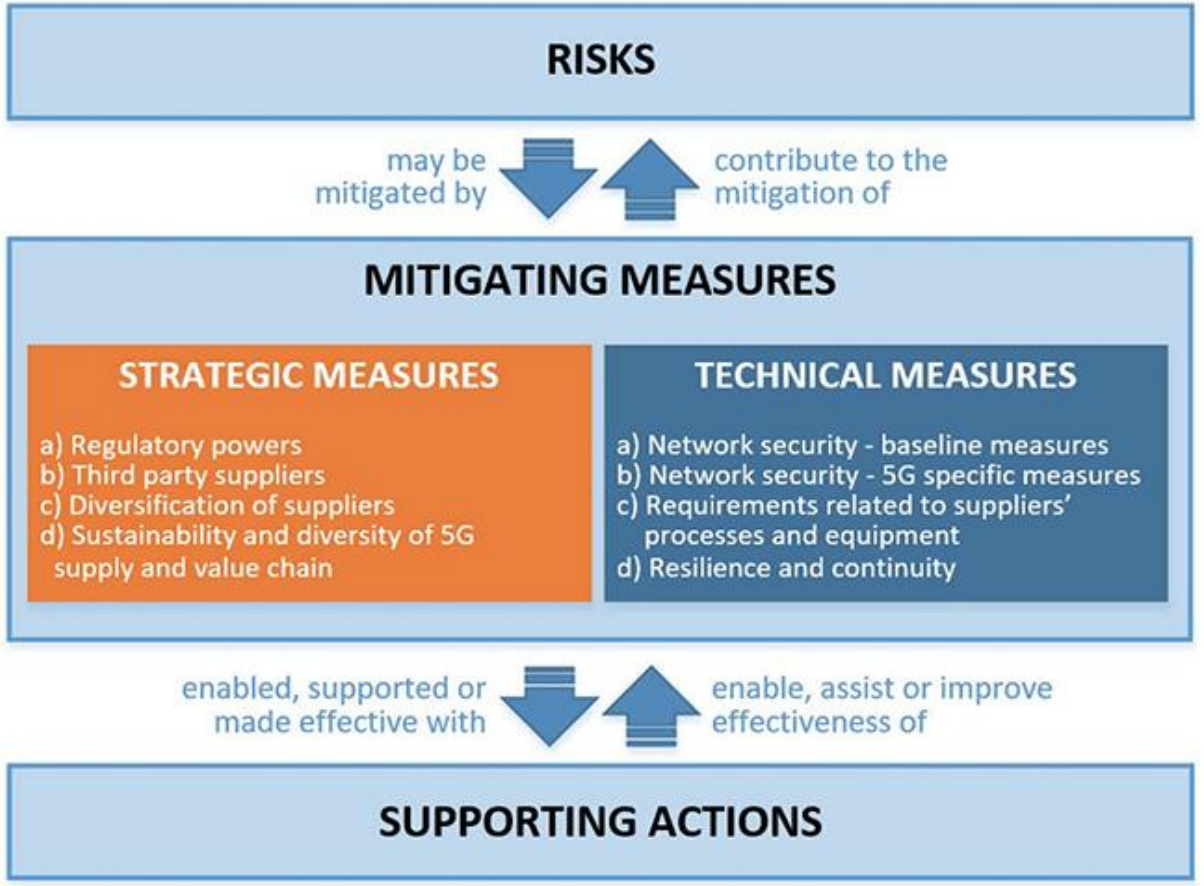
- 5G introduces service-based architecture rather than static function chains
- Virtualization and cloud-native deployment expand shared infrastructure risk
- APIs become high-value attack surfaces
- Edge computing distributes compute and control across more locations
- Network slicing adds multi-tenancy and isolation complexity
- Threats can propagate faster through orchestration and automation

5G Security Oversight: A National and Regulatory Mandate

- 5G is a foundational digital infrastructure layer
- It supports essential sectors, emergency functions, and government services
- Security failures may have systemic and cross-sector consequences
- 5G increases software, cloud, virtualization, and API dependency
- Risks include both technical compromise and strategic dependence
- National oversight is necessary to ensure resilience, continuity, and trust

The EU 5G Toolbox and Recommendation

- Recommendation (EU) 2019/534 was the official catalyst that launched the European Union's coordinated approach to 5G security
- Member States were asked to complete national risk assessment
- The findings were synthesized into a EU coordinated risk assessment and the 5G toolbox translated them into strategic and technical measures
- National Authorities retain responsibility for implementation and enforcement of the security measures

