Deloitte.

Securing Telcos' 5G adoption journey

Supporting Telcos assessing their 5G security strategy

Telecom Engineering Centre of Excellence (TEE)

EMEA Centres of Excellence

Abstract

The emergence of 5G networks is likely to fuel the growth in several industries, supporting a broad set of use cases and ultimately sparking a new era of enhanced digitalization that can transform both economies and societies. This social and economic importance turns security into a paramount component that should be regarded from the beginning of the 5G Transformation in order to mitigate eventual vulnerabilities and risks in networks that are expected to connect trillions of devices.

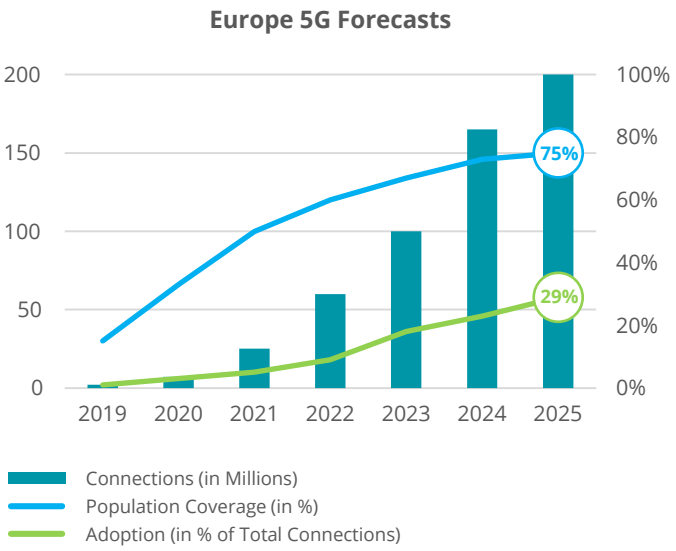
This white paper identifies key security challenges that should be tackled by Telcos during the 5G Transformation while exploring the security related opportunities that are enabled. It also provides a high level perspective on Deloitte's methodology to support Telcos successfully navigating through this journey in a 'secure-by-design' manner, thus tackling security weaknesses from Day 1 and enabling a secure 5G paradigm.

Contents

Telco's security paradigm on the 5G landscape

What is the impact and what is happening to security during 5G adoption?

The emergence of 5G networks is expected to fuel the future growth in several industries and to transform both economies & societies, supporting a broad set of use cases and ultimately sparking a new era of enhanced digitization. This **importance of 5G networks turns security into a paramount component** that should be regarded from the beginning of the 5G adoption. To illustrate this relevance, current forecasts show that, by 2025, 29% of the mobile connections in Europe are to be made through 5G. These include connections of mission critical infrastructure, such as power grids remotely operated, which have demanding security requirements.
On top of having to handle billions of connected devices, 5G creates additional security challenges that will have a significant impact on Telco's security strategy and on the requirements they need to address. The main 5G adoption impacts on Telcos' security strategy can be summarized in 4 critical domains, represented in Figure 1.



Graphic 1 - Forecast evolution of 5G growth on connections, population and adoption
Sources: GSMA (2020)

Network Architecture

Telcos should adopt a "security by design" approach when planning their NW transformation in order to maximize network security from Day 1 and prepare for the higher impacts of the 5G Standalone phase

Operations & Services

5G will create multiple market opportunities to optimise network security operations & services. Telcos should anticipate them or may fail to capture 5G full value and be surpassed by their competitors

Regulations & Standards

Telcos will need to be in close contact and pro-actively support policy makers and standards organizations in order to be better prepared to tackle the potential new 5G adoption security requirements

5G Ecosystem

Telcos should be pro-active on engaging and orchestrating the 5G ecosystem in order to drive alignment towards a holistic and homogeneous approach that increases security levels of all involved parties

Figure 1 – Main domains of 5G security transformation

5G adoption is a non-avoidable reality. Telcos need to be aware of both the security challenges they will face as well as the opportunities ahead in order to start defining **now their future 5G security strategy.**

5G security impacts: Network Architecture

What are the 4G and 5G security synergies and adoption phases?

5G adoption requires new fundamental security mechanisms for Telco's environment, which can lead to a higher network resilience and overall service security. **The evolution from a legacy network to a 5G network will be a phased one**, with each phase requiring additional security capabilities to be part of the architecture design strategy.

