SAND5G

https://sand5g-project.eu/

Implementing the EU 5G Cybersecurity Toolbox : From Policy to Operational Excellence

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

Contents

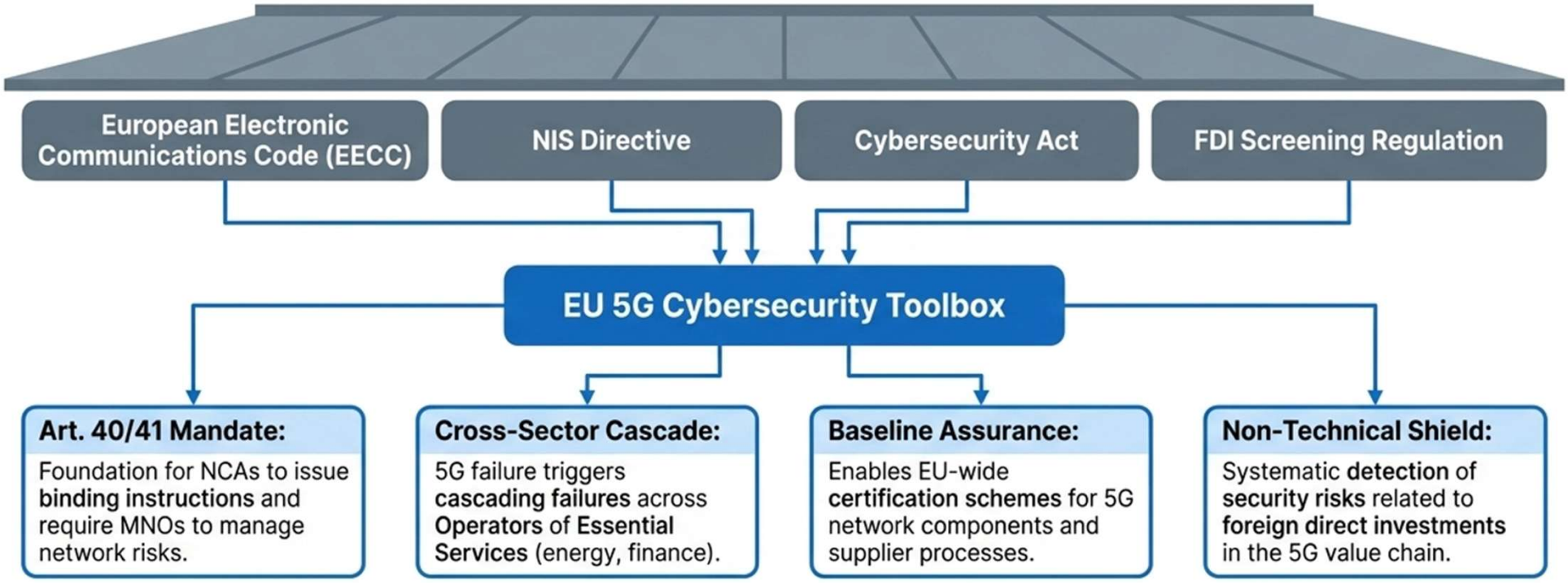
- **Module 1: The Paradigm Shift - The New 5G Security Paradigm**
  - Transition from 4G to 5G
  - The 9 Core Risk Scenarios (R1–R9)
- **Module 2 : Strategic Measures (SM01 – SM08)**
  - Regulatory Powers (SM01-SM02)
  - Supply Chain Integrity (SM03-SM06)
  - Sustainability (SM07-SM08)
- **Module 3: Technical Measures (TM01 – TM11)**
  - Network Security Baseline (TM01-TM02): Moving beyond 3GPP standards to active security management.
  - 5G Specific Controls (TM03-TM07): Deep dive into Virtualization security, strict access controls (least privilege), and on-premise Security Operation Centers (SOC).
  - Resilience (TM11): Business continuity and physical security of sensitive assets like Edge Computing nodes.

Contents

The Paradigm Shift: From 4G Evolution to 5G Revolution

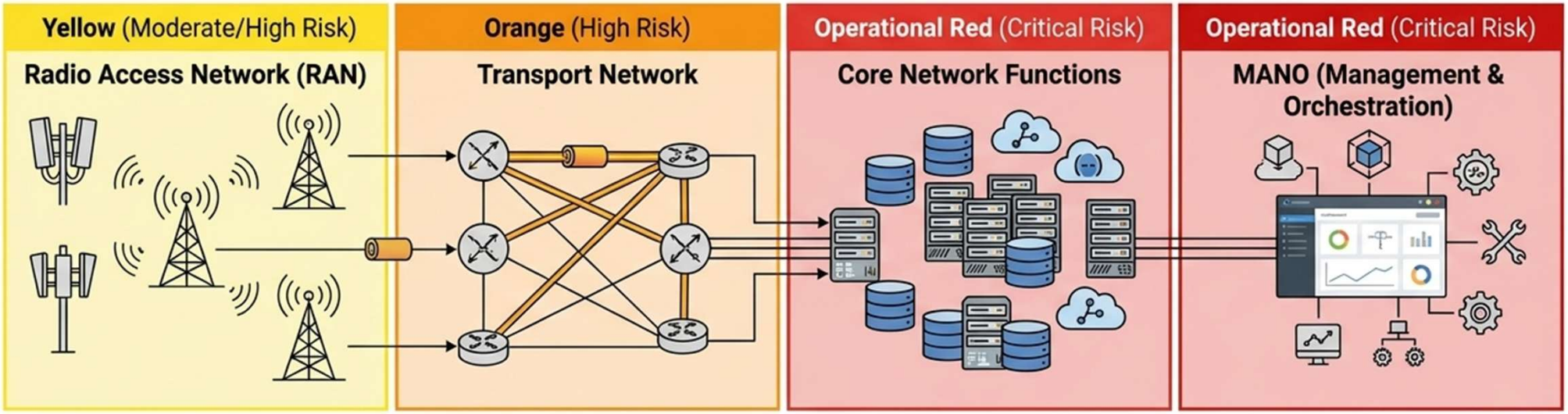
DIMENSION	4G LEGACY	5G REVOLUTION
Architecture	Dedicated, closed proprietary hardware.	Virtualized Network Functions (VNFs) & Software-Defined Networking (SDN). Continuous software integrity is paramount
Ecosystem	Direct, linear MNO-vendor relationships.	Complex value chain relying on third-party Managed Service Providers, systemic integrators, and open-source components.
Attack Surface	Centralized core routing.	Decentralized. Multi-access Edge Computing(MEC) pushes core functions closer to users, multiplying logical entry points.
Criticality	Primary concern: Data confidentiality.	Primary concern: Availability and integrity. 5G forms the backbone for critical national infrastructure (energy, health).

The Regulatory Continuum: Building on Existing EU Frameworks



Mapping the 5G Value Chain & Asset Criticality

Asset Sensitivity Heat Map embedded sectionav within in a functional 5G network topology



Growing in sensitivity as edge computing introduces core-like functions physically closer to access sites.

Critical routing hubs connecting decentralized edge nodes to the central core.

The “brain” of the network (authentication, slicing). Compromise here breaks the integrity of the entire network.

Controls the virtualized network. Compromise allows for catastrophic network-wide sabotage and espionage.

The 5G Threat Landscape: Synthesizing the 9 Core Risk Scenarios

Quadrant I: Insufficient Security Measures
R1: Misconfiguration of networks.
R2: Lack of access controls.

Quadrant II: 5G Supply Chain Risks
R3: Low product quality.
R4: Single supplier dependency.

Quadrant III: Modus Operandi of Threat Actors
R5: State interference.
R6: Organized crime exploitation.

Quadrant IV: Interdependencies & Devices
R7: Disruption of critical infrastructure.
R8: Massive power failure.
R9: IoT exploitation.

Threat Dossier [R1]: Misconfiguration of Networks

[Category: Insufficient Security**]** | **[Primary Threat Actor:** State / Hacker**]** | **[Affected Assets:** Core, Edge (MEC)**]**

Threat Actor
State actor or malicious hacker targeting the decentralised architecture.

Attack Vector
Exploits poorly configured software rules at the external interfaces or Multi-Access Edge Computing (MEC) nodes.

Impact
Unauthorised network-wide access. SDN allows a single misconfiguration to propagate and compromise core functions in milliseconds.

Regulatory Mitigation Map
TM01/TM04 (**Automated Auditing**): NCAs must mandate strict baseline security frameworks, continuous automated auditing, and rigorous virtualisation isolation protocols to prevent NFV sprawl. Static, annual IT audits are obsolete.

Threat Dossier [R2]: Lack of Access Controls

[Category: Insufficient Security**]** | **[Primary Threat Actor:** Insider / Subcontractor**]** | **[Affected Assets:** Core, Transport, MANO**]**

Threat Actor

A subcontractor with administrator privileges or a rogue staff member.

→

Attack Vector

Performs adverse operational actions due to legal requirements imposed by a third country, rogue behaviour, or poor segregation of duties.

→

Impact

Confidentiality, integrity, or availability breach, allowing unrestricted lateral attacker movement into critical core nodes.

Regulatory Mitigation Map

TM03 (Strict Access Controls & Segregation): Enforce the Principle of Least Privilege. Network administrator rights must be permanently severed from operational user rights. Supplier remote access must be drastically minimised, authenticated, and heavily logged.

Threat Dossier [R3]: Low Product Quality

[Category: Supply Chain] | [Primary Threat Actor: State / Supplier] | [Affected Assets: Virtualised Functions, Core]

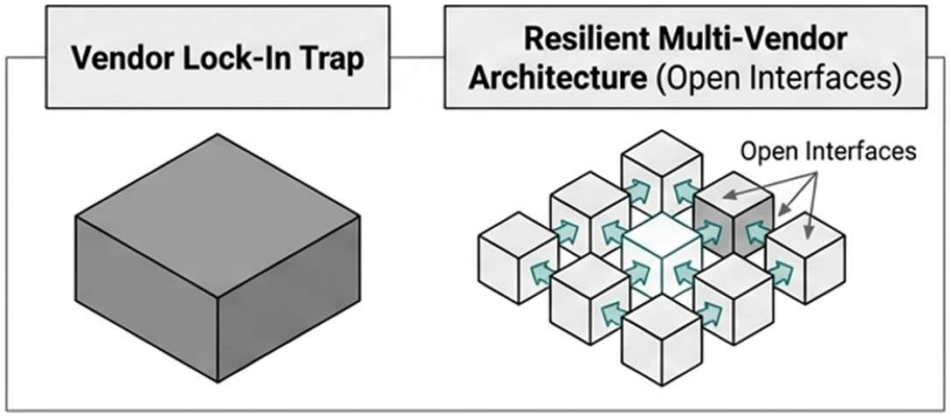
Regulatory Mitigation Map

TM07 / TM09 (Patch Management & EU Certification): Mandate cryptographic verification of patches in isolated MNO sandbox environments before live deployment. Transition national procurement guidelines to mandate EU Certified components (ENISA schemes).

Threat Dossier [R4]: Single Supplier Dependency

[Category: Supply Chain] | **[Primary Threat Actor:** Geopolitical/Commercial Market] | **[Affected Assets:** RAN, Core]

Threat Actor	Attack Vector	Impact
Trade sanctions or commercial collapse of a monopolistic supplier.	Sudden, drastic reduction in equipment availability, proprietary updates, and technical support.	Systemic network degradation. Quality drops as MNOs prioritize basic network survival and supply over proactive security patching.