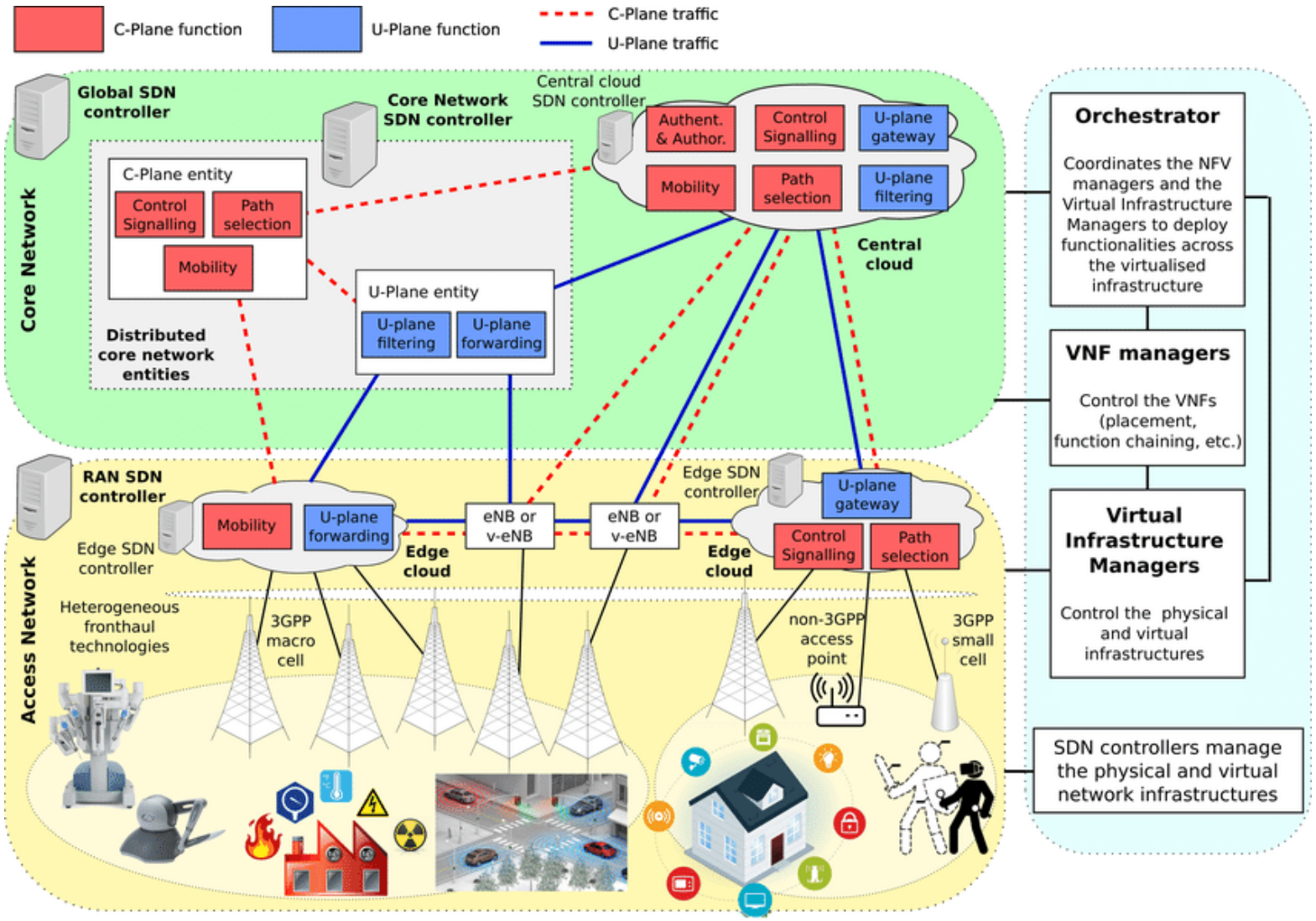


ENISA Methodology: Asset, Threat, Vulnerability, and Control Mapping

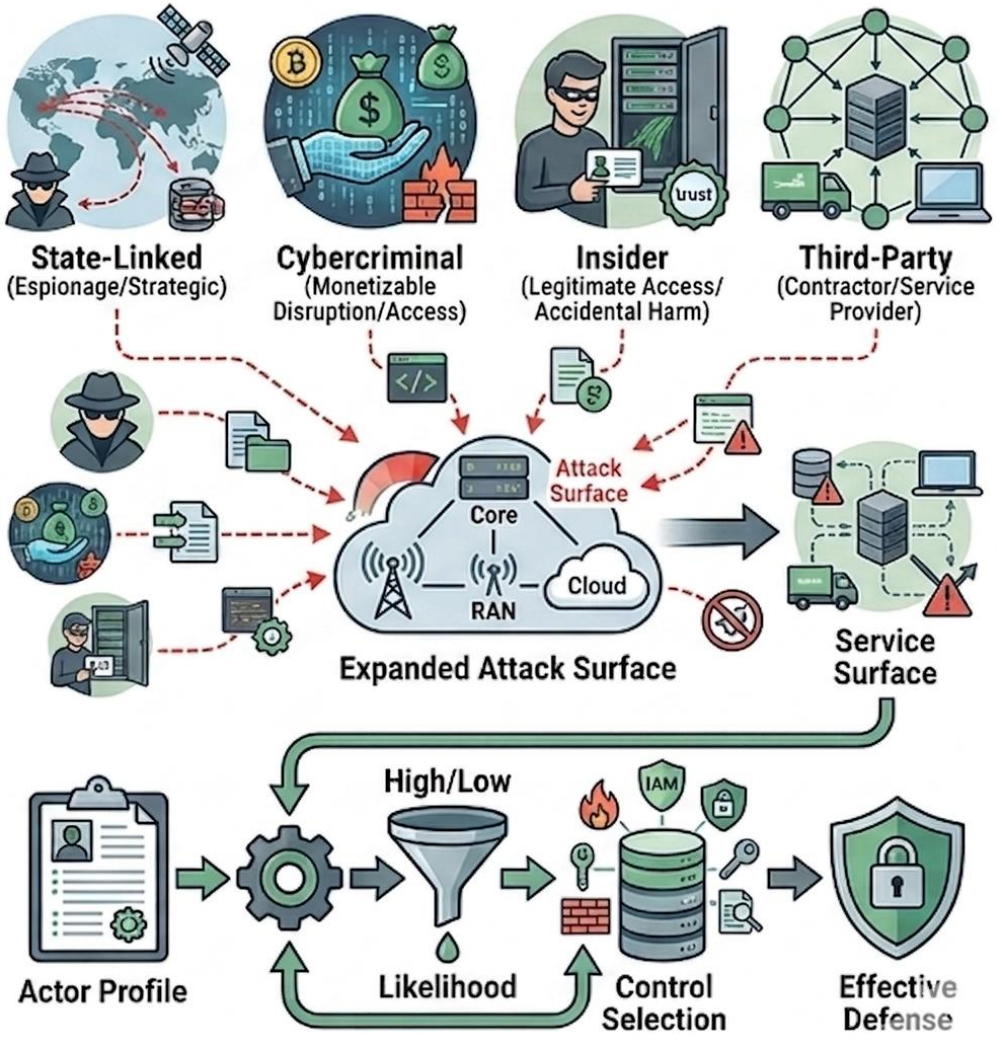
- ENISA structures 5G analysis around four critical pillars to create a "chain of security":
  - **Assets**: Identifying what needs protection, including physical hardware, virtualized network functions (VNFs), and the sensitive data flowing through network slices.
  - **Threats**: Pinpointing potential dangers, such as state-sponsored interference, signaling protocol attacks, or local data interception.
  - **Vulnerabilities**: Detecting weaknesses in the system, such as software misconfigurations or a lack of vendor transparency.
  - **Controls (Mitigation)**: Applying the EU 5G Toolbox measures (strategic and technical) to neutralize the threat-vulnerability link.
- It supports linkage between risk scenarios and mitigating controls. By utilizing this mapping, **National Authorities** can move from reactive security to proactive oversight.

Asset Taxonomy : Physical, Virtualized, Logical Components

- Physical infrastructure includes sites, equipment, transport, and facilities
- Virtualized infrastructure includes NFVI (Network Function Virtualization Infrastructure), VNFs (Virtualized Network Functions), CNFs (Cloud-native Network Functions), and hosting layers
- Logical infrastructure includes SDN (Software-Defined Networking) controllers, orchestration logic, and policy engines
- Security architecture overlays identity, trust, access control, and logging
- Assets should also include management systems and external interfaces
- National assessments must distinguish key assets from supporting



Threat Actors : State-Sponsored, Cybercriminal, Insider, Third-Party



- State-linked actors may pursue espionage, disruption, or strategic influence.
- Cybercriminal groups may target monetizable disruption or privileged access.
- Insiders may exploit legitimate access or cause accidental harm.
- Third-party service providers can expand the attack surface.
- Contractors and maintenance personnel may introduce physical or logical risk.
- Threat actor profiling helps shape likelihood and control selection.