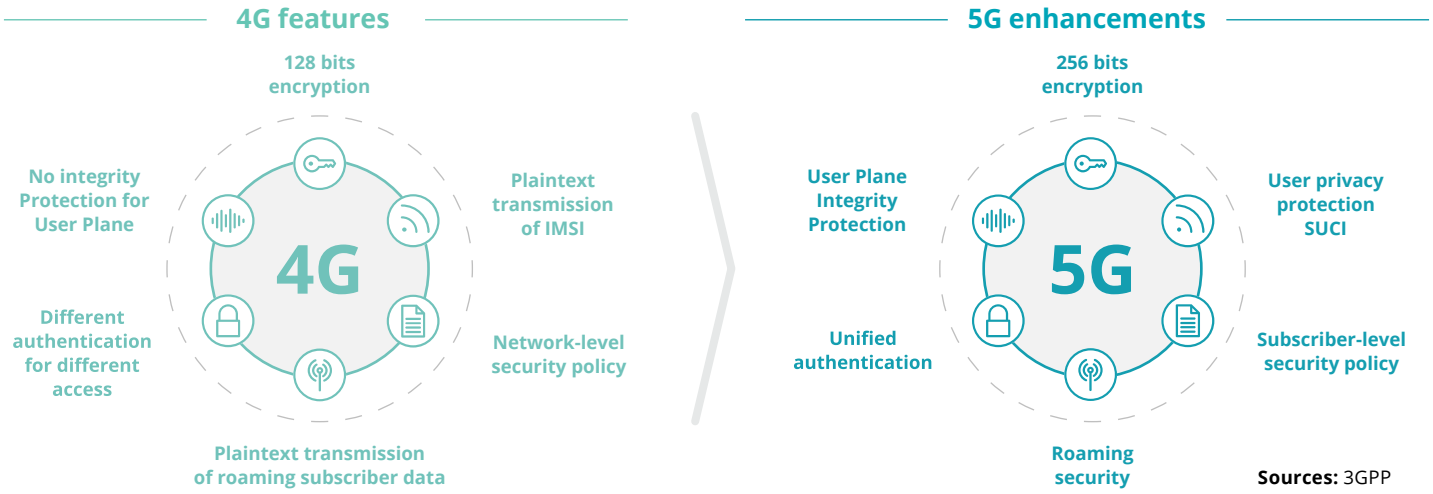


Figure 2 – Evolution of different network security features that will be enhanced with 5G

Typically, the first phase of the evolution is **5G Non-Standalone (NSA)**, in which most of the security mechanisms applied are similar to the ones in 4G but with enhancements. This is a transitional phase, **adopted by Telcos that look for a gradual network transformation**. For those who seek a more disruptive evolution, it is possible to evolve both the radio and core networks at once, enabling a direct upgrade from 4G to a fully 5G network, also known **as 5G Standalone (SA).**

