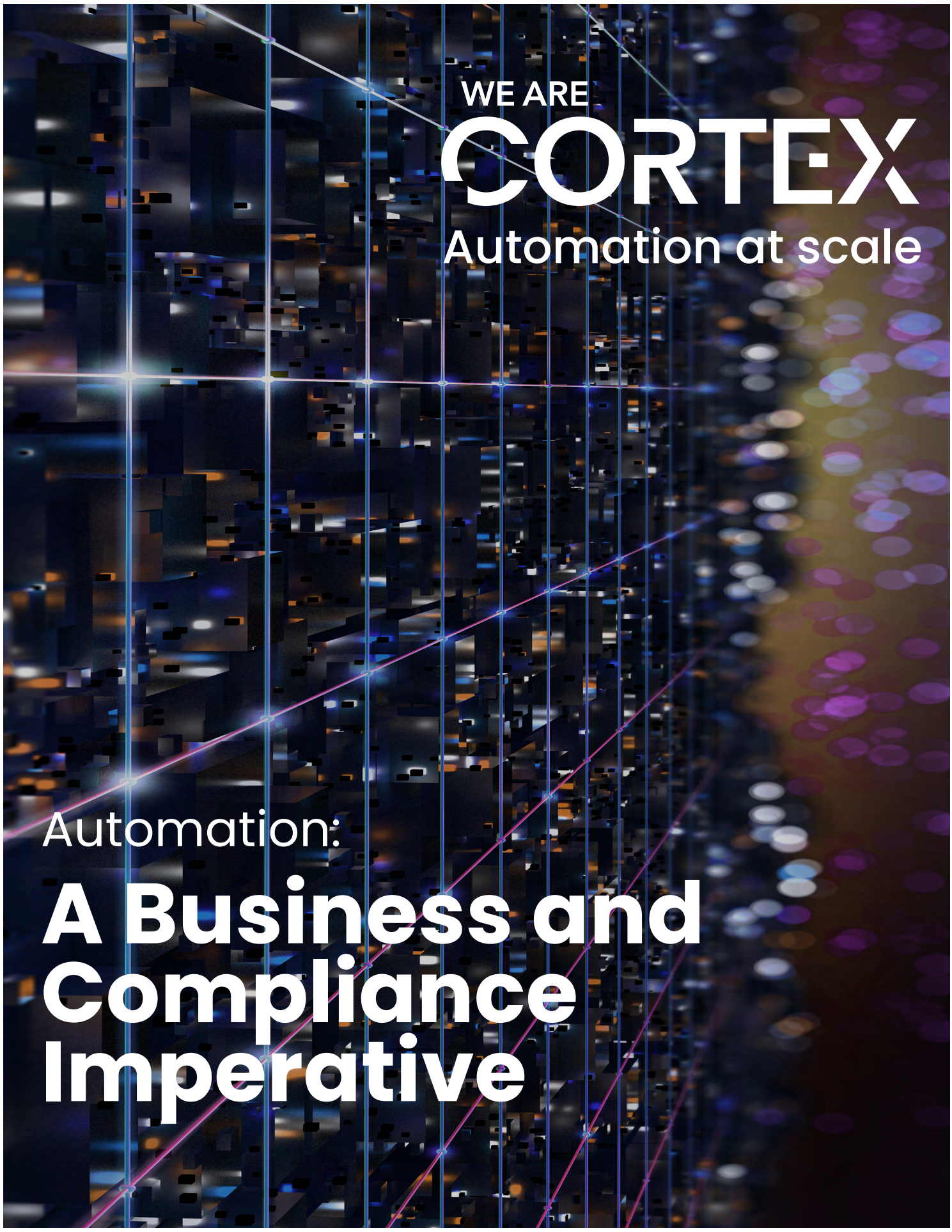


Automation:

A Business and Compliance Imperative

©2023 CORTEX Ltd.



About

We Are CORTEX

In today's rapidly evolving digital landscape, Communications Service Providers (CSPs) face immense challenges in meeting the ever-increasing demands of their customers while maintaining operational efficiency.

