THE EU CYBERSECURITY AGENCY

ENISA 5G SECURITY CONTROLS MATRIX

LAUNCH

Sławomir Bryska, ENISA

OUR GOAL

5G Security Controls Matrix
powered by ENISA

To consolidate various 5G security controls in a single repository

Numerous sources of information relevant to 5G security

Benefit to NRAs, telecom companies and other stakeholders

Review and update national regulation (CA)

Provide detailed technical guidance (CA)

Develop questionnaires for operators (CA)

Implement or review ISMS (MNO)

THE CONTENTS SO FAR

8 security domains

29 security objectives

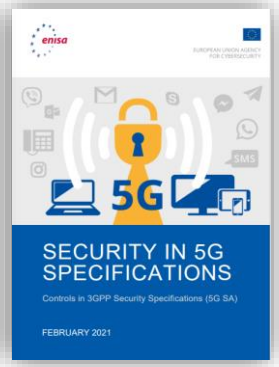
144 high level measures + evidence

399 detailed controls + evidence

Our 'integration' approach

Mapping with standards, specifications, frameworks and guidelines

Mapping with assets



Additional specs not captured in the documents to the left

DETAILED SECURITY CONTROLS - OVERVIEW

Id	Control	Evidence	Standalone (SA) or non-standalone (NSA)	Cloud deployment models (X) signifies technical possibility	Assets	Mapping to standards
SO11-034	NRFs authorize discovery requests from network functions based on the profile of the expected function/service and the type of the service consumer. If the expected function/service is deployed in a different network slice, NRF authorizes the discovery request according to the configuration of that slice. Example of such policy configuration could be that certain function/service instances are not discoverable from other network slices	NRF access logs and packet captures on the NRF confirm that an NRF returns a response with "403 Forbidden" status code if the requested NF instance does not allow discovery from other slices	SA	Private, (Hybrid), (Public)	NRF	3GPP TS 23.502, cl. 4.17.4 3GPP TS 33.501, cl. 5.9.2.1 3GPP TS 33.518, cl. 4.2.2.2.1
SO11-035	NRFs should implement Nnrf_AccessToken_Get service in accordance with 3GPP technical specification 33.501, clause 14.3	Verify that a test NF service consumer can receive an access token with appropriate claims from the Nnrf_AccessToken_Get service by sending it a request with its NF Instance Id, requested "scope", and optional information	SA	Private, (Hybrid), (Public)	NRF	3GPP TS 33.501, cl. 14.3
SO11-036	NEFs authorize requests from application functions using standard OAuth as profiled in 3GPP TS 33.501	Verification that invocation of NEF northbound APIs with valid OAuth tokens is successful	SA	Private, (Hybrid), (Public)	NEF	3GPP TS 33.501, cl. 5.9.2.3/12.4/13.4 3GPP TS 33.519, cl. 4.2.2.1.1
SO11-037	System functions (such as the Management Plane) are not accessed without successful authentication and authorization. Access control policy should restrict and/or control remote access by third parties, especially by suppliers or managed service providers considered to be high-risk or accessing the network from outside of EU. If necessary, only temporary onsite/remote access to third parties should be provided and no permanent credentials are disclosed	Verify that attempts to access a system function are only successful when logged in as a user with adequate privileges. Verify access logs to confirm that attempts for remote access by third parties are either denied, or restricted (e.g. one-time short-lived access grant), according to the documented policy (see control description). Access logs confirm that onsite/remote access by third parties, if allowed, is based on temporary or one-time passwords used only for designated tasks	SA and NSA	Private, Hybrid, (Public)	UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.1.1 3GPP TS 33.216 3GPP TS 33.511-519 NIST.SP.800-53-Rev.5, AC-2, AC-3, AC-4, AC-6, and AC-17
SO11-038	A centralized Privileged Access Management (PAM) solution is in place. Authorizations for accounts, files, and applications is reduced to the minimum required for the tasks they have to perform. Execution of applications and components shall also take place with rights that are as limited as possible. Access control policy is reviewed and revised based on 5G risk assessment	Access to critical or sensitive network components is captured in logs of the PAM solution. Documentation of the network product describes an authorization policy which includes details on the lowest access rights assigned to user accounts and applications. Verify that files and applications are not accessible without adequate privileges necessitated by the authorization policy. MNO has documented access control policy explaining how various rights in the network, such as access rights between network functions, network administrators' rights and alike are minimized. Review of policy, logs, comments and comparison with prior versions indicate that access control policy is reviewed and revised periodically in the context of evolving 5G risks.	SA and NSA	Private, Hybrid, (Public)	UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, PSF, ISF, VSF, LCM proxy, MEC orchestrator, EPC+ functions	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.6 3GPP TS 33.216 3GPP TS 33.511-519 NIST.SP.800-53-Rev.5, AC-2, AC-3, AC-4 and AC-6
SO11-039	Privilege escalation in interactive sessions (CLI or GUI) of a network product is not allowed without re-authentication	Verify that commands such as 'su' which enable a user or function to gain administrator/root privileges from another user account require re-authentication	SA and NSA	Private, Hybrid, (Public)	UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.2.1 3GPP TS 33.216 3GPP TS 33.511-519