Regulatory Mitigation Map

SM05 (Mandating Interoperability): Multiple suppliers are irrelevant if technical dependencies make switching financially impossible. Regulators must review operator procurement plans ex-ante to mandate true open interfaces.

Threat Dossier [R5]: State Interference

[Category: Threat Actor Modus Operandi] | **[Primary Threat Actor:** Hostile Non-EU State] | **[Affected Assets:** Core, Management]

Threat Actor
Foreign state actor operating entirely outside of EU legal jurisdiction.

Attack Vector
Exercises covert or extra-jurisdictional legal pressure over an equipment supplier lacking democratic checks and balances

Impact
Embedded backdoors and vulnerabilities are deployed into sensitive network assets, enabling massive-scale espionage or disruption during geopolitical crises

Regulatory Mitigation Map

SM03 (Defining 'High-Risk'):
Implement legally binding Risk Profiles. Apply outright statutory prohibitions on high-risk suppliers touching sensitive network elements (Core/MANO). This risk cannot be patched with software; it requires regulatory exclusion.

Threat Dossier [R6]: Organised Crime Exploitation

[Category: Threat Actor Modus Operandi] | **[Primary Threat Actor:** Organised Crime Group] | **[Affected Assets:** Entire Network, End-Users]

Regulatory Mitigation Map

TM01 / TM05 (SOC/NOC Sovereignty): Mandate that Network Operations Centers (NOCs) and Security Operations Centers (SOCs) reside physically within the EU jurisdiction. Limit outsourcing and require real-time threat detection linked to national CSIRTs.

Threat Dossier [R7]: Disruption of Critical Infrastructure

[Category: Interdependencies] | **[Primary Threat Actor:** Malicious Hackers / States] | **[Affected Assets:** Network Slices, Essential Services]

Regulatory Mitigation Map

TM11 (Resilience & Continuity): MNOs must legally guarantee Service Level Agreements (SLAs) for essential services. Mandate disaster recovery audits and cross-sectoral tabletop exercises to test business continuity under active duress.

Threat Dossier [R8]: Massive Power Failure

[Category: Interdependencies] | **[Primary Threat Actor:** State / Crime / Natural Event] | **[Affected Assets:** Entire Network Backbone]

Threat Actor	Attack Vector	Impact
Natural disaster, State-level sabotage, or Crime group targeting national infrastructure.	Kinetic or cyber attack on the national energy grid resulting in a massive, prolonged power outage.	Circular dependency collapse. 5G goes offline without power, while the decentralised smart grid cannot balance loads without the 5G network.

Regulatory Mitigation Map

TM11 (Resilience & Continuity): Treat 5G resilience as a National Security matter. Mandate joint risk assessments between MNOs and Energy Operators to design redundant power failovers specifically for critical routing nodes.

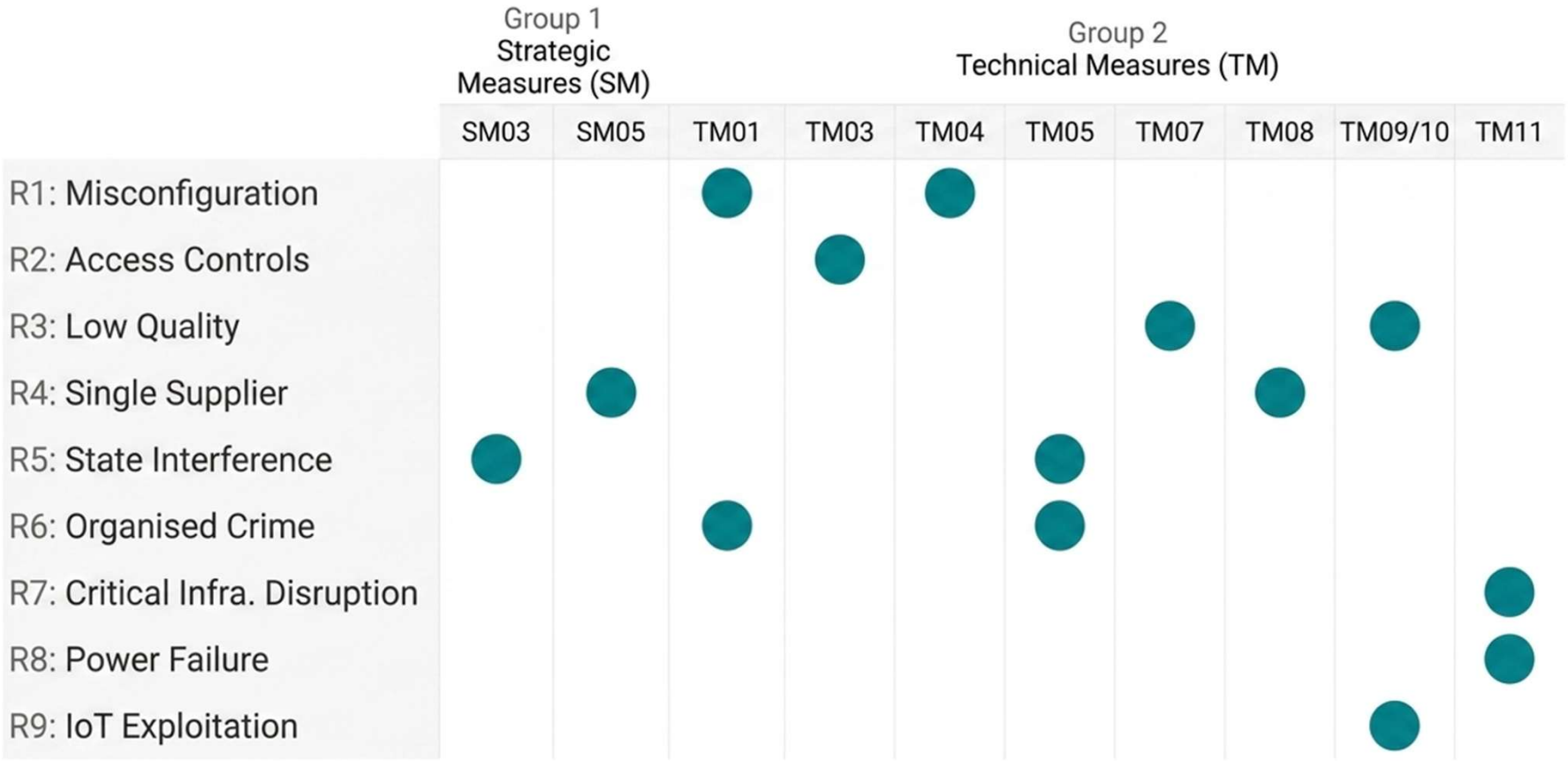
Threat Dossier [R9]: IoT Exploitation

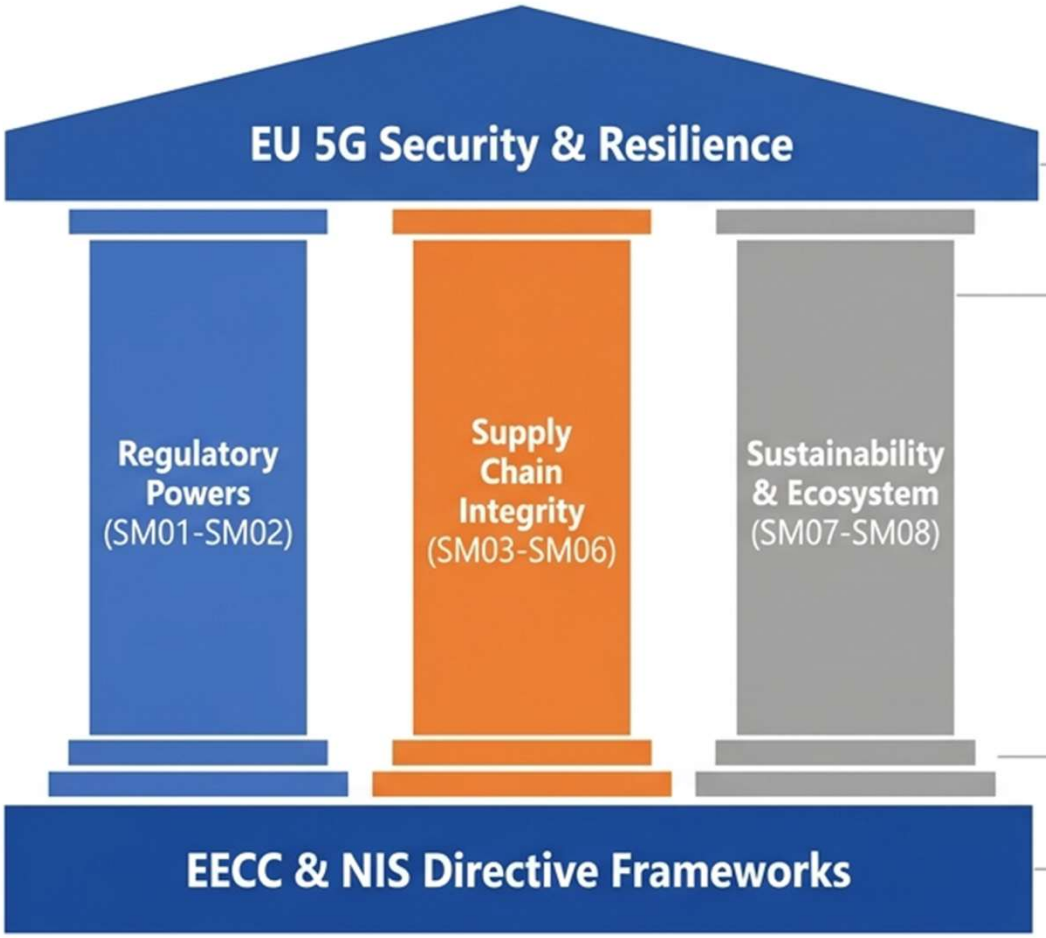
[Category: End User Devices] | **[Primary Threat Actor:** Hacktivist / State] | **[Affected Assets:** Signalling Plane, Edge]

Regulatory Mitigation Map

TM10 (Securing the Periphery): Extend EU certification requirements beyond 5G-specific infrastructure. Mandate security standards for connected end-user IoT devices and cloud services that interface directly with the network edge.

