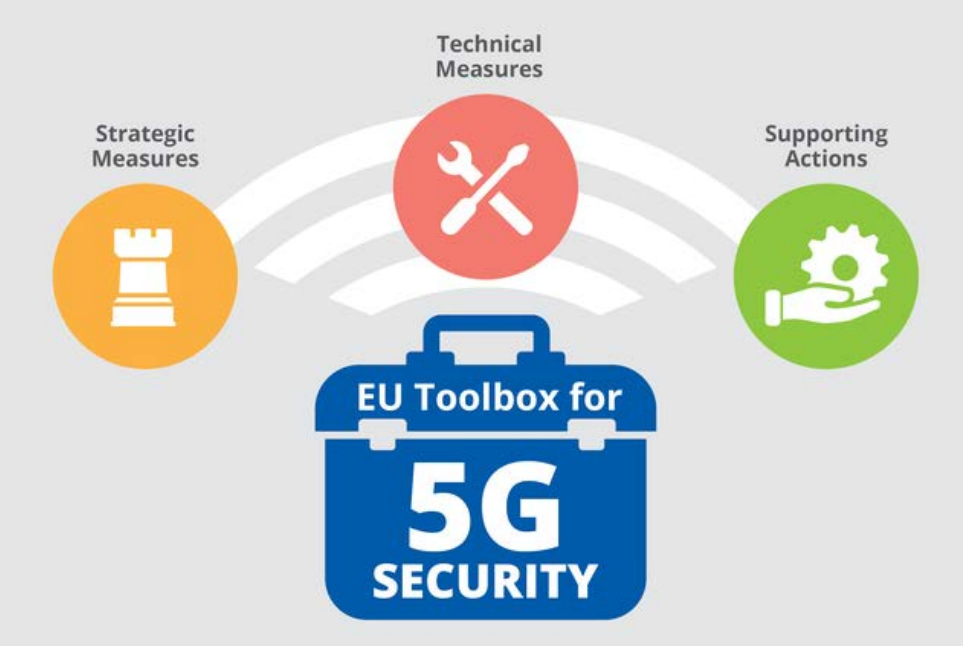
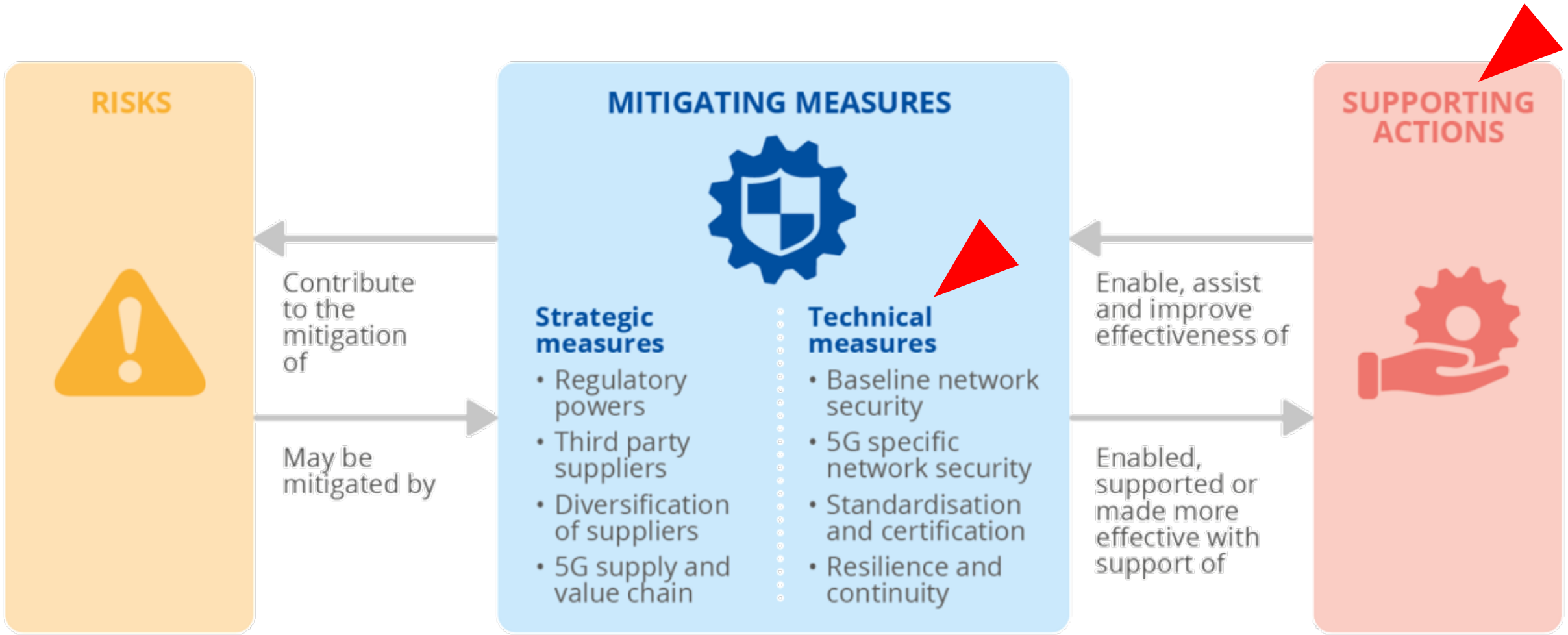
THE EU CYBERSECURITY AGENCY