Core Network Threats: Slicing, APIs, Service Exposure

- Service-Based Architecture introduces API-driven trust relationships
- Core functions are critical targets:
  - Access and Mobility Management Function (AMF)
  - Session Management Function (SMF)
  - User Plane Function (UPF)
  - Authentication Server Function (AUSF) and
  - Policy Control Function (PCF)
- Poor service authentication can allow impersonation or privilege escalation
- API misuse may enable lateral movement across core services
- Slicing can create cross-slice spillover if isolation is weak
- Signaling and policy manipulation can degrade availability and trust
- Core compromise can cascade into national-scale service disruption

Access Network Threats: RAN, MEC, Distributed Exposure

- RAN is moving toward Open RAN (O-RAN) and security now interacts with distributed cloud and edge components
- Fake or rogue access nodes remain relevant threat scenarios
- Multi-access Edge Computing (MEC) expands the processing perimeter beyond central sites
- Edge gateways fragment trust boundaries, requiring a shift from perimeter security to Zero Trust Architecture
- The network is now "everywhere" and distributed sites may have weaker physical or operational controls (Oversight Gap)
- Traffic offload and local applications complicate monitoring and forensics

Management and Orchestration: The “Master Key” Risk

- Management and Network Orchestration (MANO) coordinates lifecycle operations across virtualized functions and slices
- Orchestrators can deploy, modify, scale, or terminate services at speed
- Compromise of orchestration can affect multiple domains simultaneously
- Weak privileged access controls can create systemic exposure. Automation means a single malicious script in the MANO can disable national 5G services faster than human intervention can stop it.
- Automation amplifies both resilience and attacker impact
- Change integrity and role separation are essential oversight questions
- Logging and auditability are critical for post-incident reconstruction. Because the MANO can "delete its own history," logs must be exported in real-time to a third-party, tamper-proof location (like the SAND5G environment) for forensic reconstruction.

Protocol, Interface, and Service Exposure in 5G

5G moves from proprietary signaling to a Service-Based Architecture (SBA). Security now depends on API integrity rather than just physical cable isolation.

- 5G risks arise from protocols, APIs, interfaces, and trust relationships
- GTP (GPRS Tunneling Protocol)-related exposure can still matter in transport and mobile contexts
- HTTP/2 and service interfaces in the core increase API security importance
- Roaming and interconnection interfaces expand external dependency risk
- Poorly validated service requests can trigger misuse or denial conditions. These can cause the AMF (Access and Mobility Management Function) to crash. Because the core is software-based, a "protocol fuzzer" can crash a Network Function just like a browser crashes on a bad website.
- Protocol-level exploitation may combine with architecture flaws and weak access control

5G Interface & Protocol Risk Mapping

- Map assets by criticality: core, RAN, edge, orchestration, identity, transport
- Map threats by likelihood: API abuse, rogue nodes, insider misuse, DDoS, update compromise
- Map vulnerabilities by exploitability: weak auth, misconfiguration, weak segmentation, poor logging
- Highlight key assets with national criticality weighting
- Separate technical severity from strategic importance
- Use heatmaps to support prioritization and reporting
- Feed outputs into national risk registers and supervisory plans

ISO/IEC 27005 as a complementary Risk Management Framework for 5G Oversight

- ISO/IEC 27005 (Information security, cybersecurity and privacy protection — Guidance on managing information security risks) provides a structured cyber-risk management process
- It supports context establishment, risk identification, analysis, evaluation, and treatment
- It is adaptable to telecom and national-infrastructure use cases
- It helps standardize terminology and decision logic across teams
- It complements the EU toolbox rather than replaces it. It provides the process ("How"), while the EU Toolbox provides the requirements ("What"). Together, they create a legally defensible oversight framework.
- It supports auditability and repeatability in oversight practice.

Context Establishment: Defining National Critical Infrastructure Boundaries

- Identify national operators, relevant private 5G deployments, and shared infrastructure
- Define which services and sectors depend on 5G
- Identify cross-border interconnections and roaming dependencies
- Determine legal, regulatory, and national-security context
- Map logical boundaries for data residency and cloud-native hosting (Data Sovereignty).
- Define the "Management Boundary" for third-party vendors and MSPs (Mobile Service Providers).
- Clarify threat assumptions and assessment scope
- Define what counts as a “key asset” in the national environment
- Set time horizon and reassessment triggers

Risk Identification: Building a National 5G Risk Register

- **Comprehensive Asset Recording**: Record physical and virtual assets, threat actors, and vulnerabilities, specifically mapping them to affected network slices.
- **Strategic & Technical Risks**: Include technical risks (API vulnerabilities) alongside strategic risks such as Supply Chain lock-in, vendor sovereignty, and regulatory non-compliance.
- **Dependency & Support Tracking**: Track supplier dependencies, including software update pipelines and third-party Managed Service Provider (MSP) access models.
- **High-Impact Scenario Modeling**: Register likely scenarios such as automated orchestration compromise, cross-slice data leakage, or localized edge abuse.
- **Accountability & Lifecycle Management**: Record clear ownership, cross-departmental accountability."
- **Regulatory Alignment**: Ensure all entries align with NIS2, the EU 5G Toolbox, and national supervisory reporting requirements.

Event-Based vs Asset-Based Risk Assessment: What Authorities Need?

- Asset-based assessment starts from critical functions and dependencies
- Event-based assessment starts from threat scenarios and disruptive events
- Asset-based logic improves prioritization of key assets
- Event-based logic improves realism about exploit paths and consequences
- Combining both approaches gives better oversight value and supports better treatment and reporting decisions
- Authorities need both static architecture views and dynamic incident views
- Trigger-Based Reassessment: National Authorities should mandate reassessments when "Triggers" occur such as geopolitical shifts, new zero-day vulnerabilities, or major network topology changes.

National Impact Analysis: Beyond Technical Metrics

- Multidimensional CIA+ Assessment: Evaluate Confidentiality, Integrity, and Availability, with added focus on Signaling Integrity and Identity Privacy.
- Add national resilience and critical-sector dependence
- Estimate service outage consequences and recovery complexity
- Include social, economic, safety, and political effects
- Reflect effect on emergency and public-sector communications
- Distinguish local disruption from systemic disruption
- Use explicit criteria to improve consistency across different supervisory teams and operators

Risk Evaluation: Establishing National Tolerance & Thresholds

- Define clear, measurable limits for acceptable residual risk across the 5G ecosystem.
- Apply stricter security bars for National Critical Assets (Core, Identity, Orchestration) compared to general consumer infrastructure.
- Distinguish between "Acceptable Risk" (to be monitored) and "Intervention Risk" (requiring mandatory mitigation or removal).
- Align with Strategic & Geopolitical Priorities: Ensure evaluation reflects national security interests, the NIS2 Directive, and sector-specific resilience targets.
- Use governance structures to validate evaluation outcomes through multi-agency consensus.
- Ensure evaluation criteria are transparent and reviewable to maintain legal and regulatory defensibility.
- Tie evaluation directly to regulatory outcomes, such as license conditions and fines.