The Master Mitigation Matrix: Correlating Risks to Regulatory Action





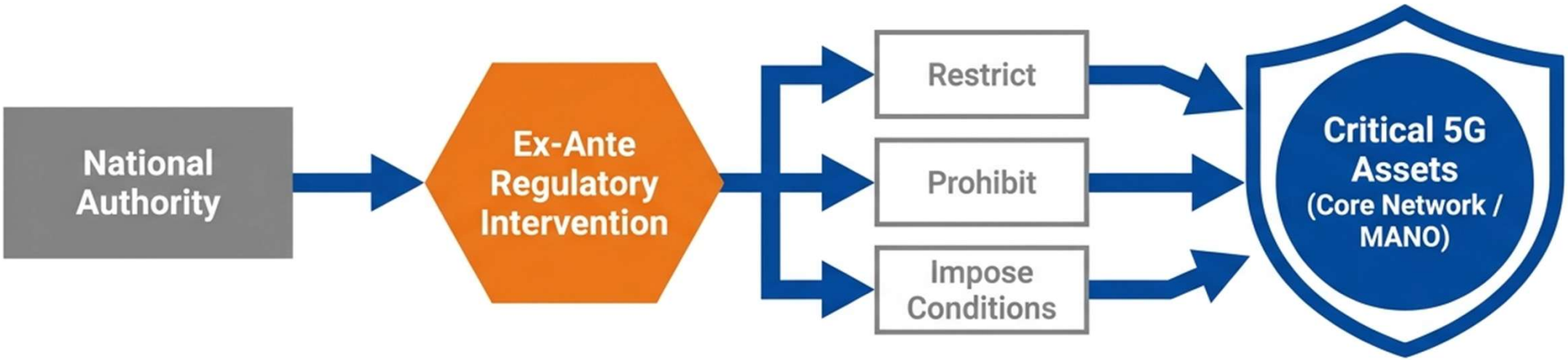
The Paradigm Shift: 5G's software-defined architecture demands a transition from reactive technical patching to proactive strategic governance.

Defining Strategic Measures (SM): Non-technical, systemic interventions addressing vulnerabilities like foreign state interference, supplier dependency, and supply chain fragility.

The Legal Anchors: Strategic measures operate as an extension of established EU frameworks, specifically the NIS Directive and the EECC.

Bridging Policy to Operations: National Competent Authorities (NCAs) must translate these EU-coordinated recommendations into binding national legislation to avoid market fragmentation.

Implementation Reality: Strategic measures are high-impact but require significant legislative effort and long-term economic calibration to balance national security with sector innovation.

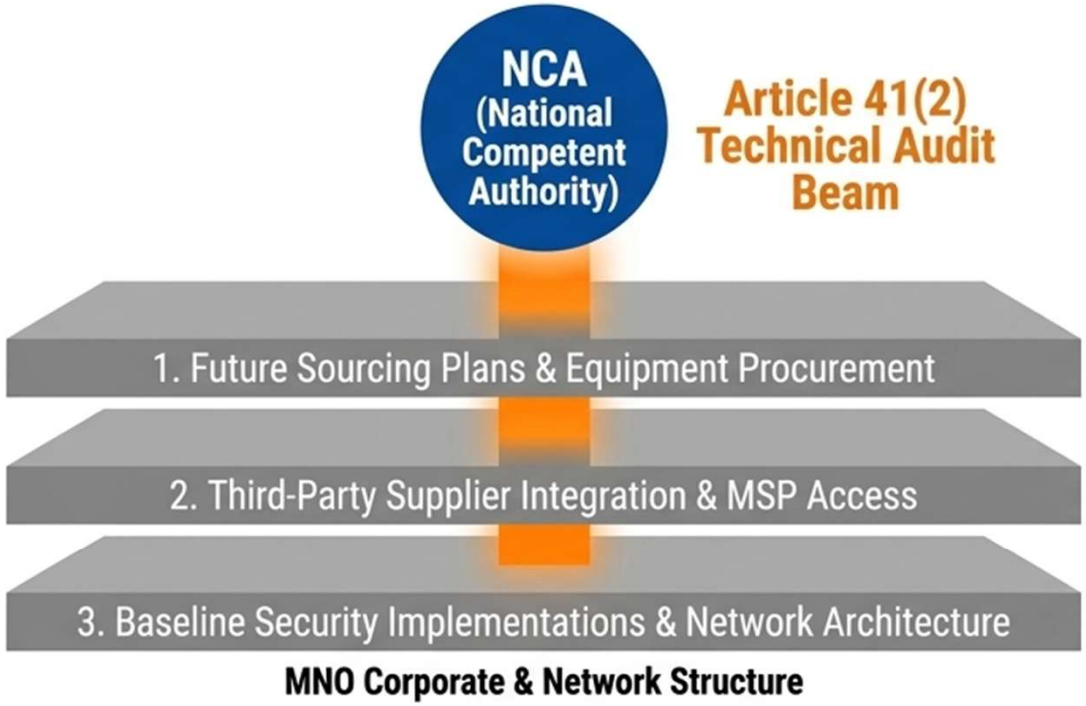


- **Shift to Proactive Governance:** SM01 requires NCAs to possess and exercise ex-ante (preventative) powers rather than relying solely on post-incident penalties.
- **Targeting the Core:** Authorities must be empowered to legally prohibit the use of equipment from 'High-Risk' suppliers for critical assets.
- **Mandating Operator Obligations:** Regulatory powers must allow the imposition of strengthened, binding security obligations on MNO signaling and management planes.

National Security Imperative: Decisions to restrict suppliers must incorporate intelligence regarding the risk of interference by non-EU countries in the 5G supply chain.

Implementation Factor: Establishing these powers requires low resource costs for NCAs but will have a high sector-specific economic impact due to forced MNO procurement sment shifts.

SM02: Auditing & Information – The Enforcement Lever



Supply Chain Visibility: Regulators must compel MNOs to provide detailed, up-to-date documentation on future 5G equipment sourcing and third-party supplier integration.

Capability Building: Auditing 5G requires specialized expertise. NCAs must invest in or contract Information Systems security audit providers versed in telecommunications.

Baseline Verification: Operators must prove how baseline technical network security measures are actively implemented, not just conceptually designed.

Invoking EECC Article 41(2): NCAs must exercise their right to mandate in-depth, technical security audits of MNOs, focusing on critical components and sensitive network parts.

Implementation Factor: Conducting rigorous, deep-dive technical audits carries significant resource costs (financial and human capital) for both the NCA and the MNOs.

SM03: Supplier Risk Profiles & High-Risk Exclusions

Beyond Technical Flaws: Assessing a supplier's risk profile must incorporate non-technical vulnerabilities, specifically the likelihood of interference from a non-EU country.

Continuous MNO Assessment: Operators must enforce rigorous supply chain audits and manage residual risks for any equipment sourced from non-excluded, but elevated-risk, vendors.

Key Risk Indicators: Evaluate strong links between the supplier and foreign governments, the absence of democratic checks and balances, and corporate ownership opacity

Mandatory Exclusions: Suppliers deemed "High-Risk" must be strictly restricted or entirely excluded from critical and sensitive key assets (Core Network, Orchestration functions).

Implementation Factor: Excluding established suppliers will trigger short-to-medium-term spikes in sector-specific deployment costs and may delay 5G rollouts.

SM04: Securing Operational Boundaries (Managed Services)

The Outsourcing Risk: Managed Service Providers and 3rd-line equipment support represent severe vulnerabilities if granted unchecked administrative access.

Imposing Legal Limits: Establish regulatory boundaries on what functions MNOs are legally permitted to outsource, particularly in security and network operations centers.

High-Risk MSP Restriction: If an MSP is evaluated as a "High-Risk" entity under SM03 criteria, they must be strictly restricted from sensitive parts of the 5G network.

Principle of Least Privilege: Mandate enhanced security provisions, strict access controls, and comprehensive logging for any remote access granted to third-party support.

Implementation Factor: Forcing MNOs to insource operations or switch MSPs carries moderate resource costs but heavily impacts MNO operational models.

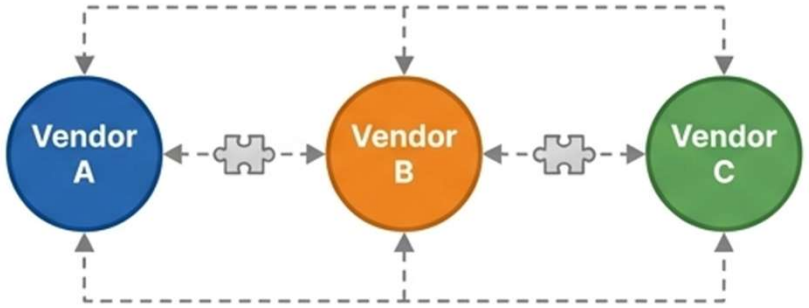
SM05: Multi-Vendor Strategy & Preventing Lock-In

Vendor Lock-In

⚠ Single Point of Failure: Monoculture Threat

Heavy reliance on a single supplier within an individual network creates severe dependencies, turning commercial failures or sanctions into catastrophic outages.

Multi-Vendor Ecosystem



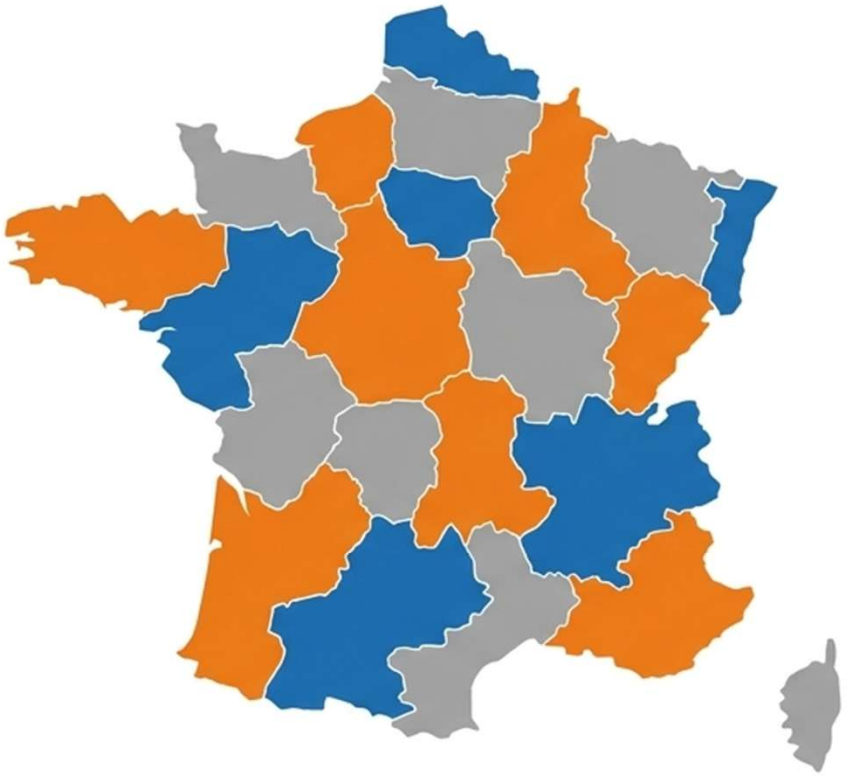
Resilience & Interoperability

Mandating Diversity: Regulators must require each MNO to document and execute an appropriate multi-vendor strategy, ensuring technical viability across radio and core networks.

Breaking Vendor Lock-In: It is not enough to simply use multiple vendors; authorities must ensure MNOs demand open interoperability to prevent technical dependencies that make switching impossible maintain a high-risk supplier.

Implementation Factor: Transitioning to interoperable, multi-vendor networks increases short-term capital expenditure (CAPEX) for MNOs but drastically reduces long-term systemic risk.

SM06: Macro-Resilience at the National Level



Beyond the Individual MNO
SM06 elevates the regulatory view from individual operator networks to the macroeconomic resilience of the entire nation's telecommunications infrastructure.

Nationwide Supplier Balance
NCAs must track the aggregate market share of suppliers across all MNOs to prevent a single point of failure at the national level.

