WE ARE
CORTEX
Automation at scale

Compliance with the TSA isn't enough for

NIS 2 compliance. Why?

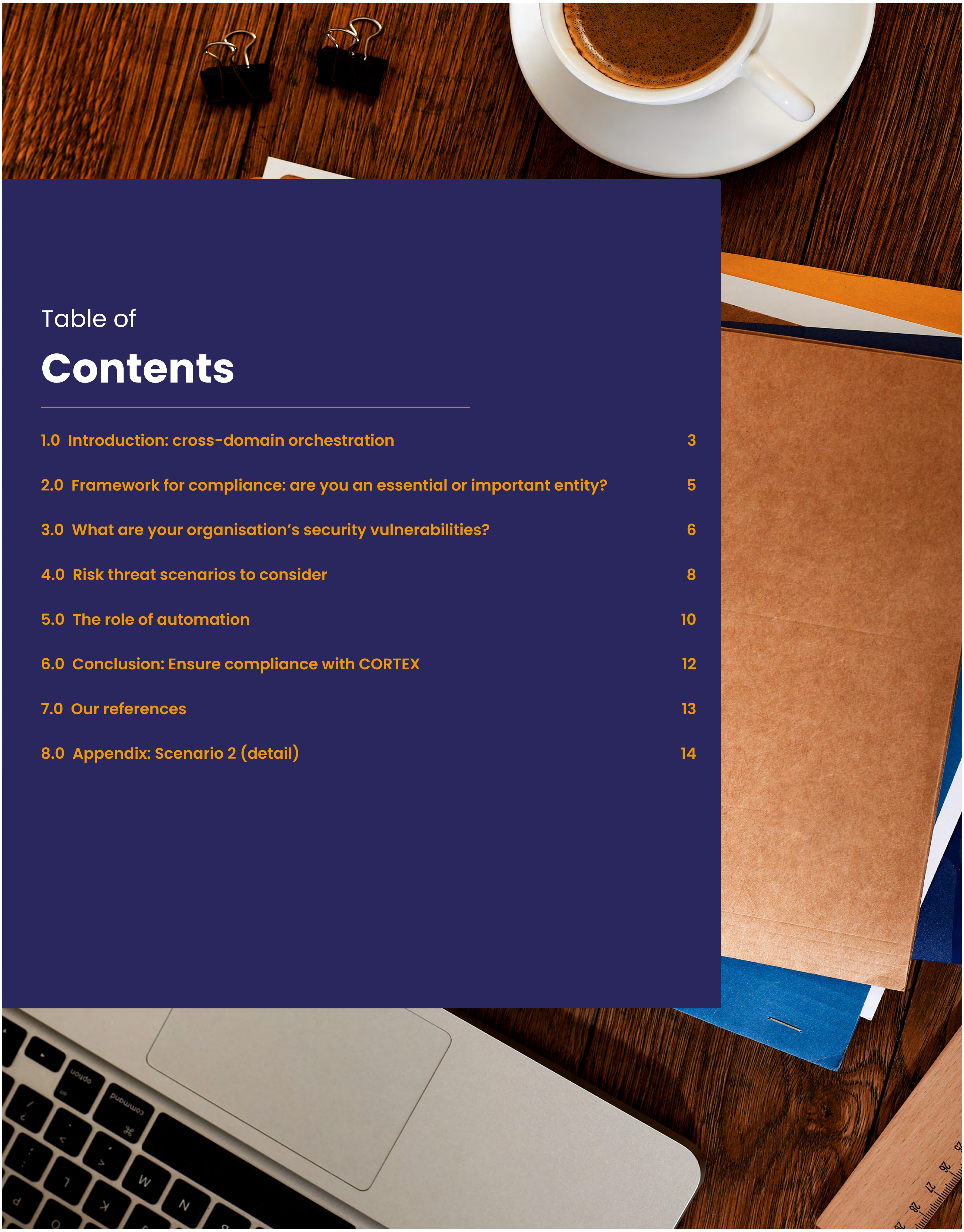


Table of

Contents

Meeting your UK Telecoms (Security) Act (TSA) 2021 and NIS 2 Directive obligations will require a cross-domain approach, but automation will be essential.