Modified extract for presentation purposes

THREE WAYS TO PRESENT ALL THE CONTROLS

SO	Sophistication level	Measure ID	Control ID	Descripion	Corresponding evidence	Standalone (SA) or non-standalone (NSA)	Cloud deployment models	Related assets	Mapping to standards
SO13: Use of encryption	**Basic**	M070		Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering	-Description of main data flows, and the encryption protocols and algorithms used for each flow -Description of justified exclusions and limitations in implementing encryption. Ability to implement encryption may also be influenced by technological limitations, like in the case of legacy networks or when old equipment and network protocols are used				-ISO/IEC 27002:2022: 8.11 Data masking -ISO/IEC 27002:2022: 8.20 Networks security -ISO/IEC 27002:2022: 8.21 Security of network services -ISO/IEC 27002:2022: 8.24 Use of cryptography -ISO/IEC 27002:2022: 8.26 Application security requirements -ISO/IEC 27002:2022: 8.27 Secure system architecture and engineering principles
			SO13-001	NAS signaling should be confidentiality protected by the MME	Packet captures confirm the encryption of the NAS signaling	NSA	Private, (Hybrid), (Public)	MME	3GPP TS 33.116, cl. 4.2.2.3.4 3GPP TS 33.401, cl. 5.1.3.1
			SO13-002	All NAS signaling messages except those explicitly listed in TS 24.301 as exceptions should be integrity-protected	Packet captures confirm the integrity protection of the NAS signaling messages with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	NSA	Private, (Hybrid), (Public)	MME	3GPP TS 33.401, cl. 5.1.4.1/8.1
			SO13-003	NAS NULL integrity with EIA0 is only used for emergency calls	Packet captures at the MME confirm that that the SECURITY MODE COMMAND message sent by the MME after successful UE authentication contains an algorithm different from EIA0 (except for emergency calls)	NSA	Private, (Hybrid), (Public)	MME	3GPP TS 33.116, cl. 4.2.2.3.3 3GPP TS 33.401, cl. 5.1.4.1
			SO13-004	eNB ensures confidentiality and integrity protection of control plane data on X2-C and S1-MME interfaces	Packet captures confirm the use of IPsec on X2-C and S1-MME interfaces	NSA	Private, (Hybrid), (Public)	eNB	3GPP TS 33.216 4.2.2.1.1/4.2.2.1.2 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
			SO13-005	eNB ensures confidentiality and integrity protection of user plane packets between the Uu reference point and the S1/X2 reference points	Packet captures confirm that the transport of user data over S1-U and X2-U interfaces is integrity, confidentially and replay-protected	NSA	Private, (Hybrid), (Public)	eNB	3GPP TS 33.216, cl. 4.2.2.1.3/4.2.2.1.4 3GPP TS 33.401, cl. 5.3.4 3GPP TS 33.501, cl. 5.4