5G Treatment: Mitigate, Transfer, Avoid or Accept

- Mitigate through technical controls, audits, and operational improvements
- Utilize service-level agreements (SLAs) for financial risk, while acknowledging that operational and security responsibility cannot be offloaded to a third party.
- Prohibit specific deployments, such as High-Risk Vendor (HRV) placement in the Core, or restrict sensitive services from being hosted in non-sovereign clouds.
- Accept only where exposure and impact remain within defined tolerance
- Implement temporary measures (e.g., enhanced logging or isolated network segments) during vendor migrations or software patching cycles.
- Tie treatment choice to evidence, not only policy preference. Ensure all treatment choices are justified by technical telemetry and forensic data
- Document rationale, timelines, and responsible actors

The 5G Ecosystem: Multivendor Dependencies and Hidden Coupling

- 5G networks depend on hardware, software, cloud, and support suppliers
- Dependencies may exist at product, update, management, or service level
- Apparent vendor diversity at the hardware level often masks a concentration of risk in shared maintenance teams or common software components.
- Shared orchestration and support tooling can create single points of failure across seemingly isolated network segments.
- Cross-domain dependencies mean a vulnerability in a private industrial 5G network can propagate to the national public core. National assessments must capture visible and invisible dependency chains
- Supply-chain risk must be tracked over the full lifecycle

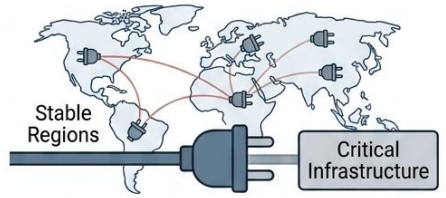
High-Risk Vendor Criteria: Technical and Strategic Indicators

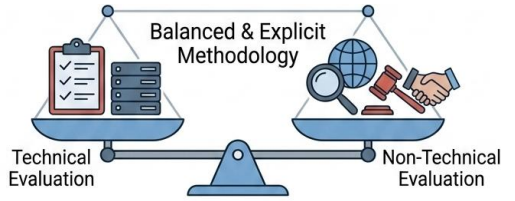
- Evaluate vendor risk through objective data: vulnerability history (CVE frequency), patch quality, and the speed of critical security updates.
- Monitor vendor support access models, remote management "backdoors," and the effectiveness of their incident responsiveness
- Assess the vendor’s corporate structure, including ownership transparency and their exposure to interference from non-democratic third-country governments.
- Evaluate vendor significance based on their 'Network Footprint.' A high concentration of equipment in sensitive architectural tiers (Core or MANO) triggers a higher risk classification due to the potential for large-scale, systemic interference.
- Measure the vendor’s capacity and willingness to meet stringent national security requirements
- Criteria must be documented to support defensible actions
- Take into consideration network product assurance as defined in Technical Measure TM01 (Network Product Assurance)

Note that Strategic Measure SM03 mandates regulatory mechanics of enforcing vendor diversity across a national ecosystem

Non-Technical Risks: Political Interference and Legal Jurisdictions

- Evaluate vendor susceptibility to third-country laws that mandate state-sponsored surveillance or bypass national trust assumptions.
- Governance opacity can complicate assurance and accountability
- Geopolitical dependency may affect continuity and resilience (reliance on suppliers from volatile regions threatens critical infrastructure)
- Non-technical factors should inform, not replace, technical evaluation
- Authorities need a balanced but explicit methodology for these factors

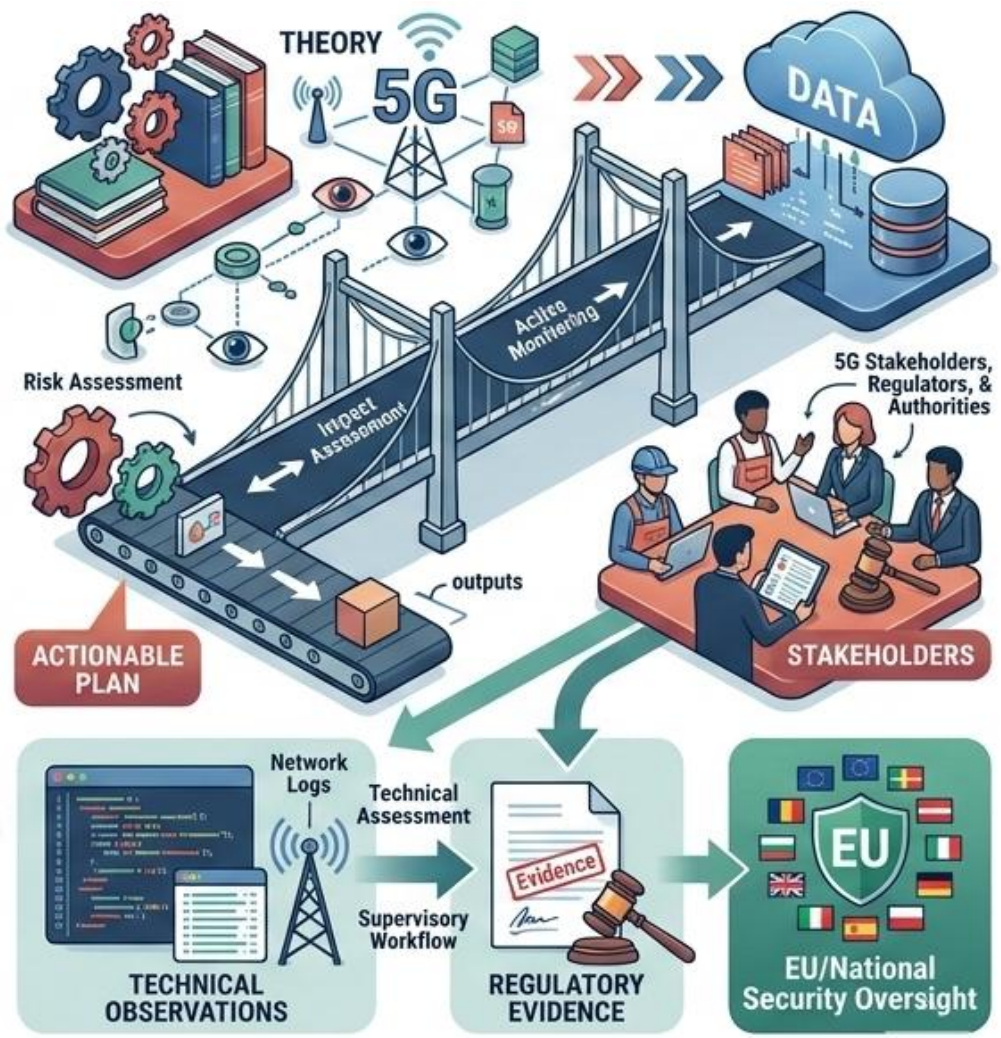




Supply Chain Integrity: Continuous Lifecycle Transparency & Evidence

- Software Bill of Materials (SBOM) improves visibility into software components and dependencies
- Update assurance helps validate integrity of change and patch channels
- Lifecycle evidence should cover build, distribution, deployment, and support
- Operators should assess who can modify, sign, deliver, and access software
- Transparency must extend to subcontractors and managed-service relationships
- Evidence should support incident response and post-event traceability
- Transparency reduces blind spots but does not eliminate risk
- New vulnerabilities may alter the risk profile of a supplier or product
- Lifecycle monitoring should be risk-based and evidence-driven