Introduction

cross-domain orchestration

The UK Telecoms (Security) Act (TSA) 2021 came into effect in 2021, while the European Union's (EU's) NIS 2 Directive (EU 2022/2555) was enacted into law on 17th October 2024. Both provide an advanced and extended framework for ensuring the security and resilience of communications networks throughout both regions.

The TSA provides the UK's communications regulator Ofcom with extensive powers to ensure that communications service providers (CSPs) are implementing the best possible security practices[1]. At its heart there are several themes:

- The ability to identify risks around security compromises.
- Taking action to reduce and mitigate these risks.
- Continuous evaluation and proactive review of security practices to prevent future security breaches.
- Responsibility on CSPs for informing network providers (and any other appropriate parties), as well as the regulator of any security breaches as soon as reasonably practicable.

The TSA takes a tiered approach to implementation. For example, Tier 1 public telecom providers (those with over £1 billion turnover) had to implement the act's obligations by 31 March 2024. While for Tier 2 providers (turnover above £50 million) the deadline is the same date in the following year – unless they supply any part of their network or a service to a Tier 1 provider (in which case it's the same deadline as for Tier 1 CSPs). Tier 3 providers are not expected to follow the measures in the code unless they supply Tier 1 or 2 providers. These obligations apply throughout the supply chain.

The NIS 2 Directive, on the other hand, is a much broader reaching framework to align the security of networks throughout the EU and does not only apply to telecommunications but to other sectors of critical national importance. Because of its over-arching impact and new requirements for governance, compliance with the UK's TSA does not result in compliance with the NIS 2 Directive.

TSA mostly relates to the operational core (IMS, RAN, and so), but NIS 2 goes further to include the perimeter of the operator domain. But the perimeter is actually harder to define than it might seem at first glance.

For example, it includes CPEs, routers, and IoT devices, which are generally positioned at the edge

of the network, and which are therefore seen as the boundary – or perimeter. But things are not quite as straightforward as that.

For example, a recent Wi-Fi hack of UK railway stations[2] (in which terrorist messages were seen by anyone using the railway station's Wi-Fi throughout the UK), shows how difficult this is difficult to define and indicates a level of fluidity.

The threat was delivered over public Wi-Fi, accessible to commuters – but targeted systems that, in turn, connect to the network, in this case, of the station operator, Network Rail, which, as a provider of critical national infrastructure is covered by the TSA. Had this happened in, say, France, NIS 2 would then apply.

So, importantly, the perimeter can also include end-user devices, such as smartphones and laptops, which are also likely to be sharing data with other enterprise applications, such as CRM and finance solutions, as well as consumer applications. It might also include IT platforms and services outside the core operator domain – so how can 'grey' areas be brought under the purview of the requisite security framework?

NIS 2 thus also extends to people, not just software and hardware. It means that NIS 2 will have far-reaching impacts for cyber security, as it seeks to proactively protect the perimeter (wherever that may be), as well as other operational domains. We Are CORTEX can bring other tools together into a single pane of glass.

It is already understood that ISO 27001 certification, while providing an excellent foundation for TSA and NIS 2 readiness isn't sufficient on its own to claim compliance. As a voluntary standard, mandatory legislation such as TSA and NIS 2 have precedence and require on-going, proactive documented measures.

Moreover, as we have noted the scope of NIS 2 is far broader than for the TSA – compliance with TSA will help, but it is not sufficient.

One of the problems is that the EU directive that forms the basis of NIS 2 sets out guidelines and scope for policy, but we have to look further for interpretation guidelines.

As such, it can take detailed study to determine where to act. In this paper, we'll consider an approach to compliance, using one specific threat scenario is a model for discussion.

Finally, it should be remembered that non-compliance has serious consequences. EU Member States can apply fines of up to €10 million or 2% of annual revenue for non-compliance with NIS 2, or for certain breaches.

Similarly, failure to comply with TSA can lead to fines up to 10% of turnover. And, if there is ongoing failure to comply, fines of up to £100,000 per day can be levied. Moreover, OFCOM has the power to impose fines at the same level for failure to explain why a code of practice has not been adhered to – and £50,000 each day for ongoing non-compliance. Finally, critical entity management bodies (i.e., C-level executives can be held personally liable for failure to meet their obligations.

The bottom line is that assumptions about existing security measures are likely to be false when considering new instruments, such as NIS 2. Read on to explore NIS 2 compliance through the context of a key network domain: the perimeter.