Our library of workstations and functional blocks provides the framework to template and create any automation flow. Any process can be automated from our framework, in a simple GUI environment that provides a staging ground and easy deployment to the live network.

We design workflows based on our composition framework and palette, allowing you to craft processes that meet your needs.

Cloud or on-premise, our solutions scale elastically, ensuring the smooth delivery of automated processes.

©2023 CORTEX Ltd.



Table of
Contents

Introduction: The Drivers of Automation 4

Background: Evolving Regulations 5
Automation 6

The Legislative Drive for Automation 7
How does this affect the CSP roadmap? 8

Focus on the Telecoms Security Act 9

An International Perspective 12

Implications for your Business 13

How to Manage the Transition 14
Achieving compliance through automation 14

We Are CORTEX: Automating your Network and Operations 16

Conclusion: Efficient, Fast, Successful 17

Our References 18

©2023 CORTEX Ltd.

WE ARE CORTEX



THE NETWORK AUTOMATION AND ORCHESTRATION MARKET IS PREDICTED TO GROW AT A CAGR OF 9.4%

Introduction:

The Drivers of Automation

Network and operational automation are now at the forefront of most Communications Service Provider (CSPs) and operator thoughts. Automation provides service agility and significantly reduces OPEX, enhances service differentiation, and boosts efficiency, never more so than in the (coming) 5G Standalone (SA) era.

That's why, according to Analysys Mason, the network automation and orchestration market is predicted to grow at a CAGR of 9.4% between 2023 and 2028, reaching $16.5 billion[1]. This growth will be partly fuelled by CSPs rolling out 5G SA and cloud-native digital transformation journeys, which demand higher levels of automation to manage network complexity.

But there is another significant driver for automation: the introduction of ever-more complex compliance regulations within the telecoms industry. Legislation, such as the UK's Telecommunications Security Act (TSA) 2021 and the updated EU Network and Information Systems (NIS2) directive, is creating regulatory pressure on CSPs to transform their networks and ensure the highest levels of security and transparency.

Data security and the need to protect against breaches are a matter of national concern and seen as a means to ensure stable international relations.

As a result, governments around the world have stepped up their efforts to protect national security from hostile actors – both geopolitical entities and individuals. Automation is key to enabling CSPs to meet those obligations.

In this paper, we explore the impact of network automation in driving digital transformation to unlock promised benefits - and show how CSPs can use automation to meet changing regulatory obligations.

"Governments and international organisations are delivering top-down requirements for network transformation, for which automation is essential."

©2023 CORTEX Ltd.



Background:

Evolving Regulations

To remain competitive in today's mobile and fixed ecosystem requires operators to provide optimum customer QoE, differentiated services, agility to ensure that they are quickest to market with innovative solutions and services, reliability, scalability, and the flexibility to meet changes on demand.

Automation is central to meeting these aims.

However, another imperative for automation is the changing face of regulatory frameworks across the globe.

Governments and international organisations are delivering top-down requirements for network transformation, for which automation is essential.

Partly driven by security risk mitigation and the need to diversify supply chains, these directives are giving automation efforts new impetus, and in many cases contain legally binding timeframes.

One notable example is the UK's TSA[2], which was introduced on 1st October 2022, and which aims to ensure the security of public electronic communications networks and services. Automation is key to meeting the obligations imposed by this act.

Importantly, many such acts impose a time limit for their implementation by CSPs. This means that, from a regulatory perspective, there is a sense of urgency, with many CSPs having to accelerate automation programmes.

So, what does this mean, in practice, for CSPs and operators?

©2023 CORTEX Ltd.



Automation

Operational and network automation is no longer a nice-to-have, but a must-have if operators are to keep pace in the digital world.

Furthermore, the introduction of 5G Standalone (SA) and future Fixed 5G bring another layer of complexity. Operators must adopt 'security first' mindsets while also developing dynamically orchestrated services and network slices.

Network slices, in particular, demand network automation to ensure optimum QoE, reliable orchestration, active monitoring, active automated hardening, service upgrades, and new service introductions and retirements.

Network automation is the process of automating network configuration, management, testing, deployment, and operation of physical and virtual devices within a network.