SAND5G: The Bridge Between Theory and Data



- SAND5G is a risk and impact assessment platform for 5G environments
- It is designed to support 5G stakeholders, regulators, and authorities
- It connects technical assessment with supervisory workflows
- It supports active monitoring and risk awareness
- It aligns with EU and national 5G security oversight needs
- It can help convert technical observations into regulatory evidence
- It is especially relevant for operationalizing risk assessment outputs

SAND5G Technical Oversight & Dynamic Risk Analysis

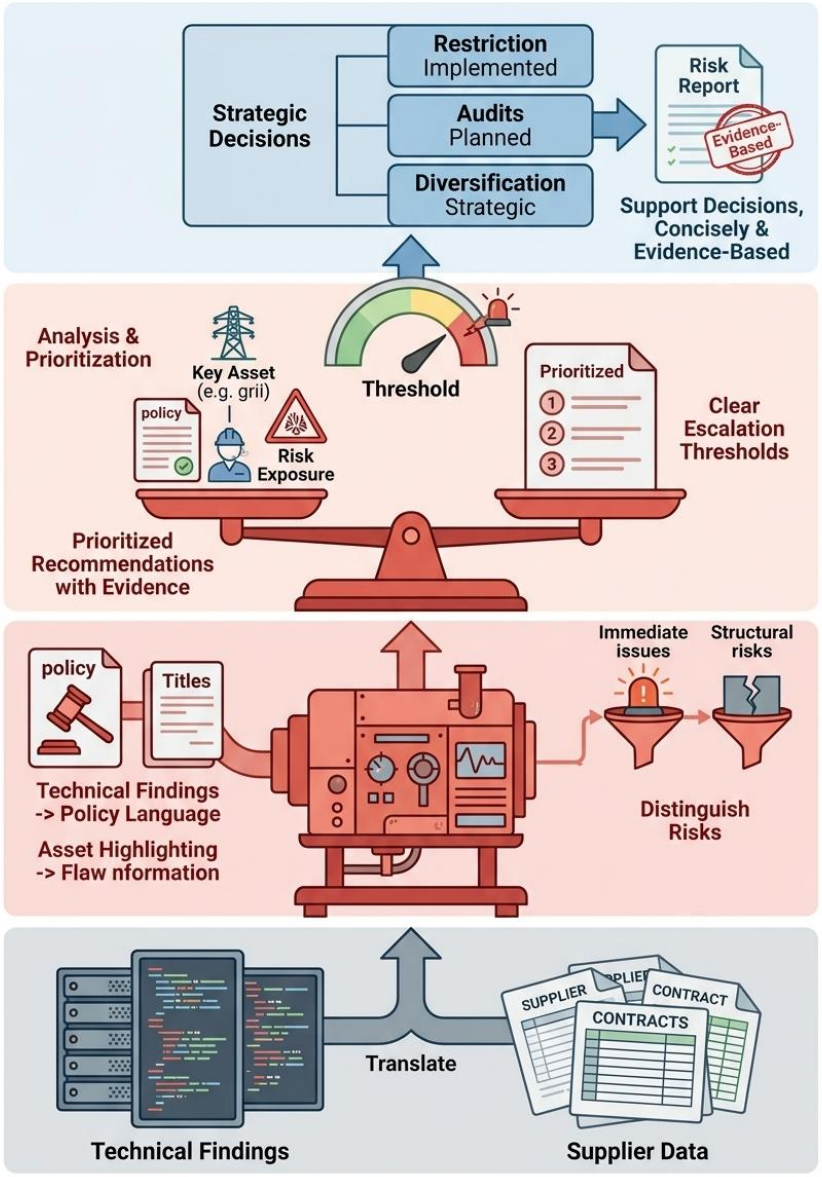
- **Integrated Environmental Awareness**: Automatically map technical findings to a baseline of regulated infrastructure and asset topologies to ensure context-aware interpretation.
- **Active Threat & Security Monitoring**: Perform continuous vulnerability assessments and penetration testing while monitoring incidents in real-time to detect deteriorating security postures earlier.
- **Structured Evidentiary Workflows**: Connect technical telemetry directly to reporting outputs, providing a repeatable basis for formal incident, vulnerability, and risk analysis.
- **Dynamic Oversight & Response**: Transition from static assessments to a "living" oversight model using customizable alert thresholds and escalation logic for priority events.
- **Multi-Perspective Situational Enrichment**: Support both compliance-oriented and threat-oriented views to enrich national risk assessments with real-time technical intelligence.