Framework for compliance:

are you an essential or important entity?

First, some context. NIS 2 (EU Directive 2022/2555) replaced the earlier NIS framework (EU Directive 2016/1148), and detailed which entities would be covered, and the level of compliance that each must achieve. This was highlighted in Annex 1, a useful summary of which has been provided by the UK's National Cyber Security Centre (see below).

As can be seen, this also summarises obligations using the terms:

- **'Essential**' (no choice in the matter)
- **'Important'** (specific requirements, but not all), and
- **'Not in Scope'** (no obligation to comply, but still recommended).

So, the first step in compliance is to determine where your organisation sits in this framework.

Figure 1: Public and private entities covered by NIS 2

Source: National Cyber Security Centre

ANNEX - I

ESSENTIAL ENTITY

(sectors of high criticality)

	Large Entities (>=250 employees or more than €50M in revenue)	**Medium Entities** (50-249 employees or more than €10M in revenue)	**Small/ Micro Entities**
Energy	Essential	Important	Not in Scope
Transport	Essential	Important	Not in Scope
Banking	Essential	Important	Not in Scope
Financial Markets Infrastructure	Essential	Important	Not in Scope
Health	Essential	Important	Not in Scope
Drinking Water	Essential	Important	Not in Scope
Waste Water	Essential	Important	Not in Scope
Digital Infrastructure	Essential	Essential	Essential
ICT Service Management (B2B)	Essential	Important	Important
Public Adminstration Entities	Essential	Essential	Essential
Space	Essential	Important	Not in Scope

ANNEX - II

(other critical sectors)

	Large Entities (>=250 employees or more than €50M in revenue)	**Medium Entities** (50-249 employees or more than €10M in revenue)	**Small/ Micro Entities**
Postal & Courier Services	Important	Important	Not in Scope
Waste Management	Important	Important	Not in Scope
Chemicals	Important	Important	Not in Scope
Food	Important	Important	Not in Scope
Manufacturing	Important	Important	Not in Scope
Digital Providers	Important	Important	Not in Scope
Research	Important	Important	Not in Scope
Entities Providing Domain Name Registration Services	All sizes, but only subject to Article 3(3) and Article 28		

What are your **organisation's security vulnerabilities?**

It is important to recognise that interpreting NIS 2 can be challenging. The directive is broad[3] and, while it clearly sets out aspirations and guidance, it does not specifically turn to implementation and practicalities. As we noted, we must search for deeper guidance and insights. For example, the NIS Cooperation Group[4] (NCG) has set out a number of risk scenarios for consideration.

Since our focus in this paper is on risk scenarios for telcos, and since we have identified the perimeter as the effective frontline, we will use this as an example to highlight the fluidity of this domain – and the challenges in ensuring NIS 2 compliance in this context. According to the NCG, the risk scenarios for telcos include:

- **Risk Scenario 1** – Supply chain attack to gain access to the infrastructure of operators – this is one reason why equipment from designated high-risk vendors have been banned across many countries, such as those in the EU, the U.S. and the U.K.
- **Risk Scenario 2** – DDOS attack to cause a large-scale network outage.
- **Risk Scenario 3** – AI-powered disinformation.
- **Risk Scenario 4** – Espionage.

Of course, it's also worth noting that the risk scenarios are different for each sector.

For example, in the electricity sector they are defined as, respectively:

- malicious activities by insider threats,
- espionage,
- hybrid attack to cause a large-scale energy network outage,
- gas shortages,
- vendor lock-in introduces vulnerabilities in products, and
- diplomatic row exacerbates vendor lock-in consequences.

So, it's clear to see that in each vertical covered by NIS 2, different vulnerabilities have been identified.

Returning to telco risks, Risk Scenario 2 is particularly relevant, because it essentially involves attacks to the perimeter, so we can see that the vulnerability of this domain has been recognised at the highest levels.

While the scenario outlined in Table 1 (below) is broad in scope, it can be seen that it actually covers an ever-changing landscape, because the devices at the edge are in constant flux and this is a dynamic environment.

That's also because, as the NCG points out:

> *"With 5G deployment and the growing number of IoT devices, the sector is rapidly expanding… [to]…stretch the surface of the networks, consequently increasing their vulnerability."*

In other words, even if the network perimeter were static today, it will change tomorrow. But, even that insight doesn't go far enough to really capture the risks, as we shall see.