In the 5G era, operators can no longer rely on competitive pricing – which is unsustainable for the telecoms industry – instead service agility, differentiation, and providing optimum QoE will be the new battleground. All of which require strategic orchestration and automation.

According to Cisco, 95% of network changes are today performed manually – this can lead to configuration errors and inconsistencies in the network and, in turn, downtime[3].

Moreover, investigations by We Are CORTEX show that, for most operators, network config checks fall into four categories:

- Known configuration and compliant
- Known configuration and not compliant
- No known configuration, and,
- Not checked for configuration

While Cisco's research shows that network changes are still largely manual, it is also clear that they may not be according to a standard or - worse still - not done at all.

In the new climate of TSA and NIS2 in Europe, and also in consideration of 5G SA, and other services, strategic automation is vital.

At this point we need to distinguish between 'process automation' and what we might term 'strategic automation'.

Automation through the intervention of RPA or bots is commonplace, but these lack contextual awareness and are not sufficient for addressing regulatory pressures.

AI has a role to play, but that must also be seen in the context of emerging governance frameworks. Strategic automation must address all current and future regulatory concerns.

Put simply, strategic automation and orchestration are critical to survival. Rising costs; ever-larger volumes of data; increased complexity; dynamic orchestration and network slicing; and elastic scalability – all mean that it is almost impossible to see how an operator could exist with largely manual approaches.

Of course, strategic automation and orchestration also brings other benefits, such as the ability to refocus teams on revenue growth and strategic opportunities, as well as cost reduction.

©2023 CORTEX Ltd.

The Legislative
Drive for Automation

The main drivers for automation and digital transformation for CSPs and operators are:

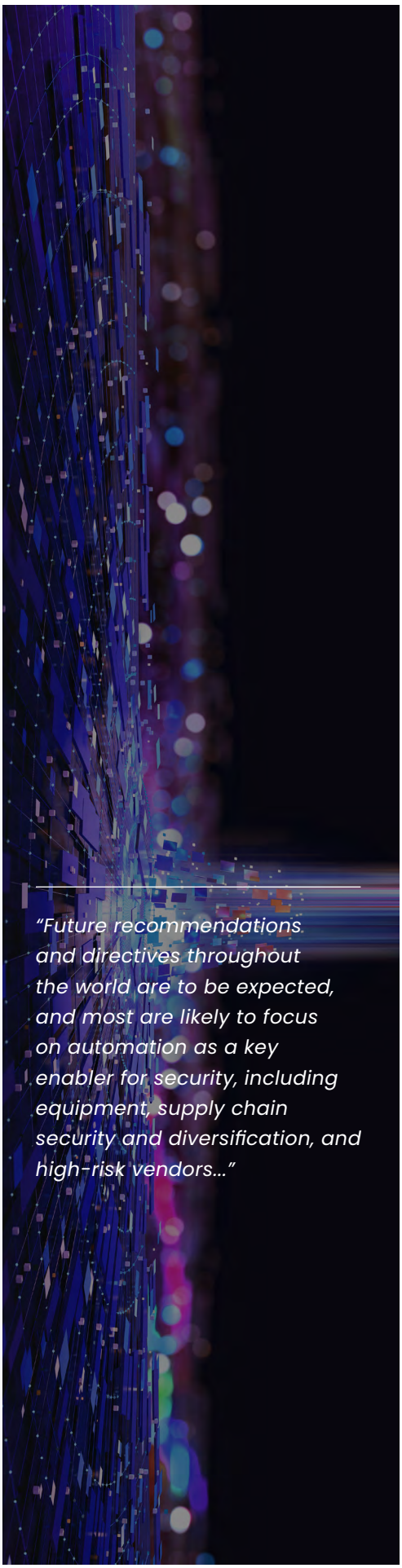
- Cost reduction (and also cost elimination by reducing the required human input)
- Risk minimisation, by removing human error, and innovation
- Capability enhancement, such as bringing a novel service to market and, more particularly with the introduction of 5G, which can only be successful through automation

However, compliance is also now a factor, as there is growing impetus from legislation, which means that, in many cases, CSPs are having to accelerate their automation programmes. Key examples of evolving regulatory obligations are the UK's Telecoms Security Act (TSA) 2021, the US Securing Global Telecommunications Act, and the Network and Information Security 2 Directive (NIS2) across the Europe Union.