Integration: Mapping SAND5G Outputs to ISO/IEC 27005 and Regulatory Reports

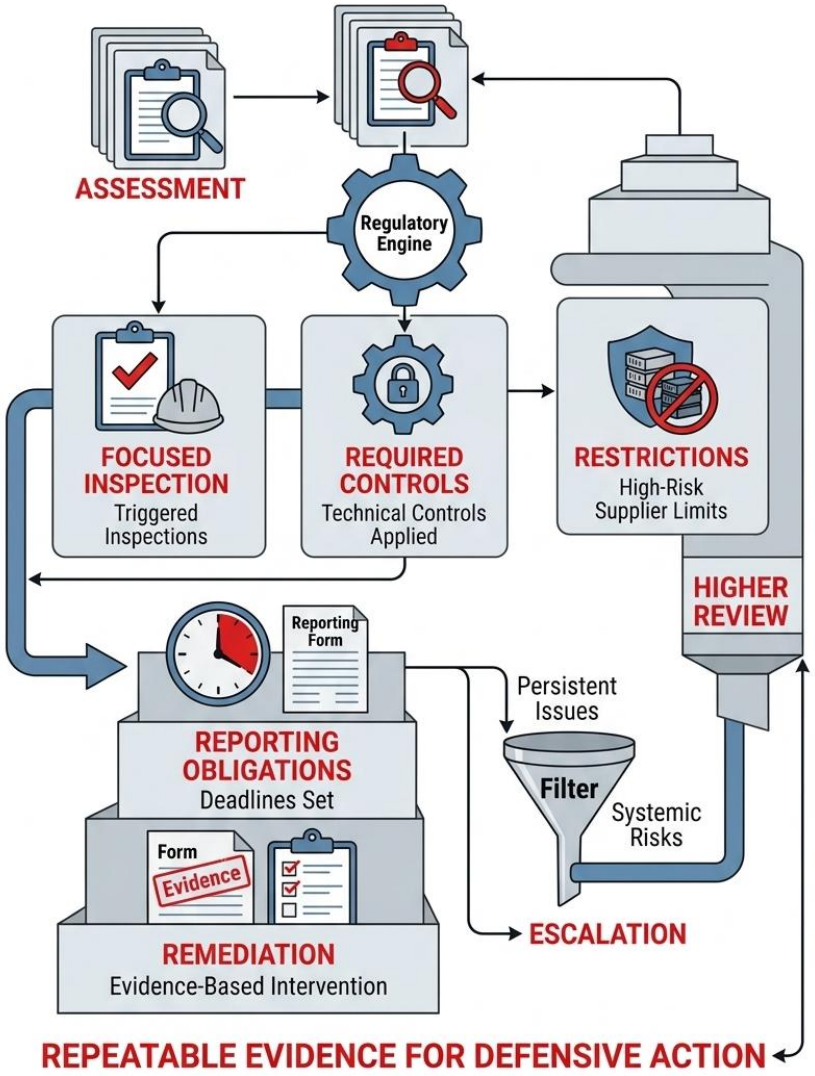
- Use SAND5G data to update risk identification and analysis
- Feed alerts and findings into risk registers and treatment tracking
- Use platform outputs to support regulatory reports and audit trails
- Align evidence with treatment decisions and reassessment triggers
- Map incident data to asset criticality and impact criteria
- Use standardized reports to support consistency across operators
- Improve traceability between technical events and policy decisions

Generating Actionable Risk Reports for Policymakers

- Translate technical findings into policy-relevant language
- Distinguish immediate operational issues from structural risks
- Highlight key assets, supplier concerns, and unresolved exposures
- Present prioritized recommendations with evidence references
- Use clear thresholds for escalation and intervention
- Support strategic decisions on restrictions, audits, and diversification
- Keep reports concise but evidence-based



From Assessment to Regulatory Action: Inspections, Restrictions, Reporting, and Review

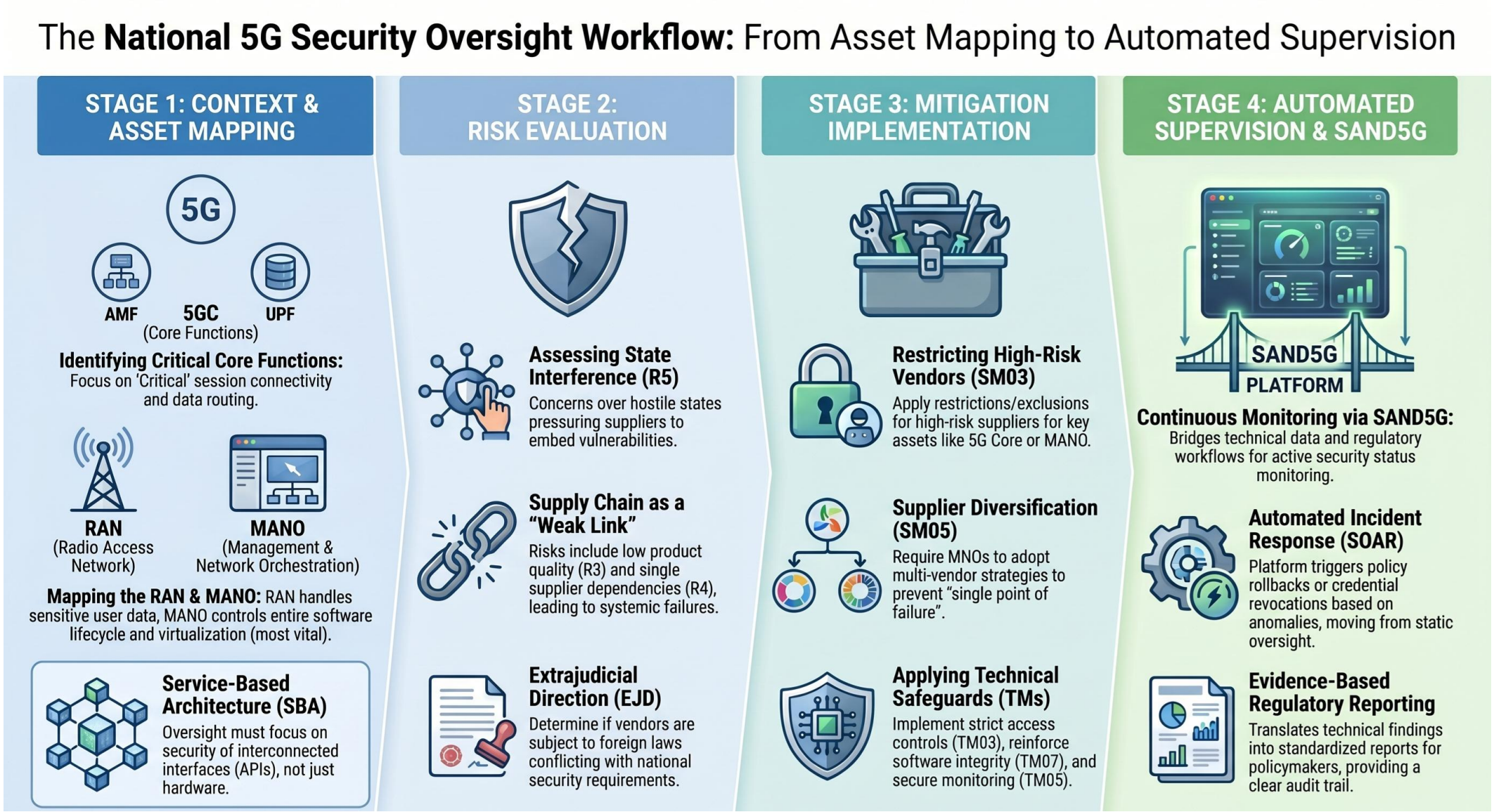


- Use assessments to trigger focused inspections
- Require additional technical controls where weaknesses are found
- Apply restrictions for high-risk suppliers in key assets where justified
- Impose reporting and remediation obligations with deadlines
- Monitor implementation and reassess residual risk
- Escalate persistent or systemic issues through regulatory channels
- Use repeatable evidence to support defensible intervention

Collaborative Oversight: Mobile Network Operators, National Authorities, Regulators, and ENISA

- Operators provide architecture, controls, and incident evidence
- Authorities assess risk, require treatment, and verify compliance
- Regulators connect findings to legal and supervisory powers
- ENISA and EU frameworks support common terminology and coordination
- Cross-agency collaboration improves consistency and resilience
- Shared evidence models reduce duplication and blind spots
- Effective oversight depends on technical and institutional coordination

The National 5G Security Oversight Workflow



Summary: 10 Essential Controls for National 5G Oversight

- **Complete** architecture-aware asset inventories
- **Identify** key assets and sensitive functions
- **Enforce** strong identity, access, and privilege controls
- **Secure** APIs, interfaces, and service-to-service communications
- **Harden** orchestration, MANO, and management planes
- **Monitor** slices, MEC, and distributed environments with criticality awareness
- **Assess** supplier risk using technical and strategic criteria
- **Reduce** concentration and vendor lock-in for key functions
- **Maintain** continuous monitoring, alerting, and audit trails
- **Link** technical findings to formal treatment and regulatory action

Thank you for the attention!