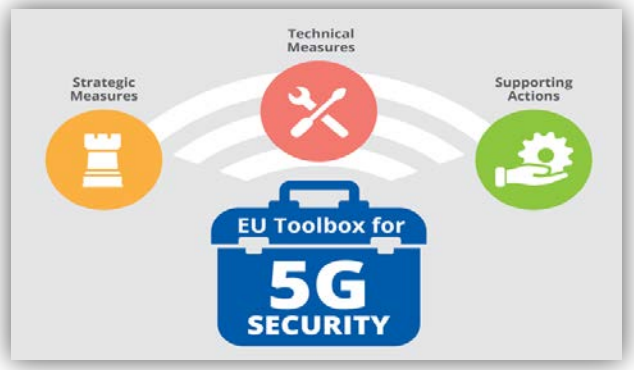
ENISA CONTRIBUTION TO THE IMPLEMENTATION OF TECHNICAL MEASURES FROM THE 5G TOOLBOX

GORAN MILENKOVIC, ENISA

TOOLBOX – THE STRUCTURE



5G TOOLBOX



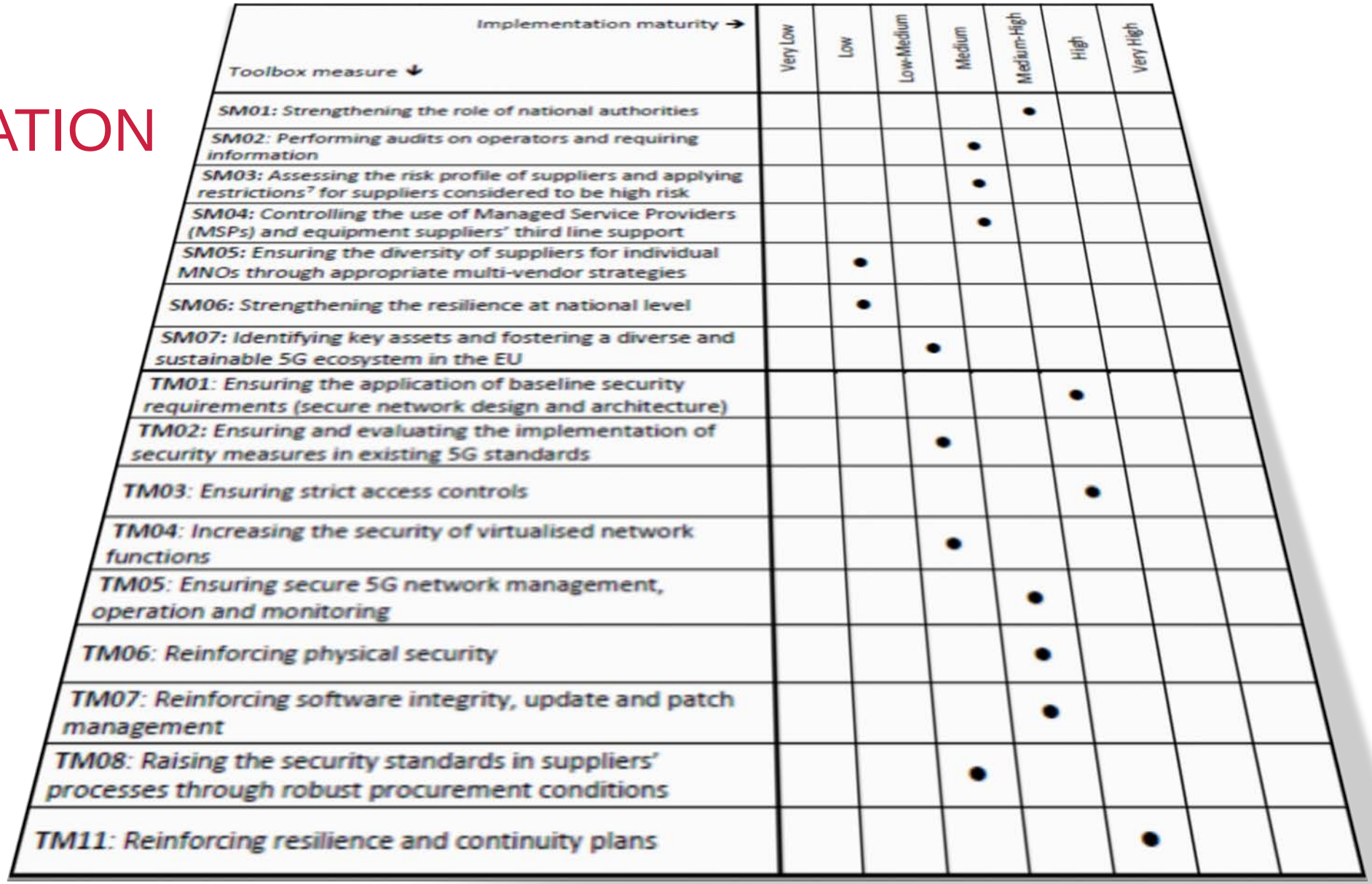
A set of **appropriate**, **effective** and **proportionate** possible **measures** to **mitigate** the cybersecurity **risks** identified in the EU coordinated risk assessment.