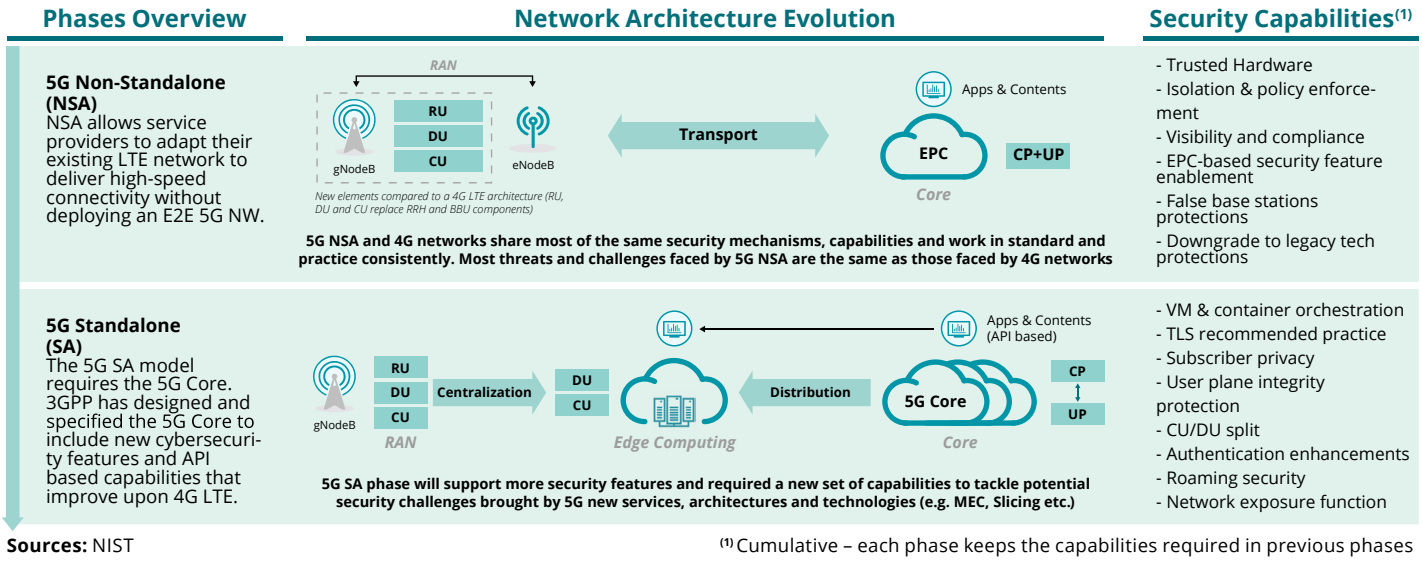


Figure 3 – Main differences and challenges between 5G NSA and SA

5G security impacts: Network Architecture

How will 5G Standalone architecture impact security capabilities?

Following **the principle of Secure by Design**, 5G architecture strategy requires that risks for each network component are identified and addressed from the beginning. While 5G NSA is a progressive evolution based on 4G architecture, **5G SA will enable new network technologies and innovative designing approaches. However, it will also demand new security capabilities and solutions** to address the threats that a service based architecture on the core network brings to a 5G SA environment, as presented in Figure 4.