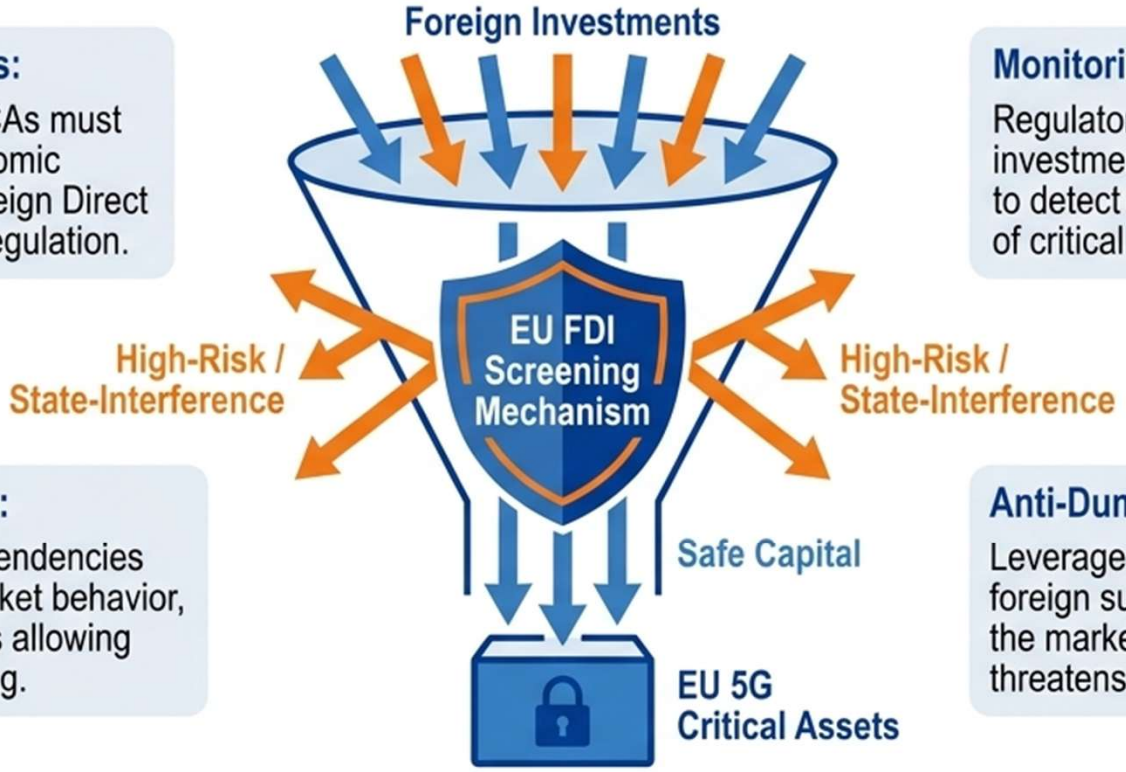
Geographic and Demographic Calibration
Authorities must ensure that a single supplier's failure would not simultaneously knock out networks in all major population centers or critical geographic zones.

Coordinated Incident Impact
Evaluate what happens to national critical services (e.g., energy grids, emergency responders) if one specific supplier's equipment is compromised universally.

Implementation Factor: Requires high cross-operator coordination by the NCA. Resource costs for the regulator are medium, but societal protection impacts are incredibly high.

SM07: Defending the Value Chain via FDI Screening

Protecting Sovereign Assets:
5G infrastructure is critical. NCAs must collaborate with national economic ministries to utilize the EU Foreign Direct Investment (FDI) Screening Regulation.



Monitoring Corporate Acquisitions:
Regulators must actively monitor investments across the 5G value chain to detect foreign state-backed buyouts of critical European tech providers.

Trade Defense Mechanisms:
Authorities should identify dependencies caused by trade-distorting market behavior, such as foreign state subsidies allowing artificially low equipment pricing.

Anti-Dumping Interventions:
Leverage EU anti-dumping rules if foreign suppliers attempt to monopolize the market through unfair pricing, which threatens supply diversity.

Implementation Factor: Primarily impacts broader economic and trade policies rather than direct MNO operations, requiring cross-ministerial cooperation.

SM08: Fostering European Capacities & R&D

Avoiding Long-Term Dependency: True security requires viable, competitive alternatives in the market. SM08 focuses on building native EU capacity in 5G and post-5G (6G) technologies.

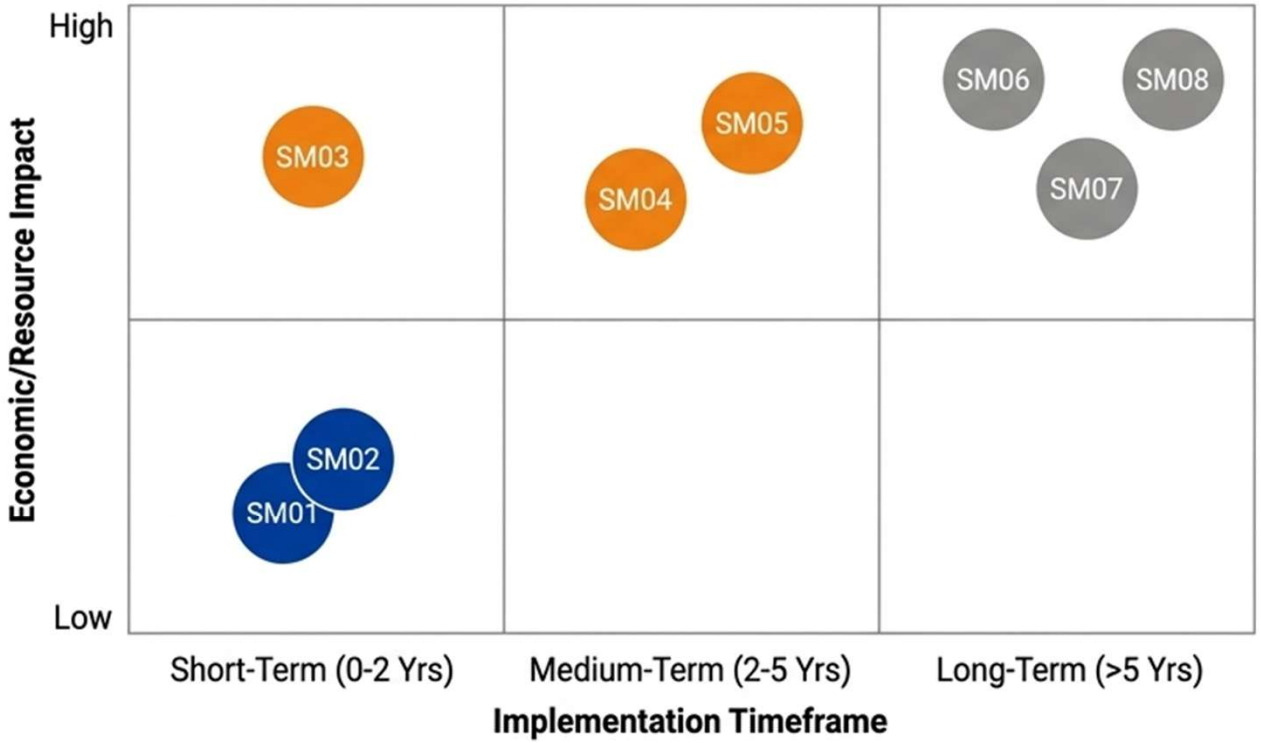
IPCEI Initiatives: Support Important Projects of Common European Interest (IPCEI) to overcome market failures in the telecommunications value chain through large-scale public-private partnerships.

Leveraging EU Funding: NCAs should encourage local industry and academia to participate in Horizon Europe, CEF Digital, and the Digital Europe Programme.

Public Procurement Leverage: Ensure public sector 5G deployment projects explicitly factor in cybersecurity risks and do not award contracts based solely on the lowest price.

Implementation Factor: This is a **long-term strategy** (>5 years) aimed at fostering innovation, requiring significant public financial resource investment.

Synthesis Matrix: Strategic Measures Implementation Roadmap



Short-Term / Immediate Action (0-2 Years)

- **SM01 & SM02**: Establish legal ex-ante powers and mandate MNO audits. (Low regulatory cost, immediate security yield).
- **SM03**: Define risk profiles and exclude high-risk vendors from the core.

Medium-Term / Structural Shifts (2-5 Years)

- **SM04 & SM05**: Phase out high-risk MSPs and enforce MNO multi-vendor interoperability. (High sector economic impact, requires procurement cycles).

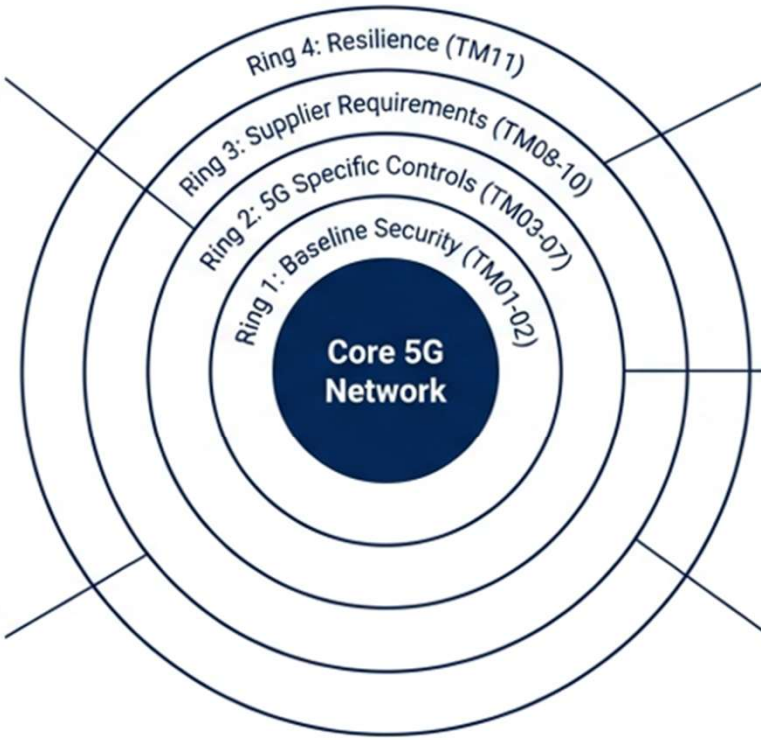
Long-Term / Ecosystem Resilience (>5 Years)

- **SM06 & SM07**: Balance the national geographic vendor layout and embed FDI screening.
- **SM08**: Invest in native EU technology capacities and 6G R&D.

Guiding Principle: Security cannot be deferred. Implement policy powers (SM01) immediately to legally force the medium and long-term supply chain transitions.

Module 3 Overview: The Technical Measures (TM) Framework

The Operational Shield



Operationalizing the Toolbox: Bridges the gap between overarching strategic legislation and day-to-day 5G technical realities.