MEASURES	Indicative timeframe[1]			Potential impact factors				SPECIFIC MEASURES	RISKS									
	Short-term	Medium-term	Long-term	Resource costs	Sector specific economic impact	Sector specific economic impact	Broader economic / societal		R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption	R9: IoT exploitation	
STRATEGIC MEASURES																		
Regulatory powers	✓			✓	✓	✓	✓	SM01										
								SM02										
Third party suppliers	✓			✓	✓	✓	✓	SM03										
								SM04										
Diversification of suppliers	✓	✓		✓	✓	✓	✓	SM05										
								SM06										
5G supply and value chain	✓	✓	✓	✓	✓	✓	✓	SM07										
								SM08										
TECHNICAL MEASURES																		
Baseline network security	✓			✓	✓			TM01										
								TM02										
5G specific network security	✓			✓	✓			TM03										
								TM04										
								TM05										
								TM06										
								TM07										
Requirements related to suppliers' processes and equipment		✓	✓	✓	✓	✓		TM08										
								TM09										
								TM10										
Resilience, continuity	✓			✓	✓			TM11										

5G TOOLBOX – TECHNICAL MEASURES OVERVIEW

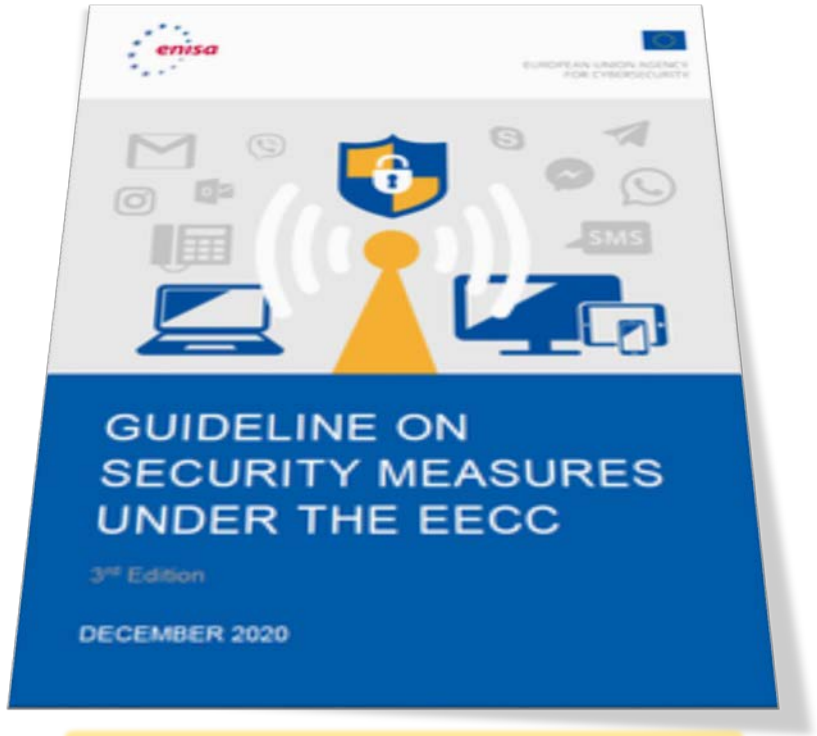
TM01	Ensuring the application of baseline security requirements (secure network design and architecture)
TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards
TM03	Ensuring strict access controls
TM04	Increasing the security of virtualised network functions
TM05	Ensuring secure 5G network management, operation and monitoring
TM06	Reinforcing physical security
TM07	Reinforcing software integrity, update and patch management