This has implications for CSPs at every business and operational level, including the technology stack, operational processes, and supply chain management and diversification. All CSPs operate under the auspices of a regulator and compliance with relevant legislation is existential – non-compliance can lead to the revocation of licenses and fines that threaten business viability.

Take just one example – the UK TSA. This act's main goal is to enhance security and resilience for critical infrastructure and to protect networks from cyber threats and attacks, private or potentially state-sponsored – a good example of the kind of thinking behind these regulations is the banning of equipment from designated 'High-risk Vendors'.

The act is not only targeted towards communication services. The UK Government has also introduced the act to safeguard the country's critical infrastructure and to ensure its reliability and resilience – including connectivity, energy, transport, healthcare, and so on. In short, the act aims to close the threat gap by creating a more secure, resilient national infrastructure.



"Future recommendations and directives throughout the world are to be expected, and most are likely to focus on automation as a key enabler for security, including equipment, supply chain security and diversification, and high-risk vendors..."

©2023 CORTEX Ltd.

How does this affect the CSP roadmap?

Importantly, the TSA outlines some tight deadlines for its implementation, with a tiered approach, including suppliers:

- For Tier 1 providers (those with over £1 billion turnover), the act's obligations must be implemented by 31 March 2024.
- For Tier 2 providers (turnover above £50 million) that deadline is 31 March 2025 – except if 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. They are still entitled to implement the Code of Practice – which given the benefits offered by automation anyway would be a sensible move.
- Importantly, these obligations also apply to suppliers, which means that any providers supplying Tier 1 and 2 CSP are subject to the same deadlines as the CSP.

Automation will be key to achieving these goals. At the same time, automation is not only required to address security vulnerabilities, it will also be needed to enable the secure exchange of data between processes and services without the need for human intervention (which, of course, represents a potential security threat).

Future recommendations and directives throughout the world are to be expected, and most are likely to focus on automation as a key enabler for security, including equipment, supply chain security and diversification, and high-risk vendors (see Section below: "An international perspective").

The industry is on a one-way path towards network and operational automation not only to support digital transformation and the efficiencies and productivity increases it provides, but also to ensure network and supply chain security, and from a regulatory perspective.

In this landscape, operators will be increasingly subject to non-compliance enforcement fines and levies by national regulators, such as Ofcom. Automation is a key lever to help avoid such penalties.



"The TSA represents a significant change for the UK telecoms industry, from a siloed reactive approach to security to a threat-led, proactive approach based on promoting resilience throughout the network and diversification of the supply chain so that there is less reliance on single entities."

©2023 CORTEX Ltd.

Focus on the

Telecoms Security Act

The TSA represents a significant change for the UK telecoms industry, from a siloed reactive approach to security to a threat-led, proactive approach based on promoting resilience throughout the network and diversification of the supply chain so that there is less reliance on single entities. Before the act, CSPs and telecoms providers were responsible for setting their own security standards; following its introduction, the TSA aims to tighten the legal duties on CSPs.

The framework is based around some overriding themes, with CSPs taking on a number of responsibilities, including:

- Imposing stronger overarching security duties on CSPs, which must be able to identify the risks around security breaches and compromises.
- Requiring specific security measures, whereby CSPs must take actions to reduce these risks.
- Demanding continuous evaluation, as CSPs must review processes on an ongoing basis and proactively act to prevent future security breaches.
- Informing those who may be adversely affected by a security compromise (including network providers).
- Updating the regulator as soon as reasonably practicable in the event of any non-compliance.

The TSA is also supported by the Electronic Communications (Security Measures) Regulations 2022[4], which provides 16 regulations outlining multiple security measures that CSPs are expected to put in place, including the duty to:

- Protect stored data, and to secure the critical functions that operate and manage these processes.
- Protect network monitoring and analysis tools from hostile state actors.
- Monitor public networks to identify potentially dangerous activity, to have a deep understanding of their security risks and to report regularly to internal boards.
- Take account of supply chain risks and understand/control who can access and make changes to the operation of their networks and services.