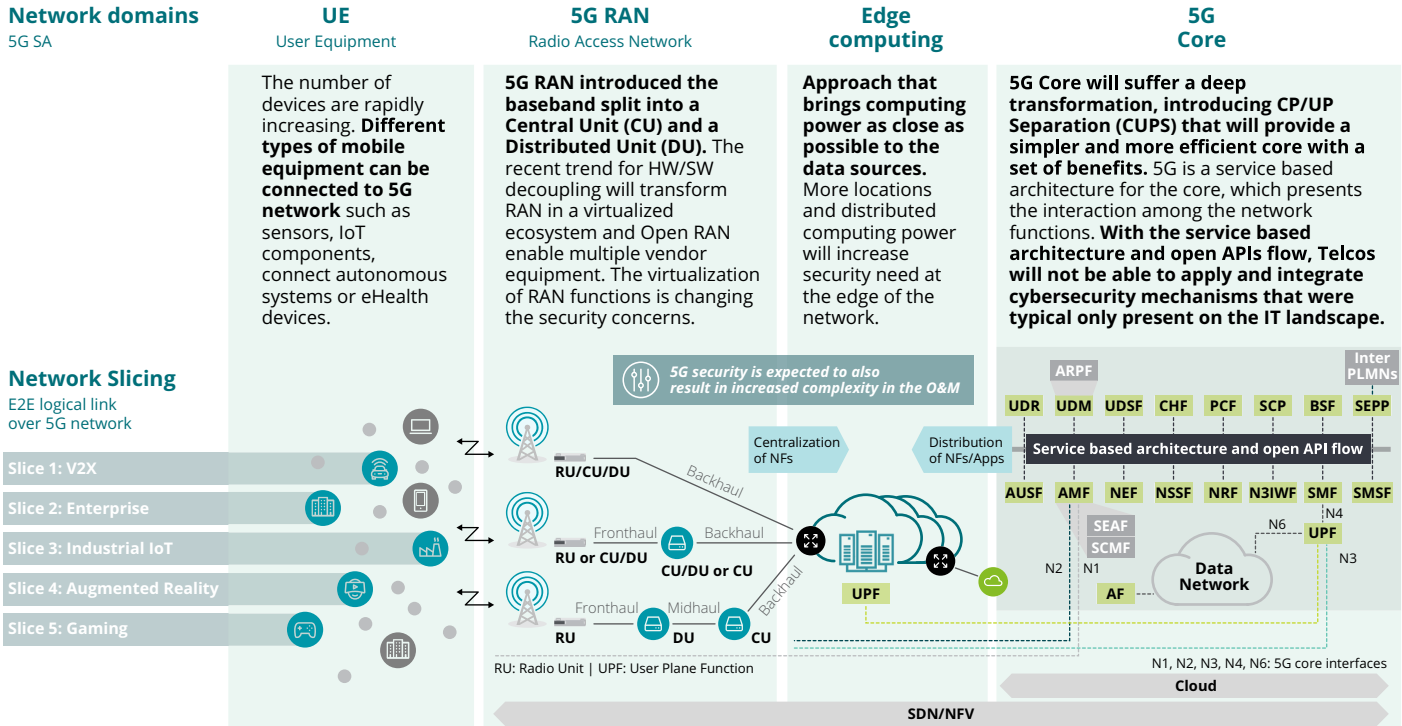


Figure 4 – 5G Standalone integration between domains and main security threats

5G evolution will impact the network from the core to the user equipment. Each domain can be responsible for different security threats, meaning that security is potentially impacted everywhere and should be considered a key design component from the start.

Telcos should adopt a "Secure by Design" approach when planning their 5G network architecture transformation in order to maximize network security from Day 1 and prepare for the higher impacts of the 5G SA phase.

5G security impacts: Operations & Services

Which shift will 5G adoption bring to security operational teams and services?

Besides the technical challenges already discussed, 5G also brings concerns and opportunities related to network operations & Telco's processes. These concerns will require an organizational shift towards automated security processes, security-centric software development methodologies and flexible security services offerings.

Security operations based on automated processes

5G will increase network complexity leading to a critical need to improve time-consuming and prone-to-errors security processes. To cope with this, network automation & orchestration capabilities will need to be introduced along 5G adoption.

Network automation will enable Telcos to:

- Reduce operational costs of network security
- Decrease response-time to threats and attacks

To take full advantage of 5G, Telcos need to increase their automation mechanisms in order to enable a closed loop zero touch operational approach supported by threat intelligence analytics and auto remediation capabilities

DevSecOps will be the standard

Telcos' organizations will need to leverage the IT concept of DevOps with an increased focus on security, assisting organizations to grow with secure software development and operational capabilities (DevSecOps methodology).

DevSecOps methodology will enable Telcos to:

- Introduce IT concepts on network security operations
- Have a secure software development approach

The 'Itzation' of network operational teams with a higher security focus, will enable Telcos new and secure ways of managing the software centric network infrastructure landscape, with increased levels of flexibility and automation

Cloud networking will allow flexible security levels

The set of 5G use cases can be so extensive that Telcos will struggle to secure them with a "one size fits all" approach. Instead, flexibility is required in order to enable different levels of security according to the clients and services needs.

Cloud flexibility will enable Telcos to:

- Follow an 'elastic' security approach
- Provide tailored security levels to clients' needs

By offering flexible security levels, that can be easily tailored to the needs of each service and customer, Telcos can support new use cases and seize the opportunity for the capitalization of 5G

5G will create multiple market **opportunities to optimise network security operations & services.** Telcos should **anticipate them or may fail to capture 5G full value** and be surpassed by their competitors.

5G security impacts: Regulations & Standards

How will 5G regulations & standards impact Telcos' security strategy definition?

Policy makers and standards organizations are expected to address society concerns related to 5G adoption, such as privacy and data protection. Effort for the **compliance with new regulations and standards is expected to increase considerably** with 5G introduction. The diversity of entities involved can make it difficult for organizations to be always on track of the latest updates.

Regulations

Compared to 4G, an **increased attention on regulations defining how 5G networks should operate is expected.** A key reason for this is that **5G use cases are more oriented to Enterprises and Government** verticals. This leads to a higher focus of policy makers, that together with standards organizations, are expected to address society concerns related to 5G secure adoption.

Regulations for privacy and data protection can be achieved in 3 phases:

Consumers require that their communications are secured and that data remains private

International and local organizations specify regulations that should be addressed by the 5G ecosystem

Industry groups collaboratively **draft principles and practices** to address the regulations

Standards

5G service providers **should work closely with standards organizations to develop a consistent E2E security framework that should be followed by all** in order to maximize security across the industry.