TM08	Raising the security standards in suppliers' processes through robust procurement conditions
TM09	Using EU certification for 5G network components, customer equipment and/or suppliers' processes
TM10	Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud)
TM11	Reinforcing resilience and continuity plans

TOOLBOX IMPLEMENTATION REPORT



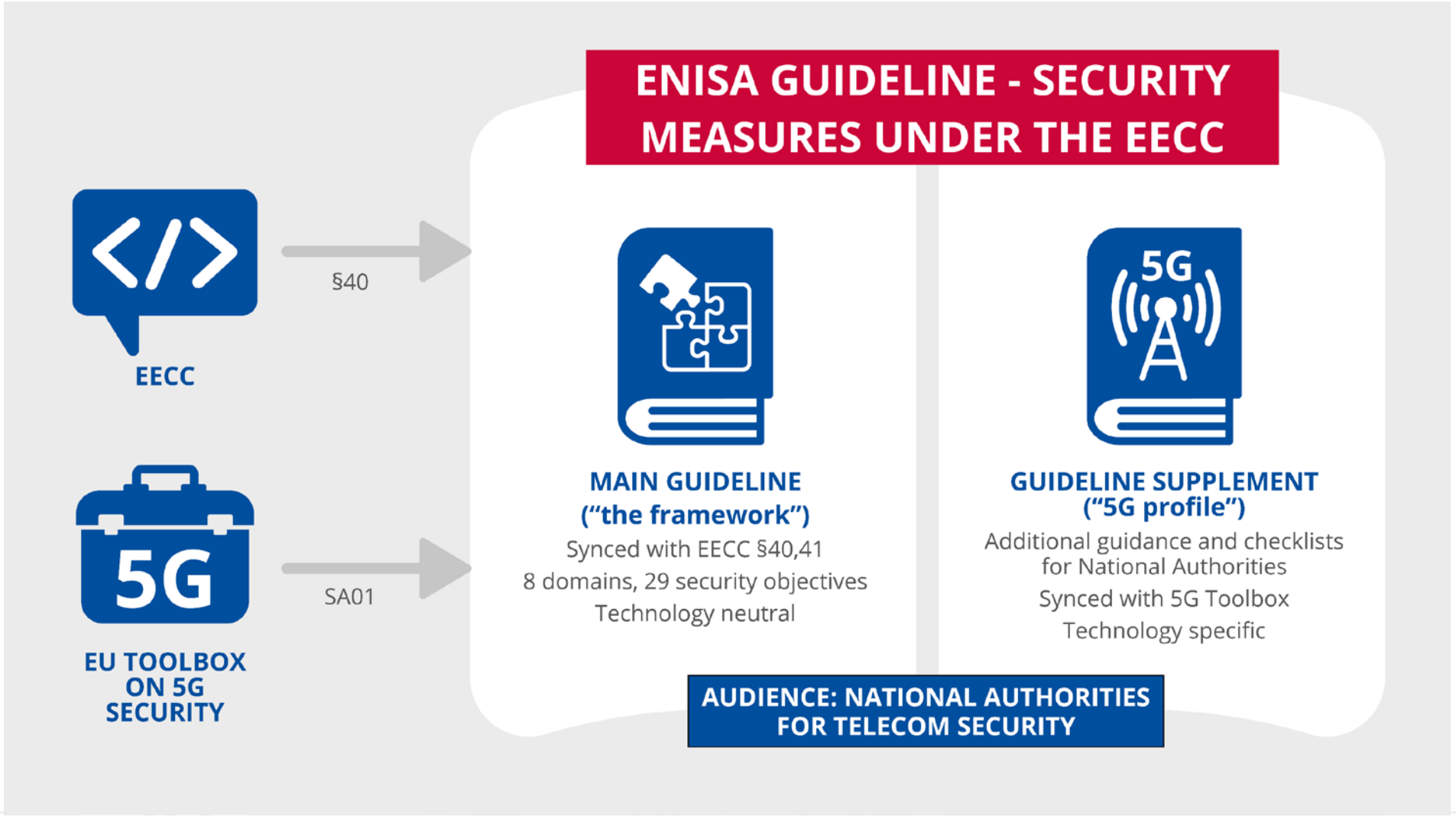
Toolbox measure ↓ / Implementation maturity →	Very Low	Low	Low-Medium	Medium	Medium-High	High	Very High
SM01: Strengthening the role of national authorities					●		
SM02: Performing audits on operators and requiring information				●			
SM03: Assessing the risk profile of suppliers and applying restrictions[7] for suppliers considered to be high risk				●			
SM04: Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support				●			
SM05: Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies		●					
SM06: Strengthening the resilience at national level		●					
SM07: Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU			●				
TM01: Ensuring the application of baseline security requirements (secure network design and architecture)						●	
TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards			●				
TM03: Ensuring strict access controls						●	
TM04: Increasing the security of virtualised network functions				●			
TM05: Ensuring secure 5G network management, operation and monitoring					●		
TM06: Reinforcing physical security					●		
TM07: Reinforcing software integrity, update and patch management					●		
TM08: Raising the security standards in suppliers' processes through robust procurement conditions				●			
TM11: Reinforcing resilience and continuity plans							●