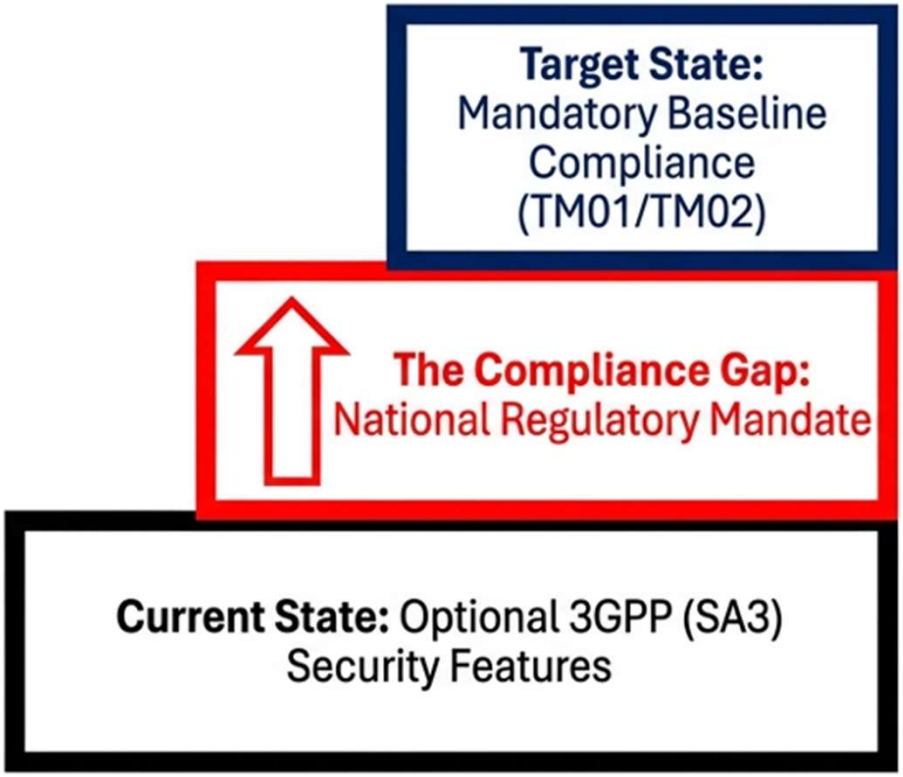
A Layered Defense Paradigm: TMs mitigate concurrent risks, ranging from misconfiguration (R1) to state interference (R5).

Beyond Vendor Trust: Mandates an operational baseline that assumes a Zero Trust posture regarding external access.

National Adaptability: EU-wide standards with built-in calibration for local market maturity and threat landscapes.

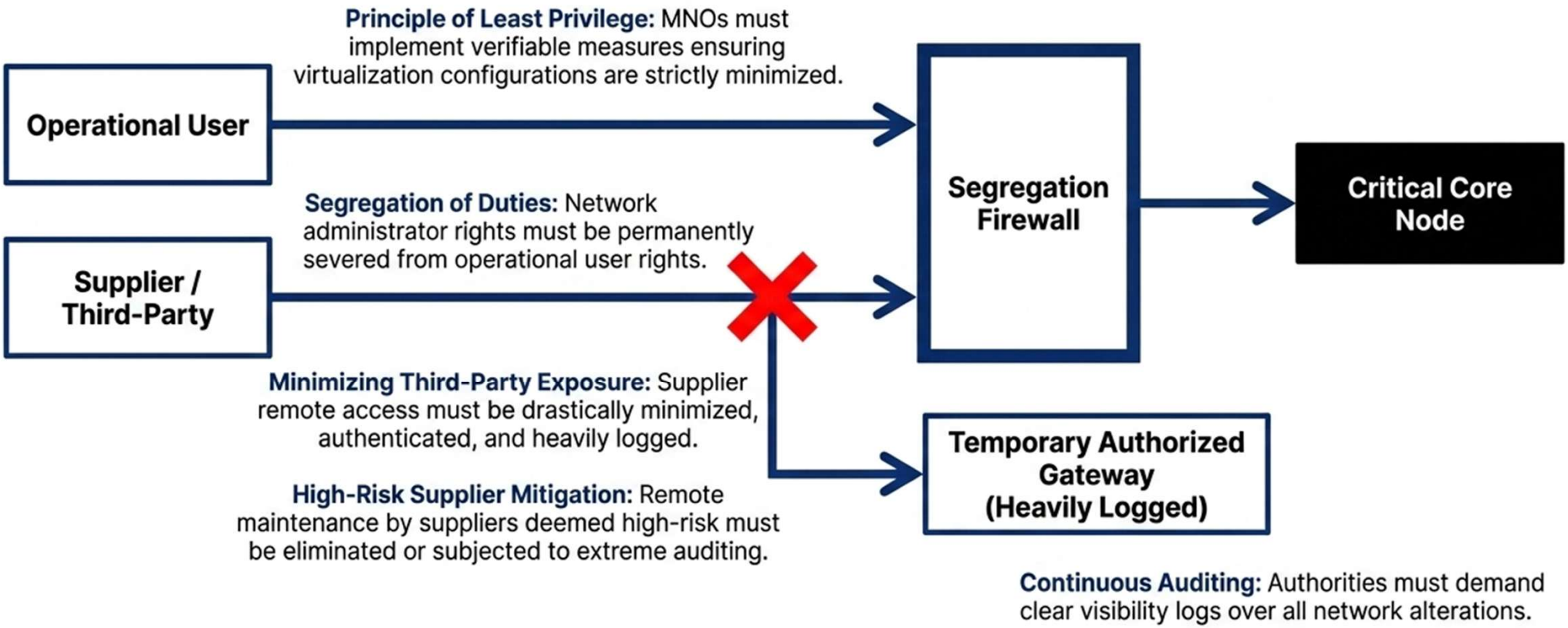
The Regulatory Link: Acts as a direct extension of the NIS Directive (Article 13a) and the European Electronic Communications Code (EECC Articles 40/41).

Establishing the Network Security Baseline (TM01-TM02)

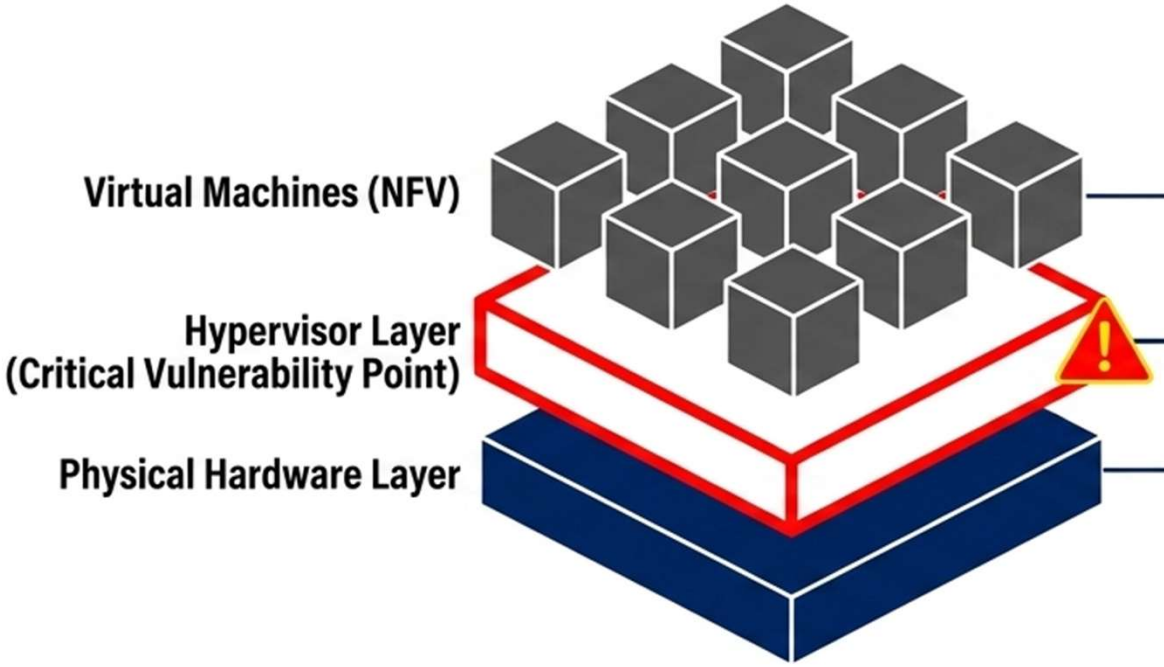


- **Mandating Secure Architecture (TM01):** Operators must document, maintain, and audit product development and daily management procedures.
- **Enforcing 3GPP Standards (TM02):** 5G possesses advanced built-in features, but many remain optional for implementation by suppliers.
- **Closing the Optional Gap:** National authorities must mandate the activation of critical 3GPP protocols to prevent downgrading attacks.
- **Continuous Risk Assessment:** Mobile Network Operators (MNOs) must submit updated assessment plans as network lifecycles evolve.
- **Implementation Profile:** Short-to-medium term timeframe with moderate resource costs for MNOs relying on existing frameworks.

Enforcing Strict Access Controls (TM03)

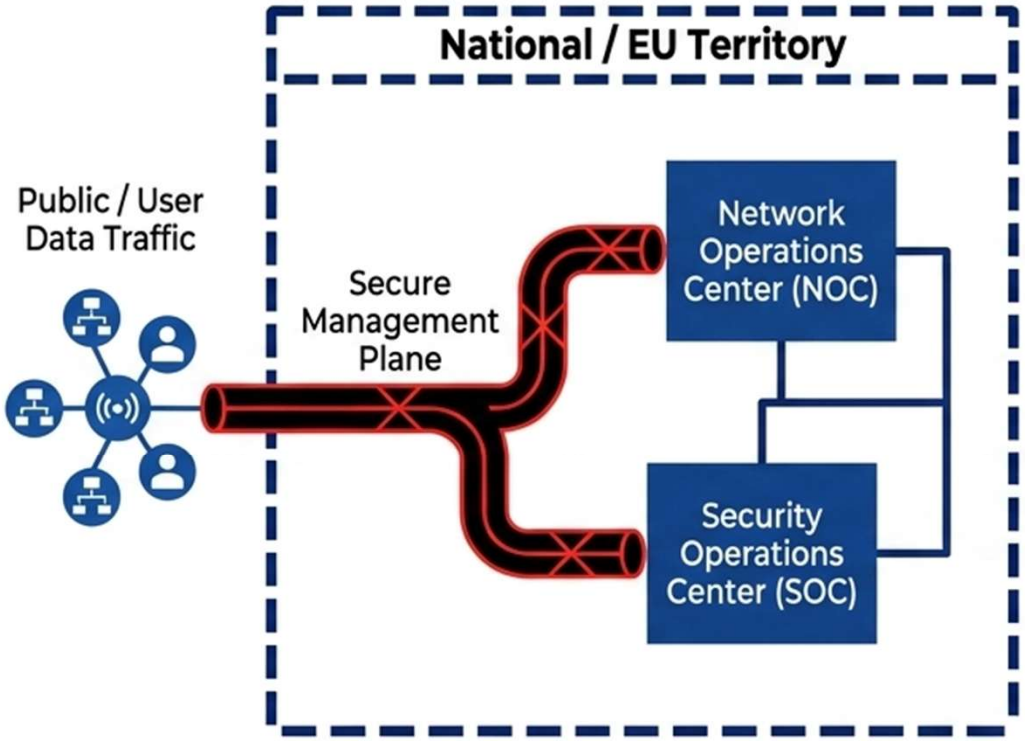


Securing Virtualized Network Functions (TM04)



- **The Software-Defined Shift:** 5G replaces physical appliances with NFV and SDN, radically expanding the attack surface.
- **Hypervisor Integrity:** The virtualization layer is the single point of failure; strict isolation prevents lateral attacker movement.
- **Physical vs. Logical Separation:** Cryptographic key management and core routing may legally require dedicated physical hardware separation.
- **Configuration Vulnerabilities:** Automated configuration auditing is mandatory to prevent R1 (Misconfiguration) in NFV environments.
- **Dynamic Security Posture:** Policies must travel dynamically with the virtual function as it scales across servers.