Definition of standards and technical specifications is an interactive process:

3GPP
Defines technical specifications for complete end-to-end systems

Technical Specifications

General policy and strategy

Standards Orgs
Telecom standards that should be adopted by the 5G stakeholders

5G Technical Specifications

Telecom Standards

Telcos will need to be in close contact and pro-actively support policy makers and standards organizations in order to be better prepared **to tackle the potential new 5G adoption security requirements.**

5G security impacts: 5G Ecosystem

Who will be involved in the 5G transformation and what challenges are expected?

The **diversity of 5G ecosystem** has the potential to boost innovation and will require a cooperation mentality between different stakeholders. This heterogeneity can positively impact network security innovation but it **may also increase security risks due to different security requirements, features and solutions from all involved parties.**

Main stakeholders in the 5G landscape

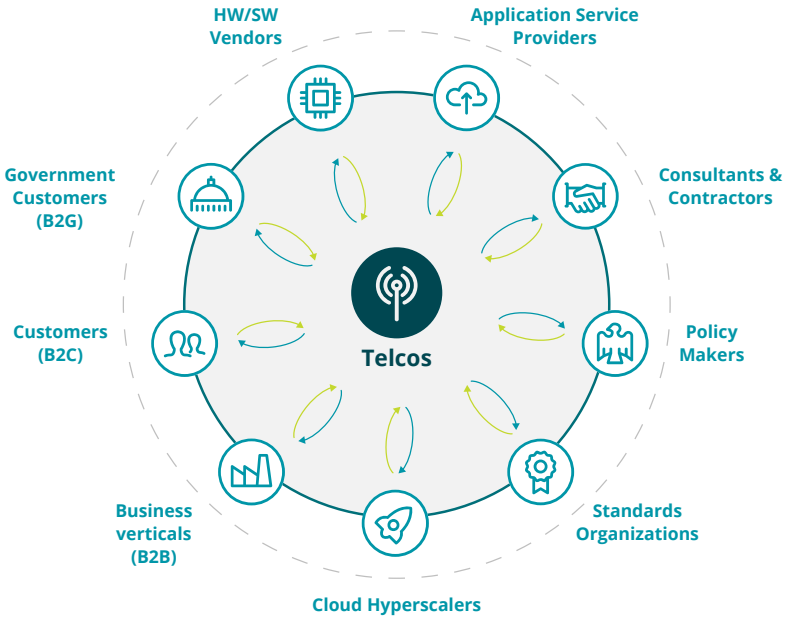


Figure 5 – 5G Ecosystem Stakeholders

Therefore, there is a need to **define and develop a common framework, applicable to the entire ecosystem,** that addresses and supports the orchestration of common security challenges.

Main Security Challenges

Multi-technologies, multi-solutions and multi-domains that will lead to a **heterogeneous interface landscape**

Increased entry points on the network and solutions from several HW/SW vendors

Existence of several policy makers and standards organizations increases the **challenge to guarantee the alignment of the entire ecosystem**

Telcos should be pro-active on engaging and orchestrating the 5G ecosystem in order to drive alignment towards **a holistic and homogeneous approach** that increases security levels of all involved parties.

Turning 5G security strategy into business reality

How 5G adoption will impact Telco's network security transformation?

The **5G adoption represents a fundamental change in the Telco's environment**, thus requiring a structured approach to tackle the security challenges along the way. It is critical to: **(i)** start defining the 5G cyber security strategy since day 1, **(ii)** have a complete visibility of the new 5G security features as Telcos progress in this transformation, **(iii)** understand the infrastructures impacted and **(iv)** define the adequate network security tools development roadmap.