However, unlike the NIS 2 directive, the NCG goes further and provides a list of assets to be considered — practical guidance absent from Directive 2022/2555 — and this extends, not just to physical or logical assets, such as may be mapped into inventory systems, but also people and roles, such as administrators and, crucially, end users.. Scenario 2 might be considered a 'simple' DDOS attack. However, when you consider what devices and applications — and end users — could be considered a perimeter threat, it becomes more fluid and unpredictable.

Table 1: Risk Scenario for telcos

See also Appendix 1

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
DDOS ATTACK TO CAUSE A LARGE-SCALE NETWORK OUTAGE	State sponsored actors/ Hacktivists	DDOS attack	Network devices Servers Internet Exchange Points (IXP) Backbone internet provider Server/ data centre provider		Unavailability of the Internet Economic Social/societal

The importance of non-compliance cannot be understated. The aim of both regulations is to ensure that national security is not compromised, which is why fines will apply for non-compliance. But it is also a clear example of why NIS 2 goes much further than the TSA or ISO 27001, because now we have to consider, for example, the mobility of users and how that, in turn, impacts the perimeter.

Directive 2022/2555 explicitly refers to remote administration and management, but we must turn to draft recommendations for implementing the application of NIS 2 for further guidance.

For example, one such[5] sets out:

"… rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers"

…and it also considers remote access and remote working. These factors can have significant impacts on the perimeter, changing the threat landscape under Scenario 2.

This means that we are confronted with an ever-changing scenario as different devices (and different applications), and the people that use them create a constantly changing edge.

When we consider 5G, remote working, remote access and more, we can see that achieving compliance with NIS 2 in the face of all possible variables, threat vectors and dynamic changes (activating a new IoT device, shifting from the main office to the remote on Tuesday and Thursday) create a flux of changing conditions that mean the perimeter can never be static.

In summary, then, the NIS 2 Directive Risk 2 scenario is crucial and should be at the forefront of thinking for all telcos and service providers, because it clearly shows how critical threats can arise at the edge, which we already know is a fluid parameter. How can you proactively protect, monitor and react to change?

Risk threat
scenarios to consider

What's needed is a clear analysis of the risks that apply to any given scenario identified. Of course, there are many aspects to consider, for example:

- **Identify entity classification:** Determine if the organisation is considered an "essential" or "important" entity under the directive
- **Gap analysis:** Identify areas that need improvement
- **Security policies:** Develop and implement security policies, processes, and controls
- **Governance**: Ensure accountability and effective governance
- **Supply chain security**: Assess and manage supply chain security risks
- **Incident response:** Establish robust incident response capabilities and well-developed incident management plans
- **Business continuity:** Ensure business continuity capabilities
- **Security audits:** Conduct regular security audits and tests
- **Employee awareness:** Conduct regular training and awareness assessments for employees
- **Incident reporting:** Send an early warning within 24 hours of becoming aware of a breach or attack
- **Cyber recovery plan:** Create a cyber recovery plan and conduct regular testing and validation.

One of the most important considerations is to take a culture-wide (as NIS 2 encompasses employee training and policies too), cross-domain approach to avoid siloes of data, which can leave security gaps.

In other words, NIS 2 compliance depends on automation implemented correctly on automation platforms that have security at their heart – stitching together core and disparate systems, including some of your other automation capabilities. Ensuring a well governed, smooth flow of data exchange is not just important, but potentially business critical, as is securing a consolidated, correlated view in the process.

A cross-domain approach is thus critical and requires three key considerations:

- Security policies
- Governance
- Security audits

The network, of course, has its core and boundaries, both of which need to be secured. The following list provides the components that need to be included:

- Network considerations:
    - Secure the core
    - Secure the transport / metro domain
    - Secure the perimeters (digital and physical i.e. User access, Access control etc. – as well as updates / access to CPE / IoT devices)
- Policy and corporate considerations:
    - Create the governance to maintain best practise.
    - Create the culture to maintain compliance

The important thing to note here is that the domains of the network do not exist in isolation. Devices at the perimeter, for example, register with systems in the core —such as policy servers, user account databases and so on — while they must also register with aggregation functions that connect to different devices in a given locality. This can be temporarily, in the case of mobile user equipment, or more lasting, in terms of home routers and broadband modems.