Sovereignty in Operations: NOCs & SOCs (TM05)



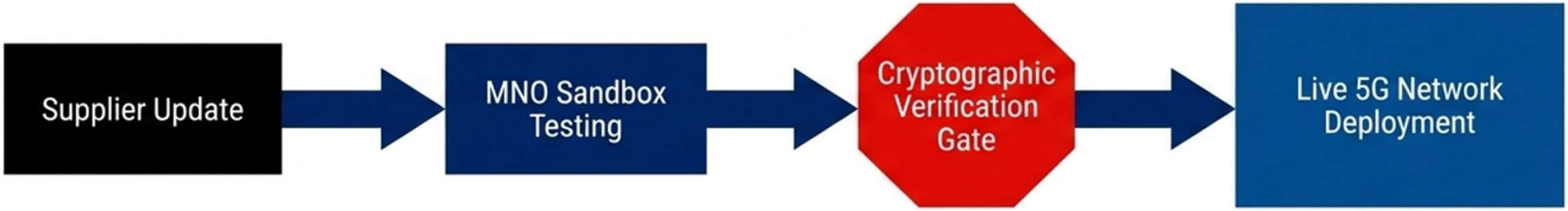
- **In-Country Mandates:** To prevent external sabotage (R5), MNOs must run NOCs and SOCs on-premise, within the nation or EU.
- **Management Plane Protection:** Network management traffic must be strictly segregated from standard user data.
- **Real-Time Threat Detection:** SOCs require clear visibility to detect core threats and compromised IoT device anomalies.
- **Limiting Outsourcing:** Managed Service Providers (MSPs) linked to high-risk suppliers must be prohibited from NOC/SOC operations.
- **Incident Response Integration:** SOCs must plug directly into national CSIRTs for rapid large-scale crisis coordination.

Hardening the Physical Edge (TM06)

4G Centralized Core	5G Distributed Edge
Centralized Data Centers	Multi-Access Edge Computing (MEC)
Few, Highly Secure Locations	Thousands of Public Locations (Hospitals, Factories, Streetlights)
Low Physical Vulnerability	High Physical Vulnerability ⚠

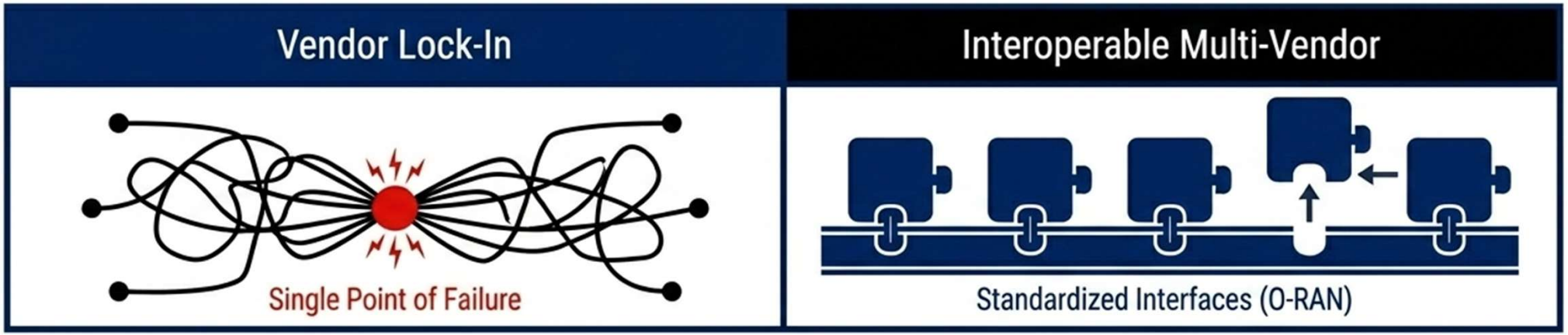
- **The Distributed Vulnerability:** 5G pushes core functions to MEC nodes in public spaces.
- **Risk-Based Physical Protection:** National standards must dictate reinforced security based on deployment criticality (e.g., hospital MEC vs. rural tower).
- **Personnel Vetting:** Physical access to critical base stations must be legally restricted to security-vetted personnel.
- **Third-Party Contractor Limits:** Hardware vendor and integrator physical access must be logged and monitored.
- **Tamper-Evident Infrastructure:** Mandate environmental sensors to instantly detect physical breaches at remote edge locations.

Software Integrity & Patch Management (TM07)



- **The Software-Driven Era:** Malicious code insertion via routine patches is a primary, critical threat vector.
- **Supplier Independence:** MNOs must retain capabilities to test patches in isolated environments without relying on supplier safety assurances.
- **Zero-Day Vulnerability Management:** Regulators must enforce strict SLAs for the prompt application of critical security patches.
- **Cryptographic Verification:** MNOs must deploy automated tools to cryptographically cryptographically verify software signatures before installation.
- **Change Tracking & Rollback:** Immutable logs of configuration changes ensure the network can instantly roll back to a safe state.

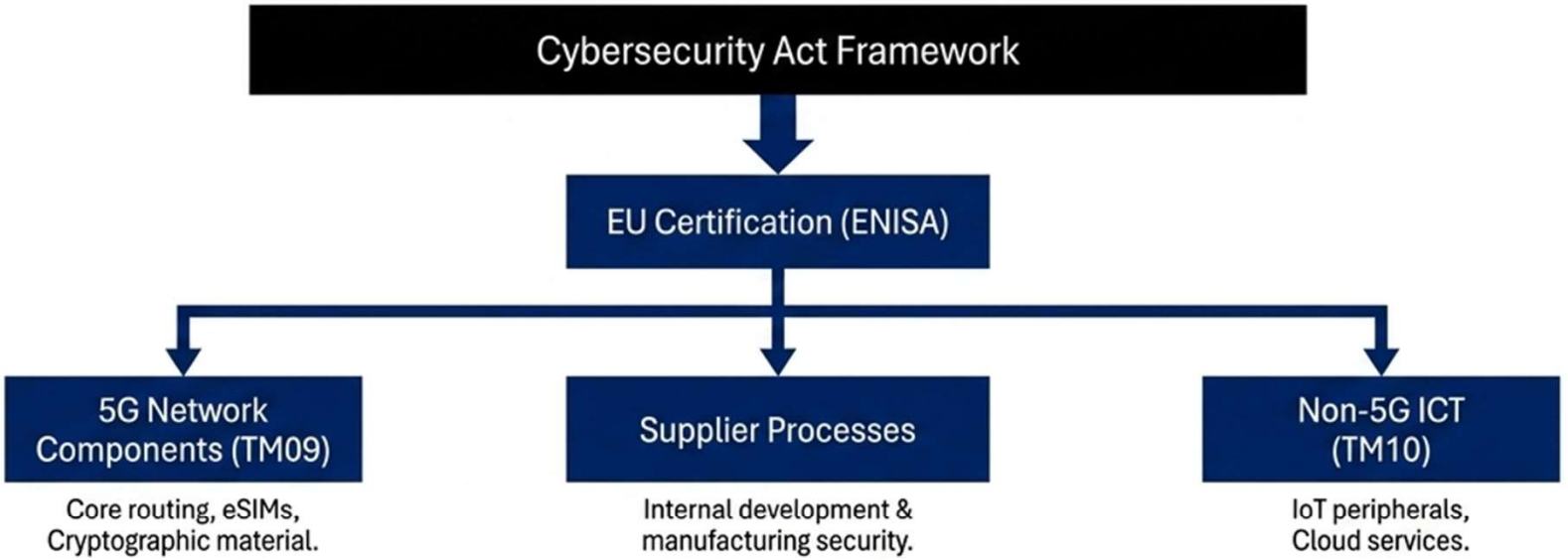
Procurement & The Multi-Vendor Strategy (TM08)



- **Security by Procurement:** RFPs must legally demand lifecycle maintenance guarantees and built-in security processes.
- **Breaking Vendor Lock-In:** Multiple suppliers are irrelevant if technical dependencies make switching impossible; mandate open interfaces.

- **The Regulatory Teeth (SM01):** Authorities can legally block high-risk supplier procurement. TM08 operationalizes this by forcing vendor diversity.
- **Nation-Wide Diversity:** Regulators must monitor the market balance to prevent systemic national failure if one vendor falls.
- **Long-Term Lifecycle Costs:** Initial OPEX/CAPEX for integration prevents the catastrophic economic impact of a single-supplier shock.

Leveraging EU Certification Schemes (TM09 & TM10)

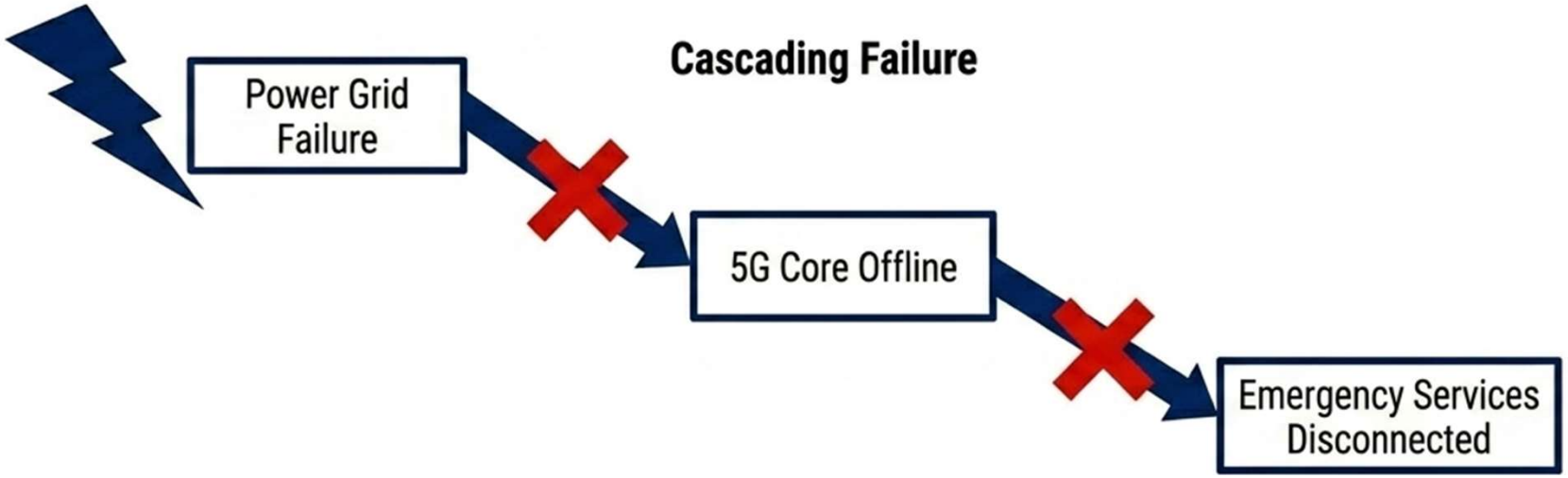


- **A Unified Security Language:** Objective verification that products meet stringent security requirements by design via ENISA schemes.
- **Targeting Critical 5G Components (TM09):** Prioritizing certification for cryptographic material and core routing across the Single Market.