Modified extract from one of the three data presentation sheets

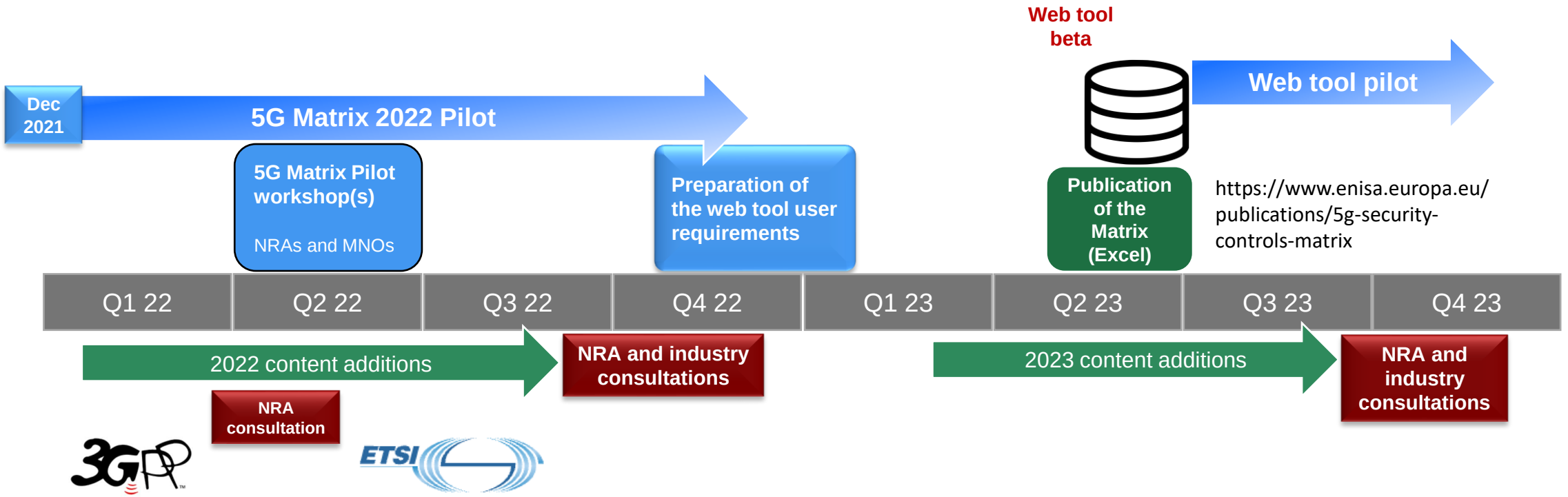
YOUR FEEDBACK MATTERS

Id	Control	Evidence	Standalone (SA) or non-standalone (NSA)	Cloud deployment models	Assets	Mapping to standards
SO13-004	eNB ensures confidentiality and integrity protection of control plane data on X2-C and S1-MME interfaces	Packet captures confirm the use of IPsec on X2-C and S1-MME interfaces	NSA	Private, (Hybrid), (Public)	eNB	3GPP TS 33.216 4.2.2.1.1/4.2.2.1.2 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
SO13-005	eNB ensures confidentiality and integrity protection of user plane packets between the Uu reference point and the S1/X2 reference points	Packet captures confirm that the transport of user data over S1-U and X2-U interfaces is integrity, confidentially and replay-protected	NSA	Private, (Hybrid), (Public)	eNB	3GPP TS 33.216, cl. 4.2.2.1.3/4.2.2.1.4 3GPP TS 33.401, cl. 5.3.4 3GPP TS 33.501, cl. 5.4
SO13-027	Negotiation of slice characteristics such as bandwidth, latency, and reliability between a communication service customer and an MNO should have replay, integrity, and confidentiality protection with TLS. Version 1.2 or 1.3 of TLS are