As a result, the emphasis must be on cross-domain approaches, because edge devices interact with systems beyond the access layer. To return to Scenario 2, if we consider a systems administrator that needs to access systems while working from a hotel room while visiting another country, we can see that the perimeter is truly elastic! The same applies if a user of corporate systems works from a temporary location and accesses enterprise software such as a CRM or ERP system. These are part of the network and remain entry points that must be guarded.

And, of course, governance is vital. Governance is the overarching framework that ensures ongoing compliance; vigilance must be constant. So, controlling who can do what and protecting against infringements is essential.

As is resilience. Building security resilience is essential, on a proactive, on-going basis. IoT devices, routers, and so on, are static entities and relatively easy to protect, but security resilience must also include fluid aspects such as end-use devices and applications. How can you achieve this?

Unlike general purpose process orchestration tools or network domain orchestrators, CORTEX is proven to enable CSPs to become self-sufficient by orchestrating 'as-is' CSP business processes, as well as large-scale planned change (digital transformations).

The role of **automation**

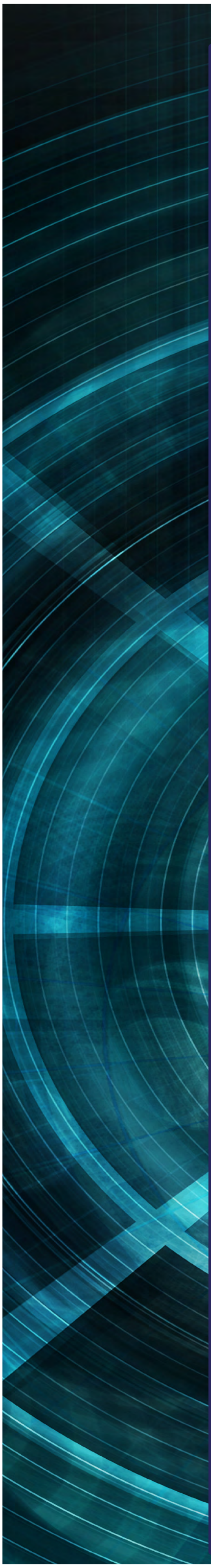
In such a challenging and dynamic landscape, automation may not be your first thought, but it can play a crucial role. That's because tracking all the events and actions that could lead to vulnerabilities or are signs of emerging attacks, as in Scenario 2 requires visibility of a chain of actions and inputs – that need to be collected and correlated from disparate systems and across all relevant domains.

Additionally, actions that can impact such systems — from admin access to updates — are also covered by NIS 2, so these need to be taken into consideration. In sum, automation of all such activities reduces the possibility for human intervention and the scope for error. Similarly, if you select the incorrect automation tools, you can expose your business to automated risk propagation.

In other words, NIS 2 compliance depends on automation implemented correctly on automation platforms that have security at their heart – stitching together core and disparate systems, including some of your other automation capabilities. Ensuring a well governed, smooth flow of data exchange is not just important, but potentially business critical, as is securing a consolidated, correlated view in the process.

But there's more than that. As noted, the correct automation confers protections – from rights access and admin control, to tracking versions and version controls, enabling updates to safely and securely proceed at scale – and that's not considering all of the obvious business benefits normally associated with automation. NIS 2 raises many questions and automation must be considered at every step in the compliance journey.

Automation offers a critical and continuous solution to security thinking and activities, even those regular updates to edge devices can be automated to ensure that they are always protected to the highest degree possible.



This not only enables updates that are applied to routers and IoT devices (as well as mobile devices, when necessary), but also the ability to allow for rollback should problems or incidents arise.

A secure automation platform is a key consideration, and sadly, few enterprise platforms have matured their security sufficiently to equip you with TSA and NIS 2 automation readiness.

Similarly, few automation platforms span multiple domains – which is a critical step towards success. Individual automations (think RPA and scripting) help but don't bring everything together under the necessary security framework and governance that telcos now operate under; ultimately, automation must include all domains as well as people over every function.

To give just one example, security rules should apply at every stage in the lifecycle of an automation – from design, to test to launch in production environments. How do you ensure that the users of the automation are not permitted to change it? Only composers should be able to edit and adapt, for example.