- **Auditing Supplier Processes:** Evaluating the security of the supplier's internal development and manufacturing pipelines.

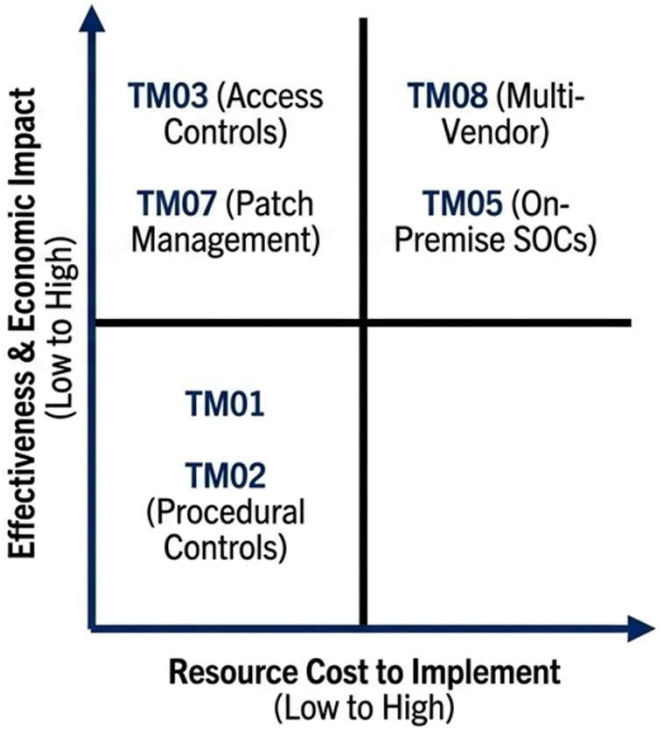
- **Securing the Periphery (TM10):** Extending certification to Cloud services and connected IoT devices where edge vulnerabilities originate.
- **Reducing Fragmentation:** Lowers compliance costs for suppliers while giving MNOs a standardized procurement metric.

Ensuring Resilience and Continuity (TM11)



- **Beyond Cyber Attacks:** Networks must withstand physical disasters, grid failures, and cascading infrastructural collapse (R7 & R8).
- **Mapping Interdependencies:** Operators are required to map out how energy or water supply failures impact 5G availability.
- **Sectoral Cascades:** MNOs must guarantee SLAs via network slicing dedicated to essential services (hospitals, transport).
- **Supplier Continuity Requirements:** Suppliers must prove long-term resilience, providing replacement parts during geopolitical crises.
- **Disaster Recovery Audits:** Regulators must mandate cross-sectoral tabletop exercises to test business continuity under duress.

Implementation Factors: Cost vs. Mitigation Impact



- **High Impact, Low Barrier (Top Left):** TM03 and TM07 offer massive risk mitigation with low structural cost.
- **High Impact, High Investment (Top Right):** TM08 and TM05 require high OPEX but prevent systemic collapse.
- **Sector-Specific Economic Impacts:** Imposing restrictions causes short-term transition costs but safeguards the broader digital economy.
- **Resource Allocation for Regulators:** Authorities must budget heavily for technical auditing personnel to supervise NFV environments.
- **Timeframe Phasing:** Procedural controls are short-term (0-2 years); supplier diversity is a medium-to-long-term objective.

Module 3 Synthesis: The Operational Excellence Blueprint

- **Integration over Isolation:** A secure 5G network requires the synchronized application of all 11 measures across the asset lifecycle.
- **Policy Becomes Code:** National authorities must translate legal text into auditable logs, technical configurations, and procurement mandates.
- **Zero Trust Architecture:** The core theme of TM01-TM11 is the continuous authentication and restriction of every device and supplier.
- **Avoiding Fragmentation:** Rigorous application across Member States is vital to securing the European Single Market.
- **Next Steps (Module 4):** Transitioning to Supporting Actions (SA) and enforcement mechanisms via ENISA and the NIS Cooperation Group.

THE SUPPORT ECOSYSTEM: ANCHORING 5G IN EU FRAMEWORKS

THE ECOSYSTEM ANCHOR

THE NIS DIRECTIVE LINK:

5G cybersecurity operates as a critical extension of existing EU network and information security frameworks, not a standalone silo.

EECC ALIGNMENT:

The European Electronic Communications Code mandates baseline security and incident reporting for all telecom providers, forming the regulatory bedrock.

ROLE OF SUPPORTING ACTIONS (SA01-SA10):

Act as the connective tissue, enabling the effectiveness of Strategic (SM) and Technical (TM) measures across the Single Market.

MARKET HARMONIZATION:

Consistent, cross-border application of SA measures ensures varying national security approaches do not fracture the European telecommunications supply chain.

IMPLEMENTATION FACTOR - RESOURCE COSTS

Leveraging established NIS and EECC compliance teams reduces regulatory burden and operational costs for both operators and authorities.

HARMONIZING SECURITY: EU CERTIFICATION & STANDARDISATION

The Compliance Pipeline

Standardising the Baseline (SA01 & SA04): Developing specific EU guidance to ensure optional security features in 3GPP standards standards are mandated as operational baselines.

Cybersecurity Act Integration: Utilizing the EU Certification framework to mandate verifiable security levels for critical 5G network components and supplier processes.

Mandating Certified Components (SA05): Moving toward an environment where core network and access functions must carry EU-wide certification to be viable for public or private procurement.

Securing Connected Ecosystems: Extending certification requirements beyond 5G-specific ICT to cloud services and end-user IoT devices interfacing with the network.

IMPLEMENTATION FACTOR - ECONOMIC IMPACT

Unified EU certification schemes prevent MNOs from facing 27 distinct national compliance regimes, driving down long-term equipment costs.

INTELLIGENCE SHARING: THE NIS COOPERATION GROUP

THE BIDIRECTIONAL INTELLIGENCE HUB

CENTRALIZED THREAT INTELLIGENCE (SA09):

Utilizing ENISA to continuously update threat landscapes and identify state-backed interference across the Single Market.

RISK PROFILE EXCHANGE (SA06):

Sharing classified insights on supplier risk profiles, ensuring a unified European stance on high-risk vendors based on non-technical vulnerabilities.

ENFORCING MULTI-VENDOR STRATEGIES:

Coordinating efforts to ensure MNOs avoid 'lock-in', where technical dependencies make switching suppliers economically or technically impossible.

INTEROPERABILITY PROMOTION:

Using the Cooperation Group to push for standardized interfaces, guaranteeing equipment from diverse vendors operates seamlessly.

IMPLEMENTATION FACTOR - SECTOR IMPACT

Shared intelligence lowers the individual analytical cost for Member States, though operators may face short-term costs adjusting procurement.

CASE STUDY: EMBEDDING SM01-SM03 INTO NATIONAL LAW

The Regulatory 'Teeth' (SM01): Granting National Authorities ex-ante powers to restrict, prohibit, or impose specific requirements on 5G equipment deployment before installation.

Defining 'High-Risk' (SM03): Assessing non-technical vulnerabilities, including exposure to foreign state interference and a lack of democratic checks and balances.

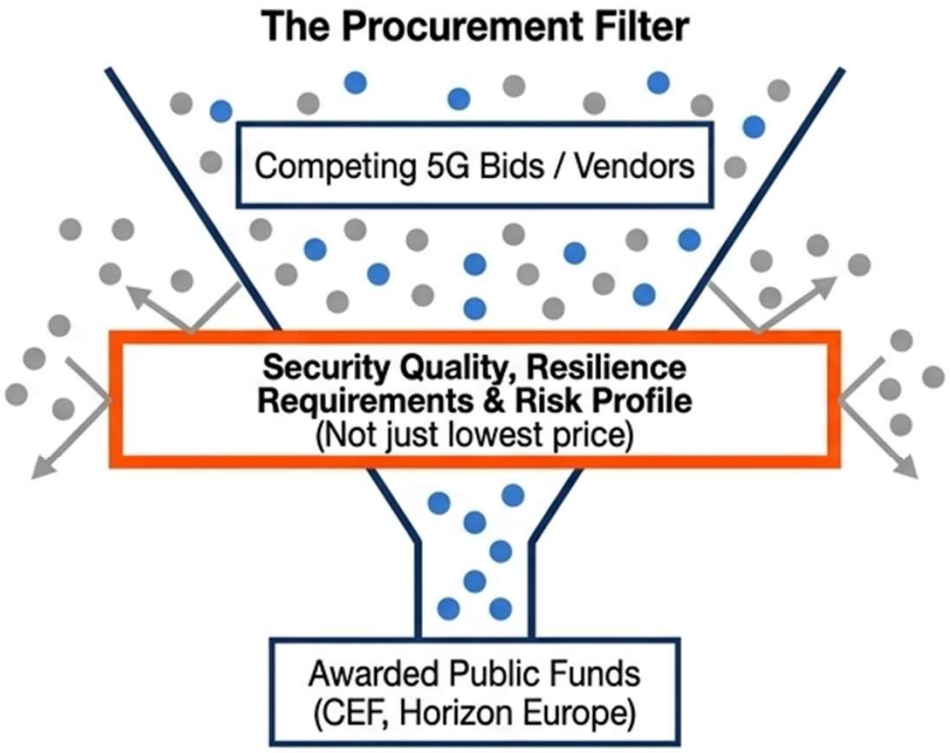
Protecting Critical Assets: Applying outright prohibitions on high-risk suppliers for sensitive elements like Core Network Functions and Network Management Systems.

Deep Technical Audits (SM02): Moving beyond MNO self-assessments; executing independent, national-level technical audits on network architectures and codebases.

IMPLEMENTATION FACTOR - SOCIETAL IMPACT

Excluding high-risk suppliers may delay rollout timelines and increase initial CAPEX, but it mitigates catastrophic national security risks.

Leveraging Public Procurement & Funding (SA10)



Re-evaluating 'Lowest Price': Shifting public procurement frameworks to weigh security, resilience, and supplier risk profiles as heavily as financial cost.

Conditioning EU Funds: Ensuring projects backed by the Connecting Europe Facility (CEF) and Digital Europe strictly adhere to 5G Toolbox mitigations.

Foreign Direct Investment (FDI): Utilizing the EU FDI Screening Regulation to monitor and block hostile investments aiming to capture critical parts of the 5G value chain.

Fostering EU Capacities: Strategically directing state aid and Important Projects of Common European Interest (IPCEIs) to build sustainable, domestic 5G/6G alternatives.

Implementation Factor - Market Dynamics
Strategic procurement reshapes the market, creating financial incentives for suppliers to prioritize built-in security over rapid, cheap production.