Next 24 questions to answer.

One goal:

Secure the network.

Good luck!

Topic 1: 5G Security Fundamentals & Architecture Shifts (1)

1. **Why is a fundamentally different risk assessment approach required for 5G compared to 4G?**
   A. 5G removes the necessity for vendor-specific risk management due to standardized interfaces.
   B. The shift from hardware-centric to software-defined architecture introduces virtualization and cloud-native risks. (1)
   C. 5G networks utilize centralized processing that eliminates the need for edge-level security oversight.
   D. Traditional models are insufficient because they cannot account for the increased physical security of 5G antennas.

2. **How does network slicing specifically complicate national 5G security oversight?**
   A. It creates a single point of failure by consolidating all user traffic into a single logical pipe.
   B. It removes the requirement for complex orchestration, making monitoring less visible.
   C. It introduces multi-tenancy isolation risks and the potential for cross-slice data leakage. (1)(2)
   D. It restricts the network to a fixed set of functions, preventing dynamic security updates

Topic 1: 5G Security Fundamentals & Architecture Shifts (2)

3. **Why is the shift to a Service-Based Architecture (SBA) a significant security challenge for 5G oversight?**
   A. It requires higher physical security for central data centers compared to 4G.
   B. It moves from static function chains to dynamic, API-driven trust relationships.(1)(2)
   C. It eliminates the need for external network interfaces, concentrating risk internally.
   D. It prioritizes hardware-based isolation over software security protocols.

4. **What factor increases the speed at which threats can propagate across a 5G network compared to previous generations?**
   A. The use of higher frequency millimeter-wave radio bands.
   B. The extensive use of orchestration and automation capabilities.(1)(2)
   C. The significant reduction in the total number of network components.
   D. The centralization of the user plane function within a single facility.

Topic 2: National Risk Procedures & the EU 5G Toolbox (1)

1. **What is the primary relationship between the EU Coordinated Risk Assessment and the 5G Toolbox?**
   A. The Coordinated Risk Assessment serves as a technical manual for hardware installation.
   B. The Toolbox translates the findings of the risk assessment into actionable strategic and technical measures. (1)
   C. The Risk Assessment is a voluntary guideline, while the Toolbox is a mandatory technical standard.
   D. The Toolbox replaces national risk assessments to ensure a single, centralized EU security policy.

2. **According to the ENISA methodology, why is "Asset, Threat, and Vulnerability Mapping" critical for authorities?**
   A. It allows authorities to automate the procurement of new network equipment for operators.
   B. It provides a way to calculate the exact financial revenue loss for a mobile operator.
   C. It creates a "chain of security" that supports proactive oversight instead of reactive response. (2)
   D. It replaces the need for Strategic Measures by focusing purely on hardware vulnerabilities.

Topic 2: National Risk Procedures & the EU 5G Toolbox (2)

3. **How does the ENISA methodology assist National Authorities in moving from reactive to proactive oversight?**
   A. By automating the procurement process for certified network equipment for all operators.
   B. By mapping assets, threats, and vulnerabilities directly to specific toolbox controls.(1)
   C. By replacing diverse national risk assessments with a single, non-negotiable EU standard.
   D. By focusing oversight exclusively on the physical security of telecommunications facilities.

4. **Within the framework of the EU 5G Toolbox, what is the primary role of "Strategic Measures"?**
   A. To define the technical specifications for core network API security.
   B. To address non-technical risks, such as third-party supplier interference or dependency.(1)(2)
   C. To provide real-time, packet-level monitoring of national network traffic.
   D. To coordinate the physical installation of base stations across border regions.

Topic 3: 5G Infrastructure Threats (Core, RAN, and MANO) (1)

1. **Why is the Management and Network Orchestration (MANO) layer considered a "Master Key" risk?**
   A. It is the only component capable of managing legacy 2G/3G signaling vulnerabilities.
   B. Its compromise allows an attacker to simultaneously manipulate or disable functions across multiple slices and domains.(1)
   C. It provides physical access control to the central office facilities where core servers are housed.
   D. It acts as the primary firewall that prevents external API calls from reaching the User Plane Function (UPF).
2. **What unique oversight challenge is presented by Multi-access Edge Computing (MEC)?**
   A. It centralizes all compute functions, making them easier for a single authority to audit.
   B. It eliminates the need for zero-trust models by securing the processing perimeter centrally.
   C. It distributes processing closer to the user, expanding the attack surface and fragmenting trust boundaries.(1)
   D. It prevents the offloading of traffic, thereby simplifying the monitoring and forensics process.

Topic 3: 5G Infrastructure Threats (Core, RAN, and MANO) (2)

3. **Within the 5G Service-Based Architecture (SBA), what is a primary risk identified for critical core functions such as the AMF (Access and Mobility Management Function) and UPF (User Plane Function)?**
   A. These functions rely exclusively on physical cable isolation, making them immune to remote software-based signaling attacks.
   B. API misuse or poor service authentication may enable lateral movement or impersonation across core services. (1)
   C. Compromising these core functions is restricted to local data impact and cannot cascade into national-scale service disruption.
   D. The shift to SBA eliminates the need for trust relationships between network functions, removing the threat of credential theft.

4. **What specific vulnerability can a "protocol fuzzer" exploit in the software-based 5G core network?**
   A. The physical signal attenuation caused by environmental obstacles.
   B. Poorly validated service requests that can crash a Network Function like the AMF.(2)
   C. The lack of geographical diversity in rural radio access points.
   D. The inherent delay in manual intervention by human network operators.

Topic 4: Risk Identification, Evaluation, and Treatment (1)

1. **When applying the 5G Treatment, what is a mandatory requirement for National Authorities when choosing a risk treatment option?**
   - A. Authorities may offload all operational and security responsibility to third-party vendors through service-level agreements (SLAs).
   - **B. All treatment choices, such as restricting high-risk vendors from the Core, must be justified by technical telemetry and forensic data rather than only policy preference.(1)**
   - C. Risk avoidance is the only permitted treatment for high-risk vendors regardless of their network footprint.
   - D. Temporary mitigation measures, such as isolated network segments, are only required during major network topology changes.
2. **Which of the following conditions is a primary "trigger" that should mandate a national 5G risk reassessment?**
   - A. A shift in the retail pricing models offered by a major domestic mobile operator.
   - **B. A major change in the network topology or the discovery of a significant new zero-day vulnerability.(1)**
   - C. The successful completion of a routine annual marketing review by the National Regulatory Authority.
   - D. A vendor's decision to update its corporate logo or global branding strategy.