The Telecommunications Security Code of Practice supplements the TSA, with responsibilities tiered (as listed above) to ensure that smaller CSPs do not carry an unfair burden.

"...the new act and supporting frameworks and code of practice requires CSPs to act now. Any CSP that does not comply with these security duties can be fined a maximum of 10% of their annual turnover, and, in the event of a continuing failure to comply, a rolling fine of £100,000 per day."

©2023 CORTEX Ltd.

The Code of Practice provides guidance on the key concepts that providers need to consider when complying with the TSA.

Section 2 covers the following:

- Network Architecture
- Governance
- Protection of data and network functions
- Prevention of unauthorised access or interference
- Protection of certain tools enabling monitoring or analysis
- Preparing for remediation and recovery
- Monitoring and analysis
- Reviews
- Supply chain
- Testing
- Patching and updates
- Assistance
- Competency

Importantly, Section 2.63 of the Code of Practice covers automation, stating:

> *"Automation allows for rapid prototyping and testing of new features, security patches and changes. This approach supports network resilience by limiting errors caused by human interaction and by allowing quicker remediation should issues occur. The approach supports network security by increasing the speed at which updates and changes can be made, allowing the provider to keep pace with the threat environment."*

©2023 CORTEX Ltd.

Section 3 of the Code of Practice covers technical guidance and includes the following themes:

- Management plane
- Network oversight functions
- Signalling plane
- Monitoring and analysis
- Third party supplier measures
- Customer premise equipment
- Supporting business processes
- Retaining national resilience and capability
- Virtualisation

Put simply, the new act and supporting frameworks and code of practice requires CSPs to act now. Any CSP that does not comply with these security duties can be fined a maximum of 10% of their annual turnover, and, in the event of a continuing failure to comply, a rolling fine of £100,000 per day.

Failure to provide information or to explain a failure to follow the Code of Practice to Ofcom could result in a fine up to a maximum of £10 million, or for a continued failure, £50,000 per day.

Given the complexity of meeting these obligations, automation is the only solution – a manual approach is not an option. Automation is essential for data exchange and to eliminate human error or security vulnerabilities that might be caused by human intervention. Every step of the process is a potential vulnerability, so employing automated workflows can narrow this security gap.



FAILURE TO PROVIDE INFORMATION OR TO EXPLAIN A FAILURE TO FOLLOW THE CODE OF PRACTICE TO OFCOM COULD RESULT IN A FINE UP TO A MAXIMUM OF £10 MILLION, OR FOR A CONTINUED FAILURE, £50,000 PER DAY.

©2023 CORTEX Ltd.

An International
Perspective

It's not just the UK that is moving down this regulatory path – which demands automation to manage network complexity and to remove human error or intervention. In late 2022, the US Federal Communications Commission (FCC) officially implemented the provisions of the Secure Equipment Act[5], which is aimed at prohibiting the use of communications equipment from Chinese suppliers Huawei, ZTE, Hytera Communications, Hikvision, and Dahua that are deemed to pose a risk to US national security.

In September 2022, the US Senate passed the Securing Global Telecommunications Act, which requires the Department of State develop and submit to Congress a strategy to promote the use of secure telecommunication infrastructure in countries other than the US.

Most notably, the State Department must also report to Congress "on efforts by China and Russia to advance authoritarian interests or oppose fair, industry-led processes at the International Telecommunication Union, the U.N. agency involved with setting telecommunications standards and related regulatory activities; and opportunities for greater collaboration with allies and partners to promote secure information and communications technology infrastructure in countries other than the United States."

Meanwhile, in January 2023, the EU published the new Network and Information Security 2 (NIS2) Directive – member states have 21 months i.e., until 17th October 2024 to integrate the provisions of the directive into local legislation. The Directive is designed to help organisations protect themselves against cyber threats and to ensure that the EU's cyber infrastructure is more secure and robust.