NEW ENISA GUIDELINE FOR TELECOM SECURITY



Published on 10-Dec-2020

GUIDELINE CONCEPT



ENISA GUIDELINE (CONT.)

Chapter 3: ~~ART.13A~~ EECC DEFINITIONS AND TERMINOLOGY	
Chapter 4: SECURITY MEASURES	
D1: Governance and risk management	SO 1: Information security policy
	SO 2: Governance and risk management
	SO 3: Security roles and responsibilities
	SO 4: Security of third party assets
D2: Human resources security	SO 5: Background checks
	SO 6: Security knowledge and training
	SO 7: Personnel changes
	SO 8: Handling violations
D3: Security of systems and facilities	SO 9: Physical and environmental security
	SO 10: Security of supplies
	SO 11: Access control to network and inf. sys.
	SO 12: Integrity of net. and inf. systems
	SO 13: Use of encryption
	SO 14: Protection of security critical data
D4: Operations management	SO ~~13~~15: Operational procedures
	SO ~~14~~16: Change management
	SO ~~15~~17: Asset management

D4: Operations management	SO ~~13~~15: Operational procedures
	SO ~~14~~16: Change management
	SO ~~15~~17: Asset management
D5: Incident management	SO ~~16~~18: Incident management procedures
	SO ~~17~~19: Incident detection capability
	SO ~~18~~20: Incident reporting and communication
D6: Business continuity management	SO ~~19~~21: Serv. continuity strategy and contingency plans
	SO ~~20~~22: Disaster recovery capabilities
D7: Monitoring, auditing and testing	SO ~~21~~23: Monitoring and logging policies
	SO ~~22~~24: Exercise contingency plans
	SO ~~23~~25: Network and information systems testing
	SO ~~24~~26: Security assessments
	SO ~~25~~27: Compliance monitoring
D8: Threat awareness	SO 28: Threat intelligence
	SO 29: Informing users about threats
Chapter 5: SUPERVISION	
Chapter 6: MAPPING TO INTERNATIONAL STANDARDS	

Updated New

Published on 10-Dec-2020

5G SUPPLEMENT

What is it and what does it contain?