recommended. Cryptographic keys/certificates for TLS authentication are protected	Verify by successfully setting up test connections with slice management interface and negotiating different slice characteristics via TLS. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	SA	Private, Hybrid, (Public)	Network Slice Instance	3GPP TR 33.811, cl. 4.4.1
SO14-004	Subscription permanent identifier (SUPI) is encrypted to derive the Subscription Concealed Identifier (SUCI) using a non-null protection scheme by default. A null-scheme may be used in the following cases: (1) if the UE is making an unauthenticated emergency session and does not have a 5G-GUTI to the chosen PLMN, (2) if the home network has configured "null-scheme" to be used, or (3) if the home network has not provisioned the public key needed to generate a SUCI	Verification of UE authentication confirms that SUPI is not transmitted in clear text. Inspection of the protection scheme in the SUCI confirms a non-null protection scheme was used or one of the special conditions for using a null-scheme is met	SA	Private, (Hybrid), (Public)	UDM, AUSF	3GPP TS 33.501, cl. 6.12

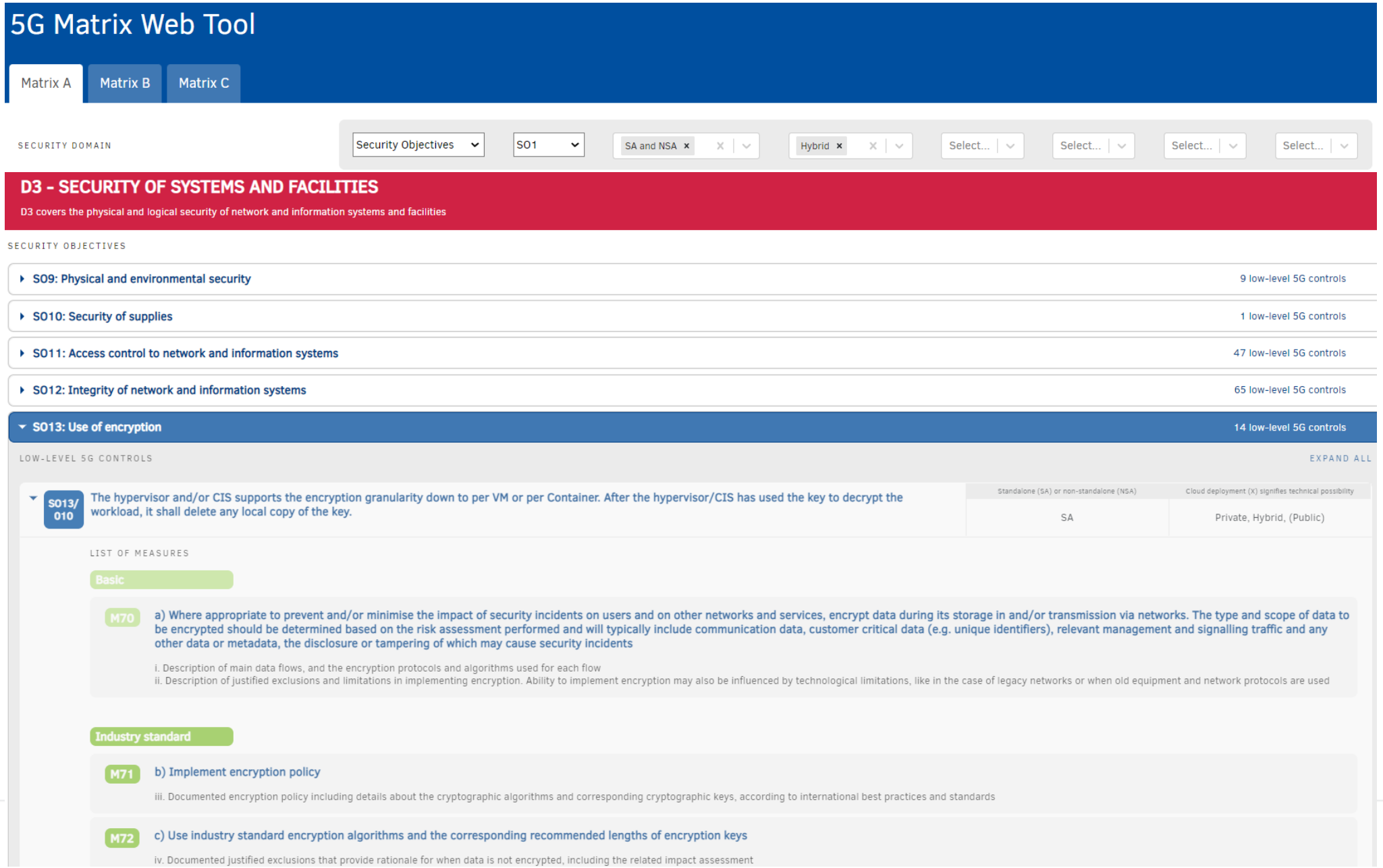
Modified extract for presentation purposes