Resilience and Cross-Sector Interdependencies (SA07, SA08)

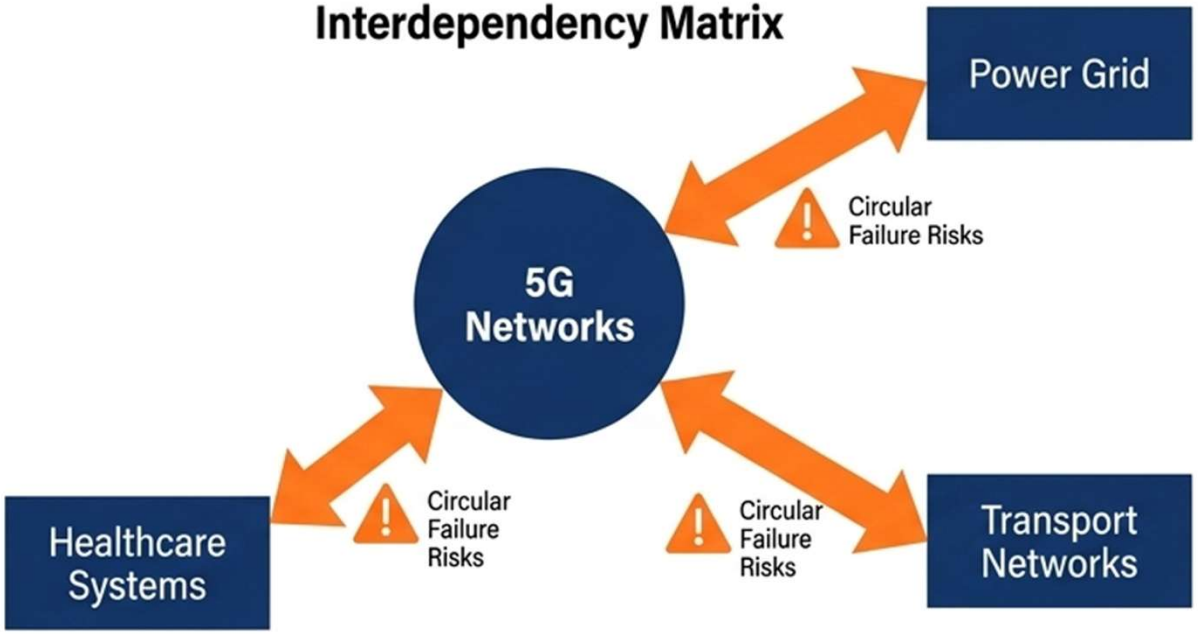
Circular Dependencies (SA08): Recognizing that 5G relies heavily on the power grid, while smart power grids increasingly rely on 5G for telemetry and load balancing.

Cross-Sector Audits: Mandating joint risk assessments between Mobile Network Operators (MNOs) and Operators of Essential Services (OES) under the NIS Directive.

Blueprint for Large-Scale Incidents (SA07): Establishing rapid response protocols for cross-border cyber crises affecting European 5G infrastructure.

National Cyber Exercises: Integrating complex 5G outage scenarios—such as state-backed attacks on edge computing nodes—into national disaster simulation drills.

Implementation Factor - Continuity Costs
Designing networks with redundant power and failover systems increases operational costs but is essential to prevent cascading national blackouts.



Module 5 : Implementation Roadmap

1. RISK PRIORITIZATION

Categorize national assets. Identify critical vulnerabilities via EU Coordinated Risk Assessment methodology.

2. GAP ANALYSIS

Rigorously audit existing Article 13a telecom mitigations to isolate regulatory and operational shortfalls.

3. MEASURE SELECTION

Deploy targeted Strategic (SM) & Technical (TM) measures. effectiveness against implementation friction.

4. FRAMEWORK INTEGRATION

Anchor selected toolbox measures within broader EU frameworks (NIS Directive, EECC).

5. ENFORCEMENT

Utilize ex-ante regulatory powers to mandate strict compliance and exclude high-risk suppliers.

A Methodical Approach to 5G Security:

Transitioning from abstract EU policy to operational excellence requires a structured, step-by-step deployment roadmap tailored to specific national contexts.

REGULATORY IMPLEMENTATION TIP

Avoid 'policy paralysis'. This is not a one-off checklist, but an iterative lifecycle. As 5G architecture evolves—particularly with standalone 5G and edge computing—NCAs must continuously cycle through these five steps.

Steps 1 & 2: Risk Prioritization and Gap Ana

Gap Analysis Blueprint

EU RISK SCENARIO	THREAT ACTOR	AFFECTED ASSETS	MITIGATION STATUS
R1: Misconfiguration	State / Hacker	Core, MANO	
R2: Lack of Access Controls	Insider / MSP	Core, Transport	
R3: Low Product Quality	Supplier	All Assets	
R4: Single Supplier Dependency	State / Commercial	RAN, Core	
R5: State Interference	State-Backed	Core, Management	

CRITICAL OPERATIONAL GAPS IDENTIFIED

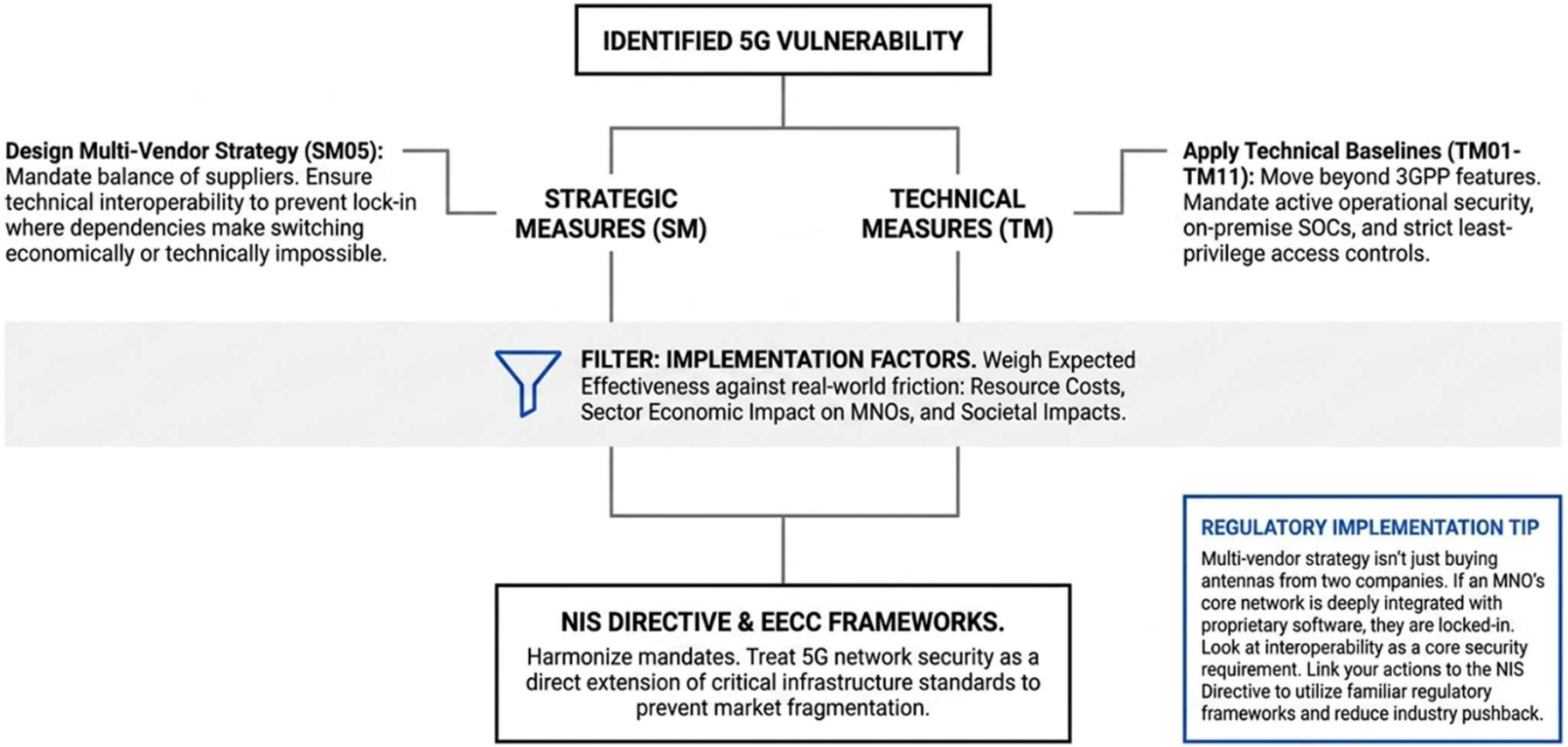
Diagnostic Directives

- **Contextualizing the Threat**: Map R1-R9 against national infrastructure, isolating dependencies like localized power grids.
- **Asset Sensitivity Mapping**: Categorically classify Core network functions, NFV management, and orchestration (MANO) as 'Critical'.
- **Auditing the Existing Baseline**: Comprehensively review legacy mitigations currently enforced under Article 13a.
- **Stakeholder Information Gathering**: Mandate MNOs submit up-to-date sourcing plans and Managed Service Provider (MSP) contracts to assess real market exposure.

REGULATORY IMPLEMENTATION TIP

Information is your primary tool. You cannot regulate what you cannot see. Demand deep-dive technical audits from MNOs. Note that legacy 4G regulations only looked at technical quality; 5G demands you analyze the geopolitical risk profile of the supplier. This is the most significant operational gap today.

Steps 3 & 4: Measure Selection & Framework Integration



REGULATORY IMPLEMENTATION TIP

Multi-vendor strategy isn't just buying antennas from two companies. If an MNO's core network is deeply integrated with proprietary software, they are locked-in. Look at interoperability as a core security requirement. Link your actions to the NIS Directive to utilize familiar regulatory frameworks and reduce industry pushback.

THANK YOU

Questions

- **1. What is the main "Audience Objective" for regulators during the Stage 1 Paradigm Shift?**
- A) To sign new contracts with international vendors
- B) To identify critical assets and map the new decentralized attack surface
- C) To increase the cost of 5G SIM cards
- D) To eliminate the use of cloud computing in telecommunications

Questions

- **2. Under Strategic Measure 01 (SM01), what specific power is granted to National Authorities to provide "regulatory teeth"?**
- A) The power to set monthly subscription prices
- B) Ex-ante powers to restrict or prohibit equipment deployment before installation
- C) The authority to manage the social media accounts of MNOs
- D) The power to tax vendor profits at a higher rate

Questions

- **3. How does the Toolbox define a "High-Risk" supplier (SM03)?**
- A) Based strictly on the physical durability of their hardware
- B) Based on the company's annual revenue and market share
- C) Based on non-technical vulnerabilities, such as exposure to foreign state interference
- D) Based on whether the supplier offers the lowest price in the market

Questions

- **4. Which security concept is a core focus of Technical Measures?**
- A) Password-only authentication
- B) Zero Trust architecture and Network Functions Virtualization (NFV) security
- C) Physical perimeter fencing for all 5G towers
- D) Manual data entry for all network logs

Questions

- **5. How does the NIS Cooperation Group function as a "Bidirectional Intelligence Hub"?**
- A) By selling 5G equipment to Member States
- B) By exchanging Threat Intelligence (SA09) and Supplier Risk Profiles (SA06) between authorities
- C) By acting as a central bank for telecommunications funding
- D) By managing the customer service departments of European MNOs

Questions

- **6. In the Interdependency Matrix (SA08), why is the relationship between 5G and the Power Grid considered "circular"?**
- A) Because they are owned by the same companies
- B) Because 5G relies on the grid for power, and smart grids rely on 5G for load balancing
- C) Because they both use the same type of copper wiring
- D) Because the EU mandates they use circular logos in their branding

Answers

- 1. Correct Answer: B
- 2. Correct Answer: B
- 3. Correct Answer: C
- 4. Correct Answer: B
- 5. Correct Answer: B
- 6. Correct Answer: B