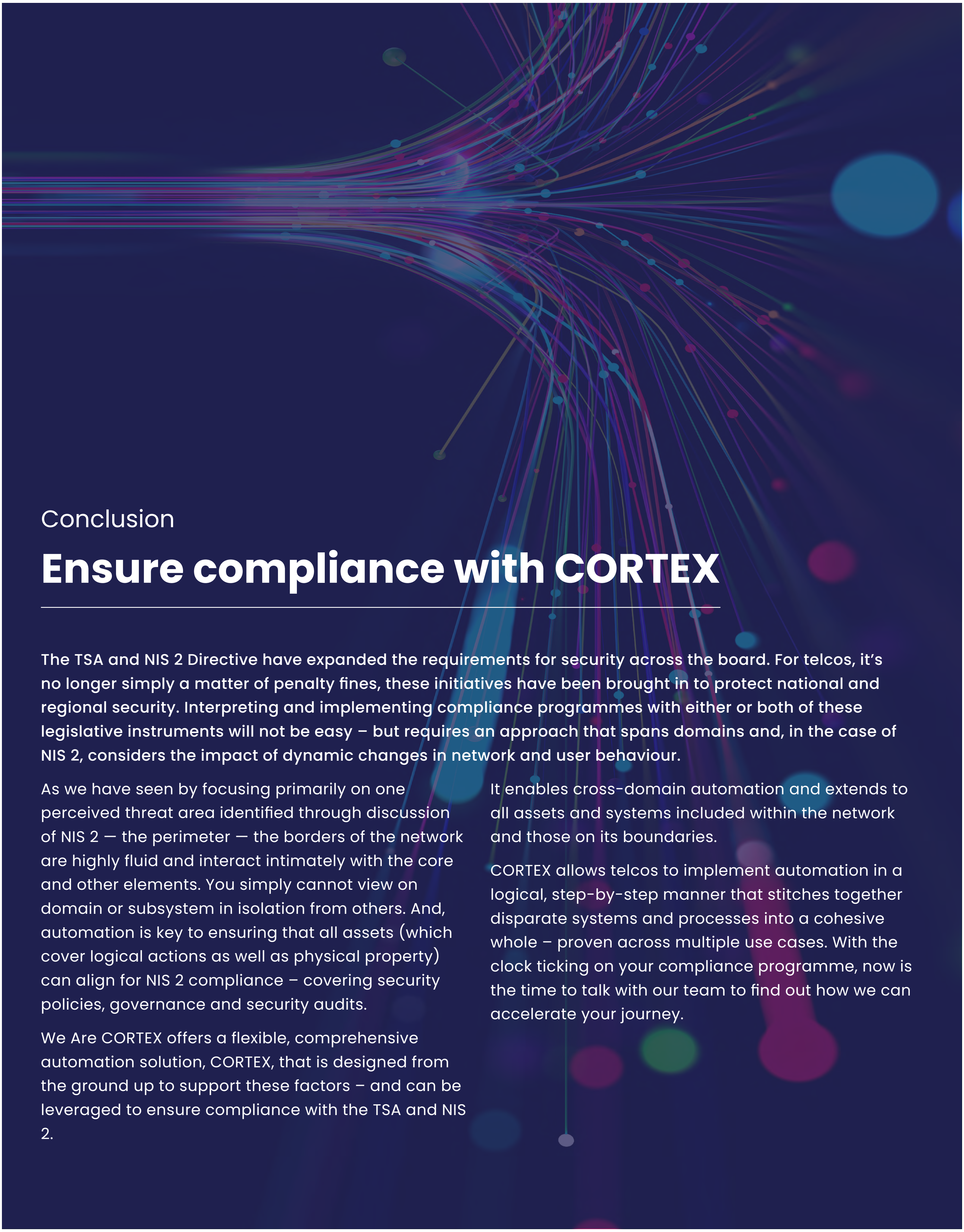
Like all parts of your operation, automation must be carefully governed, not just in terms of users and system access, but with all full control of revisions and changes – being able to automate something is only a very narrow part of the answer, as an organisation you must control the complete lifecycle with appropriate safeguards that extend to the different stakeholders and roles.