Typical 5G Secure Adoption Key Phases

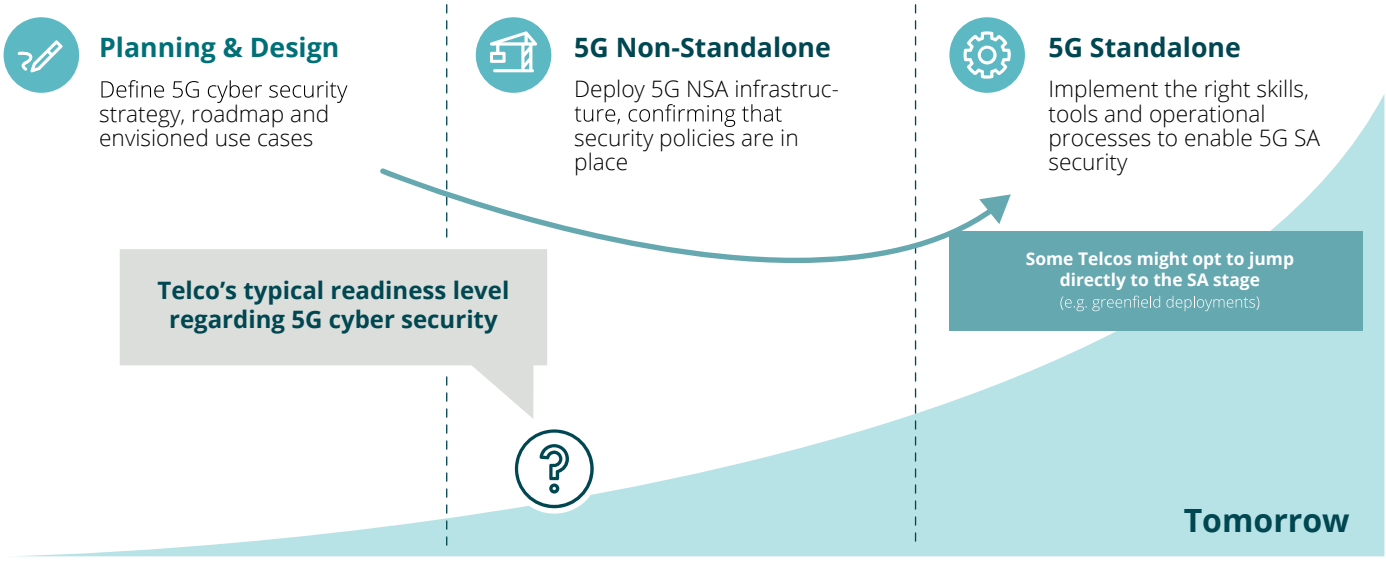


Figure 6 – Representation of the phases for 5G Secure Adoption

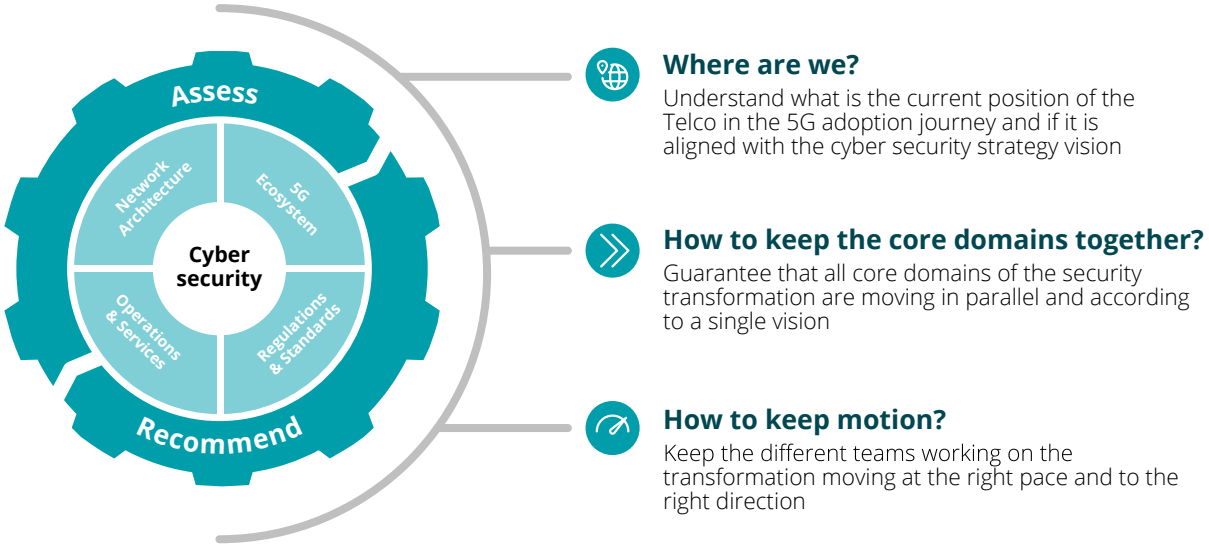
Today	Tomorow
Limited automation mechanisms in place for end-to-end data protection	**'Itzation' and automation of security,** with new security features & capabilities for the network
Increasing number of connected devices and criticality of exchanged data	**Devices compliant** with common security **regulations & standards**
Complex ecosystem with a **lack of a holistic security approach**	**Improved security controls** of the applications, network and cloud

Telcos will be facing a multitude of security challenges in their journey to 5G SA, being crucial for them to **define a structured approach that considers all key domains of the transformation** in order to tackle such challenges.