- Supplements the main guideline; uses same domains and security objectives
- Provides additional supervision guidance for authorities on security measures relevant for cybersecurity of 5G networks
  - 8 checklists with 70 checks - questions to consider in supervision - to ensure implementation of strengthened security measures for security objectives under each domain
  - Additional informative guidance on security aspects of new technologies (e.g. virtualization, slicing, edge computing) - with recommendations and references to relevant best practices and standards

GUIDELINE DOMAINS: TOOLBOX MAPPING

	D1: Governance and risk mgt.	D2: Human resources security	D3: Security of systems and facilities	D4: Operations management	D5: Incident management	D6: Business continuity management	D7: Monitoring, auditing, testing	D8: Threat awareness
TM01	■	■	■	■	■	■	■	■
TM02			■				■	
TM03			■				■	
TM04			■				■	
TM05		■			■		■	■
TM06		■	■					
TM07			■	■			■	
TM08	■							
TM09	■							
TM10	■							
TM11						■		

Published on 14-Dec-2020

UPDATED 5G THREAT LANDSCAPE

What does it contain?

- Updated architecture (UPDATE)
- Considered 5G migration options (NEW)
- Added management processes (Vendor, Operators, Security Assurance) (NEW)
- Made a detailed vulnerability analysis (NEW)
- Mapped threat exploitation (NEW)
- Mapped toolbox measures and controls (NEW)
- Updated asset inventory (UPDATE)

In preparation

STUDY ON CONTROLS IN 5G SPECS

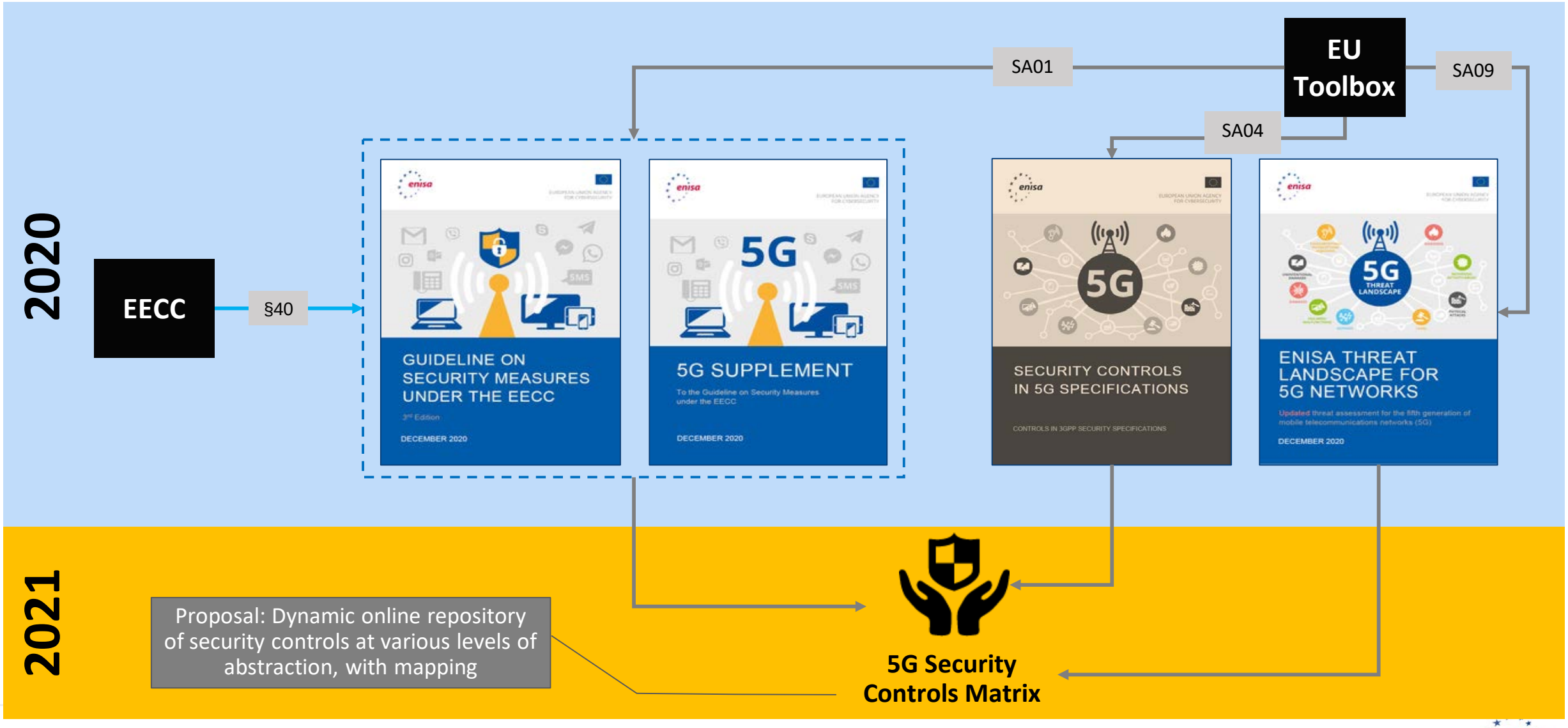
Why?