Its aim is to impose security requirements, address supply chain security and introduce harmonised enforcement requirements throughout the region. It also addresses the importance of information sharing and (inter)national cooperation in the field of crisis management. Clearly a manual approach would be ineffective – again, automation will be key to its success.

Furthermore, an explanatory consultation on the future of electronic communications and infrastructure, run by the European Commission between February and May 2023, explicitly mentioned the vital role that automation will play. "Promoting cross-sectoral cooperation is critical, for stakeholders, because connectivity, cloud, and automation are key drivers for many vertical industries", it stated[6].

In Australia, the Security of Critical Infrastructure Act 2018 focuses on managing "the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure."

©2023 CORTEX Ltd.



Implications
for your Business

CSPs and operators simply cannot miss the automation opportunity because of the significant business benefits it provides. Just some of the advantages include:

- More efficient operations – automated network tasks can be run significantly faster than manual operations and eliminate human error or intervention.
- Reduced operational costs – network automation helps organisations to reduce manual labour costs, removes errors, helps CSPs to achieve business goals quicker, increases efficiency, and optimises network and operational tasks, saving money.
- Automation allows CSPs to focus on strategic goals – as processes are automated, it frees up time and resources for CSPs to focus on strategy and innovation.
- Improved network and business insight – automation provides accurate data for better analysis and greater visibility that can enable better strategic business planning.

However, just as importantly, automation is key to helping operators meet their compliance obligations in an increasingly demanding and complex regulatory environment – failure to comply can lead to financial (and reputational) implications for UK-based CSPs. As other countries adopt similar legislation, this risk is only set to increase.

As a result, automation is inevitable not just from the perspective of digital transformation, but also from a regulatory perspective, with the increased focus on network security highlighted by the TSA, which accelerates the need for automation.

The challenge is how to keep up. How do CSPs embrace automation to profit as a business, while reducing the costs and implications of compliance?

We Are CORTEX can help you manage this transition to more efficient business operations and to achieve compliance.

©2023 CORTEX Ltd.

How to

Manage the Transition

Automation is a journey. You can start wherever you want, but automation can be delivered incrementally. A common mistake is to imagine that everything must be automated, everywhere all at once – that's simply too ambitious for any CSP, particularly one that's already moving ahead with network modernisation plans and extending its coverage footprint, whether through ongoing fibre rollout or increased 5G coverage.

What you need is a guide – a map for that journey that allows you to identify and target the automation opportunities that are optimised for your business. Executing one component allows others to be addressed in turn, closing the gaps, and spreading automation as a discipline throughout your business. The end goal is fully autonomous operations – but each step enables another, so eventually all silos can be closed. This can be achieved in a graceful, stepwise manner that delivers immediate benefits while ensuring there is no disruption along the way.

But what do we really mean by automation? Automation in this sense means removing manual steps from operational and business processes, while also retaining human oversight. This means thinking about the core processes – and considering how these are affected by the legislation.

Achieving compliance through automation

To illustrate how automation helps in practice, we provide simple – but highly effective examples – each of which must be considered when implementing programmes to ensure compliance with the TSA and other relevant legislation.

System access auditing

A major operator had a manual process for systems and buildings access, which created significant complexity for IT and HR teams. The shortcomings of the existing processes were particularly apparent when considering changes in the organisation, such as new starters, those leaving – and those moving from one team or department to another.

We Are Cortex created a new, automated solution for SLAM – Starter, Leaver and Mover – governance. The new solution connects to different systems (such as Microsoft Active Directory, Identity access management systems, and more) to enable policy-based audit against employee status and access rights. The solution automatically flags and generates reports on all violations of the appropriate policies.

The result was a greater than 99% reduction in unauthorised access to accounts by leavers and movers, and a more than 99% reduction in costs. Such automated solutions will be essential in the context of the TSA and other regulations.

"A major UK operator delivers IT services and communications to one of Europe's largest call centre providers, employing around 22,000 people globally.

Unfortunately, there was a high degree of employee churn, which posed significant challenges for the SLAM process. As a result, the operator was beginning to fail the agreed SLAs – which could have led to termination of the contract."