Turning 5G security strategy into business reality

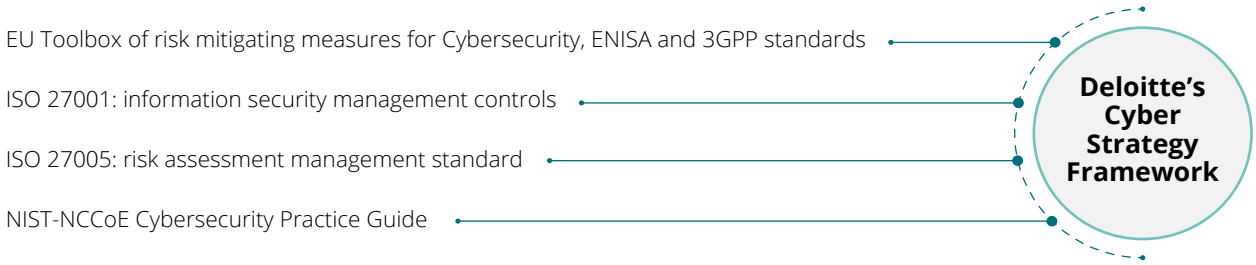
How can we support Telcos strategizing this transformation?

It is crucial to **constantly understand what is the position of the Telco in its 5G adoption journey,** how to keep the core domains progressing in parallel under a single vision and how to **maintain the pace and the strategic direction.**



Deloitte has defined an **agile approach that is the basis of an assessment that can identify Telco's readiness towards a fully secure 5G network.** Based on the outcomes of the assessment and on Telco's strategy for 5G, Deloitte is able to **identify a set of recommendations to improve the current 5G Cyber Security strategy.**

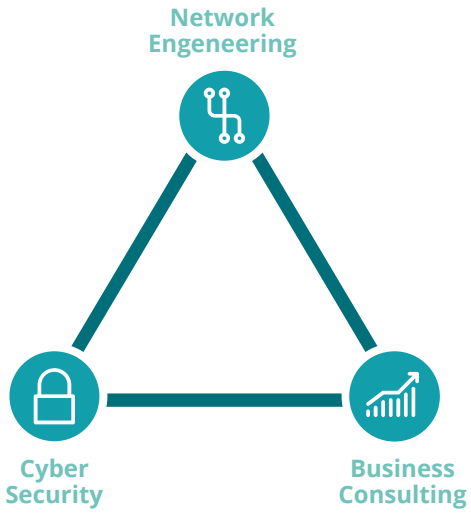
To have a clear view on Telcos cyber security needs, **Deloitte's framework includes support for assessments based on industry reference practices, standards and guidelines** like EU Toolbox, ISO 27001, ISO 27005 or NIST Cybersecurity Practice Guide.



Our framework will **support the assessment of the 5G security in all its domains** enabling an **exhaustive identification of the steps needed to drive a secure 5G adoption.**

How can Deloitte help clients safely navigate 5G?

Deloitte combines the strengths of all practices including thought **leadership, talent, resources, and global reach. This allows the firm to provide clients with unique insights,** leading edge ideas/methods, actionable analysis, recommendations, and extensive hands-on implementation experience – all firmly grounded in deep industry knowledge and focused on business impact.



Deloitte is unique in its service offerings in the **Network Engineering and Cybersecurity domains**, associating high technical expertise with business strategic consulting skills **and a set of tools & accelerators in the 5G area that can help our clients reach their goals faster than the competition**

Who to contact?

Frederico Macias
+351 966 850 347
fremacias@deloitte.pt

Luís Abreu
+351 964 240 065
labreu@deloitte.pt

Pedro Sanguinho
+351 965 895 861
psanguinho@deloitte.pt

André Santiago
+351 912 767 219
ansantiago@deloitte.pt

Acknowledgements

Special thanks to Deloitte professionals who contributed to this publication in terms of researching, providing expertise, and coordinating:
Paulo Costa | Tiago Pires | Luís Pinto | Nuno Deus | Filipe Monteiro | Tiago Marques

Deloitte.