- Toolbox SA04, supporting TM02

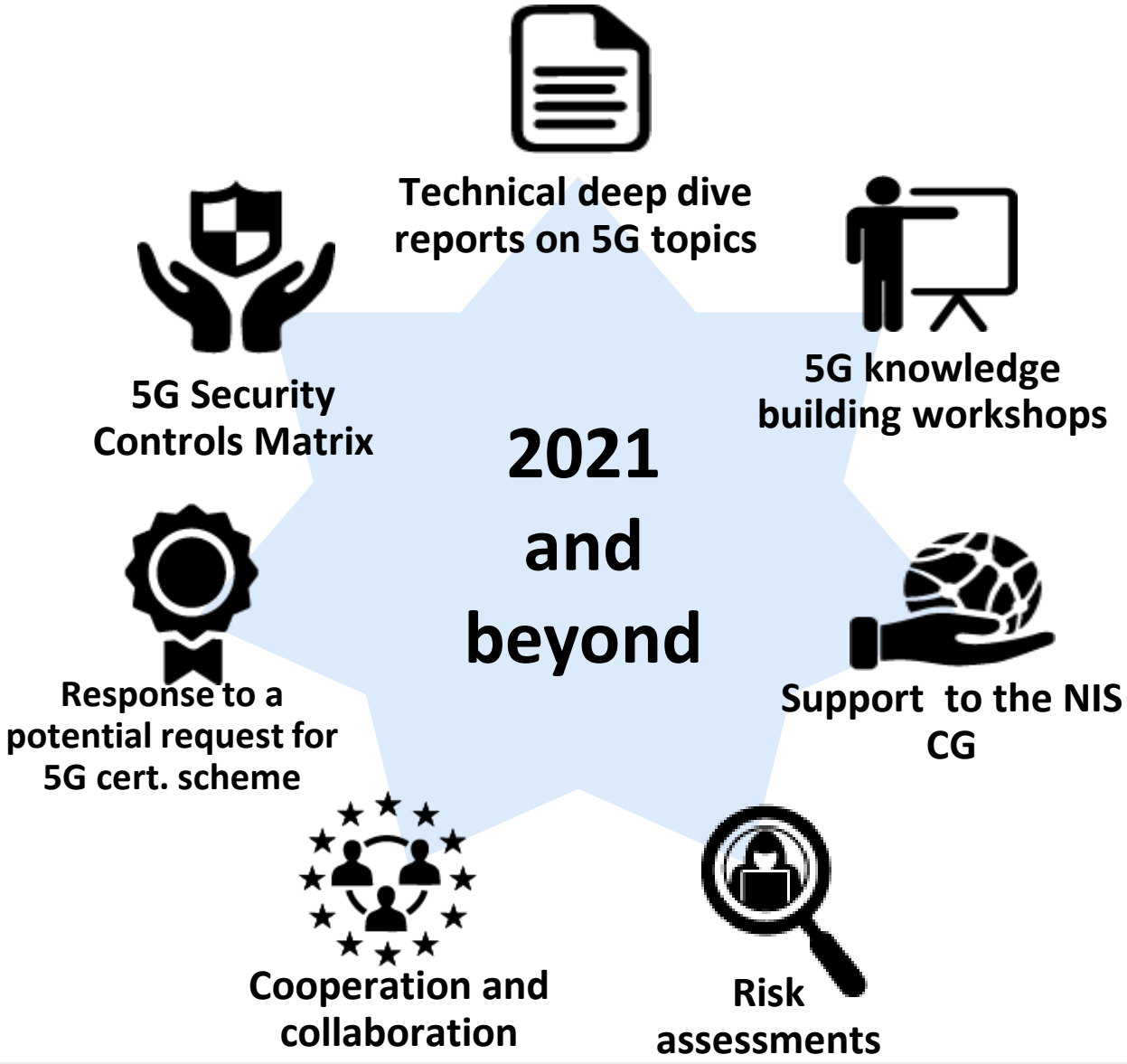
What?