2022-2023 TIMELINE

5G Security Controls Matrix
powered by ENISA



WEB TOOL BETA



Pre-release web tool extract

2023 CONTENT ADDITIONS

Non-technical controls based on

ISO/IEC 27002:2022

NIST SP 800-53, Rev 5

ISO 22301 – Business continuity management systems (Requirements)

ISO/IEC 27005 – Information security risk management

SO	ISO 27002:2022	NIST 800-53 CF subcategory…	…or exact NIST section (if CF subcategory does not map)	Existing non-technical controls from '5GControls' tab
13	8.11, 8.20, 8.21, 8.24, 8.26, 8.27	PR.DS-1, PR.DS-2	SC-13 (cryptographic protection)	-
14	5.33, 8.11, 8.20, 8.21, 8.24, 8.26, 8.27	PR.DS-1, PR.DS-1	SC-12 (key creation and management)	-
15	5.37, 7.13, 7.14, 8.9, 8.10, 8.11, 8.12, 8.21, 8.31	PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-6, PR.IP-7		SO15-002, SO15-003, SO15-004, SO15-024, SO15-026, SO15-027, SO15-028, SO15-029, SO15-030
16	5.8, 8.4, 8.18, 8.19, 8.25, 8.28, 8.29, 8.31, 8.32	PR.IP-2, PR.IP-3		SO16-001, SO16-002, SO16-003
17	5.9, 5.10, 5.11, 5.12, 5.13, 5.32, 5.33, 7.8, 7.9, 7.10, 7.13, 7.14, 8.1, 8.9,	ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5		SO17-001, SO17-002, SO17-003, SO17-004, SO17-005, SO17-006, SO17-007, SO17-008, SO17-009, SO17-010, SO17-011, SO17-012, SO17-013, SO17-014
18	5.24, 5.25, 5.26, 5.27, 5.28, 6.8	RS.CO-1, PR.IP-9, PR.IP-10, RS.RP-1, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2		SO18-001, SO18-002
19	5.24, 5.25, 8.7	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5		SO19-001, SO19-002, SO19-003, SO19-004, SO19-005, SO19-006

Extract from scoping table

LET’S JOIN OUR EFFORTS!

Specific questions about the Matrix?

How could the Matrix best assist you in your work?

Interested in piloting the web tool?

Which content additions should we focus on next?

5G Security Controls Matrix

powered by ENISA

THE EU CYBERSECURITY AGENCY

Thank you!

ALL FEEDBACK, ADVICE, IDEAS, SUGGESTIONS WELCOME

To view the Excel Matrix

https://www.enisa.europa.eu/publications/5g-security-controls-matrix

To send us your feedback

ENISA-NIS-Directive@enisa.europa.eu