Perhaps the key difference in NIS 2 is the ways in which supporting documents spell out assets that should be considered as part of the overall approach. As previously noted, this goes far beyond network systems (routers, transport and so on), extending to 55 different categories[6].

These cover operating systems, firmware, protocols and software applications, among other considerations such as real-time data and network topology. In other words, it seeks to cover every level in the network and operational systems and domains – automation must also embrace all such layers.

To return, for the final time, to our remote worker case, not only access to systems must be secured via VPNs, but also the interactions of different software packages that are linked must also be protected – can the CRM when used by this operative access data in another third-party system resident on the cloud when the user is outside the corporate main office infrastructure? Understanding NIS 2 means thinking about all possible such interactions and interpreting the provisions of the source directive.

NIS 2, then, raises difficult questions, but it should be apparent that automation is the fundamental tool to achieve cross-domain compliance. But the automation tools need to consider these inter-domain challenges – which is what our platform CORTEX enables.



Conclusion

Ensure compliance with CORTEX

The TSA and NIS 2 Directive have expanded the requirements for security across the board. For telcos, it’s no longer simply a matter of penalty fines, these initiatives have been brought in to protect national and regional security. Interpreting and implementing compliance programmes with either or both of these legislative instruments will not be easy – but requires an approach that spans domains and, in the case of NIS 2, considers the impact of dynamic changes in network and user behaviour.

As we have seen by focusing primarily on one perceived threat area identified through discussion of NIS 2 — the perimeter — the borders of the network are highly fluid and interact intimately with the core and other elements. You simply cannot view on domain or subsystem in isolation from others. And, automation is key to ensuring that all assets (which cover logical actions as well as physical property) can align for NIS 2 compliance – covering security policies, governance and security audits.

We Are CORTEX offers a flexible, comprehensive automation solution, CORTEX, that is designed from the ground up to support these factors – and can be leveraged to ensure compliance with the TSA and NIS 2.

It enables cross-domain automation and extends to all assets and systems included within the network and those on its boundaries.

CORTEX allows telcos to implement automation in a logical, step-by-step manner that stitches together disparate systems and processes into a cohesive whole – proven across multiple use cases. With the clock ticking on your compliance programme, now is the time to talk with our team to find out how we can accelerate your journey.

Our references

1. https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted
2. See, for example: https://www.openaccessgovernment.org/cyber-attack-disrupts-wi-fi-services-at-major-uk-railway-stations/182822/
3. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
4. EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors (Follow up to the Council Conclusions on the EU's Cyber Posture of 23 May 2022 and Council Conclusions on the EU Policy on Cyber Defence of 22 May 2023).
5. Ref. Ares(2024)4640447 - 27/06/2024
6. See Annex 2.3 in EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors

Appendix:

Scenario 2 (detail)

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
DDOS ATTACK TO CAUSE A LARGE-SCALE NETWORK OUTAGE	State sponsored actors/ Hacktivists	DDOS attack	Network devices Servers Internet Exchange Points (IXP) Backbone internet provider Server/ data centre provider		Unavailability of the Internet Economic Social/societal

Context:

A State actor threat agent supported by a hacktivist group, engages in large-scale DDoS attacks on the communication networks and infrastructures of several EU countries, with the aim of causing social unrest and disrupting economic activities, including, for example, the disruption of digital and online payments, other digital services and logistical processes.

Technical:

The attackers use Domain Name System (DNS) amplification and a pre-prepared botnet of infected home routers and other end-user devices. Some operators are able to stem the flow by using AI-enabled cyber defence measures that are able to re-route, filter and block malicious traffic. Other operators across the EU do not manage to deal with the attack.

Impact:

Network outages on the affected operators last for several hours. While the attack is not fully mitigated and access restored to some of the most critical customers, cascading effects take place with significant impact. The economic impacts are initially local, as shops and industries would be able to provide very few services without communications. Industries and businesses beyond the geographical coverage of the current scenario could be affected shortly after.

Damage can escalate if the financial sector is hit. The messaging network for financial transactions, for instance, suffers persistent disruptions over a substantial period (e.g., transactions processing, digital banking services, etc.), further limiting the overall economic activity and trade.

We Are CORTEX

Kings Park House
22 Kings Park Road
Southampton
SO15 2AT

Phone:	+44 23 8254 8990
Email:	hello@wearecortex.com
Visit:	wearecortex.com