Topic 4: Risk Identification, Evaluation, and Treatment (2)

3. **In a national 5G impact analysis, what is the "CIA+" assessment designed to evaluate?**
   A. Only the direct financial cost of network downtime for mobile operators.
   B. Confidentiality, Integrity, and Availability plus Signaling Integrity and Identity Privacy.(1)
   C. The maximum download speed available to general consumers in urban areas.
   D. The total number of mobile devices that can connect to a single base station.

4. **According to the 5G Treatment Decision Tree, why is "Transferring" risk through SLAs not applicable?**
   A. Third-party vendors are legally prohibited from signing security-related SLAs.
   B. Operational and security responsibility cannot be fully offloaded to a third party.(2)
   C. Insurance companies do not offer coverage for cybersecurity incidents in telecom.
   D. Risk transfer is only applicable to hardware failures, not software vulnerabilities.

Topic 5: Supply Chain & High-Risk Vendor (HRV) Assessment (1)

1. **Which of the following is a "Strategic Indicator" that must be evaluated when identifying a high-risk vendor?**
   A. The specific frequency range at which the vendor's radio equipment operates.
   B. The vendor's susceptibility to interference from third-country governments based on corporate structure.(1)(2)
   C. The average price of the equipment compared to other international suppliers.
   D. The total number of years the vendor has been operating within the European market.
2. **How does a Software Bill of Materials (SBOM) contribute to supply chain integrity in 5G oversight?**
   A. It provides a comprehensive list of all physical hardware components in a data center.
   B. It serves as a legal waiver that transfers all security accountability from the operator to the sub-contractor.
   C. It improves transparency into software component dependencies and potential hidden vulnerabilities.(3)
   D. It automatically generates patches for zero-day vulnerabilities in third-party managed services.

Topic 5: Supply Chain & High-Risk Vendor (HRV) Assessment (2)

3. **What does "hidden coupling" mean in the context of the 5G supply chain ecosystem?**
   A. Two different vendors sharing the same physical base station site or antenna tower.
   B. Seemingly diverse hardware vendors sharing common software components or maintenance teams.(1)
   C. The mandatory end-to-end encryption of all network signaling interfaces.
   D. The contractual relationship between a mobile operator and its retail marketing partners.

4. **Which indicator would trigger a higher risk classification for a vendor, based on their "Network Footprint"?**
   A. A high concentration of equipment in sensitive tiers like the Core or MANO.(2)
   B. A large volume of consumer-grade mobile handsets currently in use by the public.
   C. The presence of a local administrative sales and marketing office within the country.
   D. The total number of years the vendor has been in operation globally.

Topic 6: SAND5G Platform & Technical Oversight (1)

1. **What is the primary function of "Integrated Environmental Awareness" within the SAND5G platform?**
   A. It monitors the physical power consumption and cooling efficiency of 5G data centers.
   B. It maps technical findings to regulated infrastructure and asset topologies for context-aware interpretation.(1)
   C. It provides a universal security score that replaces the need for a national risk assessment.
   D. It automatically identifies the geographical location of all rogue access nodes in real-time.
2. **Why are customizable alert thresholds essential for the SAND5G oversight platform?**
   A. They allow authorities to ignore technical findings that do not align with political priorities.
   B. They enable the platform to align technical monitoring with specific national risk tolerance levels.(2)
   C. They provide a cosmetic dashboard feature used primarily for public relations reports.
   D. They eliminate the need for human analysts by automating all regulatory intervention decisions.

Topic 6: SAND5G Platform & Technical Oversight (2)

3. **How does "Integrated Environmental Awareness" on the SAND5G platform improve national oversight?**
   A. By monitoring the temperature and power efficiency of physical server rooms.
   B. By mapping technical findings to regulated infrastructure for context-aware interpretation.(1)
   C. By predicting the long-term economic costs of national 5G deployment.
   D. By automatically approving all software updates for operators without human review.

4. **Within the SAND5G platform, what is the primary purpose of "Structured Evidentiary Workflows" for National Authorities?**
   A. To automate the daily retail billing and spectrum trading operations of national mobile network operators.
   B. To transfer the legal and operational security responsibility of the network from the operator to the platform developer.
   C. To connect technical telemetry directly to reporting outputs, providing a repeatable basis for formal risk and incident analysis.(1) (2)
   D. To provide a public-facing portal for consumers to report signal quality and coverage issues in rural areas.

References

1. **Michaelides, S., Lenz, S., Vogt, T., & Henze, M. (2025).** *Secure integration of 5G in industrial networks: State of the art, challenges and opportunities*. Future Generation Computer Systems, 166, 107645. DOI: https://doi.org/10.1016/j.future.2024.107645.

2. **European Commission. (2021, March).** *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures* [Factsheet]. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

3. **ENISA. (2022, March).** *5G Cybersecurity Standards: Analysis of standardisation requirements in support of cybersecurity policy*. Authors: François Cosquer, François Zamora, & Alf Zugenmaier. Editors: Erika Magonara & Sławomir Górniak. ISBN: 978-92-9204-568-5. Available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA - 5G Standards.pdf

4. **ENISA. (2020, December).** *ENISA Threat Landscape for 5G Networks: Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)*. Editors: Marco Barros Lourenço, Louis Marinos, & Lampros Patseas. ISBN: 978-92-9204-445-9. Available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA 5G Threat Landscape - Update.pdf

5. **Nair, P. (2021, October 13).** *Securing your 5G infrastructure to the edge and beyond* [Presentation for ENISA]. Cisco Systems. Available at : https://www.enisa.europa.eu/sites/default/files/2024-10/enisa_presso.pdf

6. **Dias, J., Malta, S., & Santos, R. (2026, February 12).** *Security Challenges in 5G Network Slicing: A Risk-Based Analysis and Conceptual Framework*. Journal of Cybersecurity and Privacy (JCP), 6(1), 00035. Available at: https://www.mdpi.com/2624-800X/6/1/35

7. **SAND5G Project. (2024, July 30).** *D2.1: Security analysis for 5G and beyond networks*. Deliverable funded by the European Union's Digital Europe programme under grant agreement No 101127979. Available at: https://sand5g-project.eu/wp-content/uploads/2025/01/public-deliverable-D2.1.pdf

8. **Condoluci, M., & Mahmoodi, T. (2018).** *Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges*. Computer Networks, 146, 65-84. DOI: https://doi.org/10.1016/j.comnet.2018.09.005