- High-level overview of key standards and specs for 5G security
- Detailed analysis of security measures in 3GPP security specs
  - Analysis of optional security controls
- Analysis of main aspects not covered by standards and specifications
- Findings and best practices

HOW IT ALL FITS TOGETHER



ENVISAGED NEXT STEPS

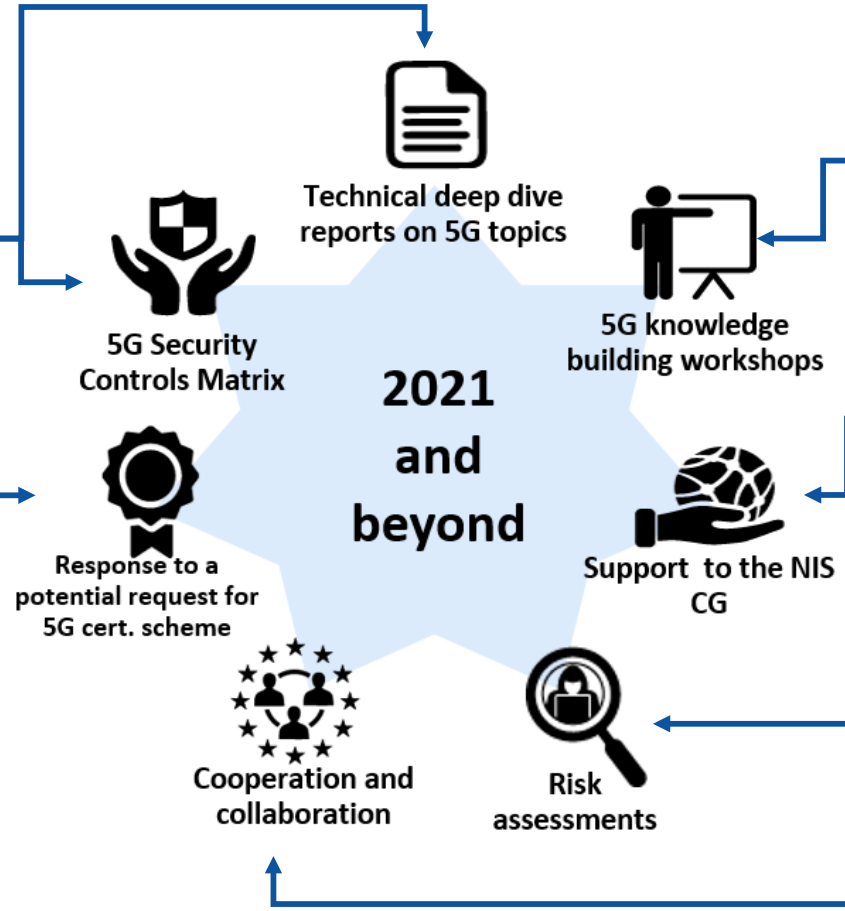


ALIGNMENT WITH EU STRATEGY

The new **EU Cybersecurity** strategy
Trust and security at the heart of the
EU's Digital Decade

- 1.4: Securing the next generation of broadband mobile networks
- Appendix: Next steps on cybersecurity of 5G networks:

Key objective 1: Ensuring convergent national approaches for effective risk mitigation across the EU
Area: Capacity building and guidance on technical measures



Key objective 2: Supporting continuous exchange of knowledge and capacity building

- Area: Continuous knowledge building
- Area: Risk assessments
- Area: Cooperation among stakeholders

Key objective 3: Promote supply chain resilience, and other EU strategic security objectives
Area: Certification

THANK YOU!

QUESTIONS?

Goran Milenkovic

+30 2814409610

goran.milenkovic@enisa.europa.eu

www.enisa.europe.eu