©2023 CORTEX Ltd.



System access management

A major UK operator delivers IT services and communications to one of Europe's largest call centre providers, employing around 22,000 people globally.

Unfortunately, there was a high degree of employee churn, which posed significant challenges for the SLAM process. As a result, the operator was beginning to fail the agreed SLAs – which could have led to termination of the contract.

The We Are CORTEX team created an automation solution integrated with the HR, Identity Access Management System, Identity Governance and Administration system, and the IT systems. The automation executes the SLAM process at machine speed, making sure all necessary access requirements are observed, granting or revoking access when triggered by HR processes.

The solution met all agreed objectives and exceeded expectations. After one year, more than 80% of HR requests for SLAMs were fully automated, processing more than 500 change requests per day. After 18 months, SLAM accuracy was reported at more than 90% and the average time to process a request was reduced to less than two minutes.

Configuration compliance requests

MTTR – Mean Time To Resolve – is a key metric widely used as a KPI in Service Level Agreements. One leading CSP was unable to process the 10 million compliance checks on more than 150,000 devices required – and, as a result, was in continual breach of its own SLA with key customer accounts.

We Are CORTEX worked with the CSP to implement a solution that now accesses and validates remote device configuration, confirming that it matches technical requirements – including security parameters and firmware version, as well as service-specific settings. When discrepancies are identified, the solution automatically resolves them by reconfiguring the device. Tickets and change requests can also be raised when manual intervention is required.

Within four months, the operator had achieved the required SLA performance, with 90% compliance secured. MTTR was reduced to near real-time from the previous 24 hours.

©2023 CORTEX Ltd.

We Are CORTEX:

Automating your Network and Operations

At We Are CORTEX, we enable you to automate any process in your network and operations, based on our reusable components. We'll help you target your efforts on the automation opportunities that deliver the best return, in the least time – giving you the tools to automate your complete network and service portfolio – and the ability to extend to future service propositions and technologies.

We do this by designing workflows based on our composition framework and palette, allowing you to craft processes that meet your needs. We can integrate with any interface – from REST to proprietary APIs, protocols, and legacy solutions. This integration means that we can execute the actions that are required at each step in the automation flow – seamlessly.

Reusability is key for implementing automation across all functions and network layers. Our library of workstations and functional blocks provides the framework to template and create any automation flow.

Any process can be automated from our framework in a simple GUI environment that provides a staging ground and easy deployment to the live network. Each block can be reused in other processes, accelerating your transformation, and providing simple replicability.

Automation extends to lifecycle management and is aligned with your transformation programmes. When you change a platform or solution, it's easy to update our algorithm to extend to new interfaces. Everything is re-deployable, regardless of how your network evolves.

We can also support clients to retrospectively implement automation – for example, for network changes and self-healing routines, with zero failures. It is, however, generally more cost effective if change is implemented from the ground up. Given the complexity of 5G networks and dynamic services and slices, strategic automation from the outset is the only possible way to achieve this, at scale.

We are completely vendor neutral, and our solutions deliver effective automation across all network, OSS and BSS platforms. This extends to the legacy footprint that many CSPs continue to maintain – as well as your future platforms, such as those required for 5G SA – so you can easily integrate with your orchestration and operational platforms to ensure seamless automation as you transform your network.

Six months to autonomy

Key to the transition is to enable self-sufficiency, so you can follow your own roadmap and implement functional automation across your organisation. In just six months, you'll be able to run your own automation programme, based on our kick-start programme. Our goal is to make you self-sufficient, so you can implement automation across your entire operations.

©2023 CORTEX Ltd.



Conclusion:

Efficient, Fast, Successful

Automation has become a key imperative for all CSPs. In addition to the internal (and external) benefits that agile service delivery and real-time autonomous operations will deliver, automation is also essential to meet the challenge posed by new regulations, such as the UK's TSA.

With a strict timetable and stiff penalties in place, automation can no longer be postponed. CSPs must select the right targets for their automation efforts and successfully execute implementation programmes, ensuring they cover all compliance gaps along the way.

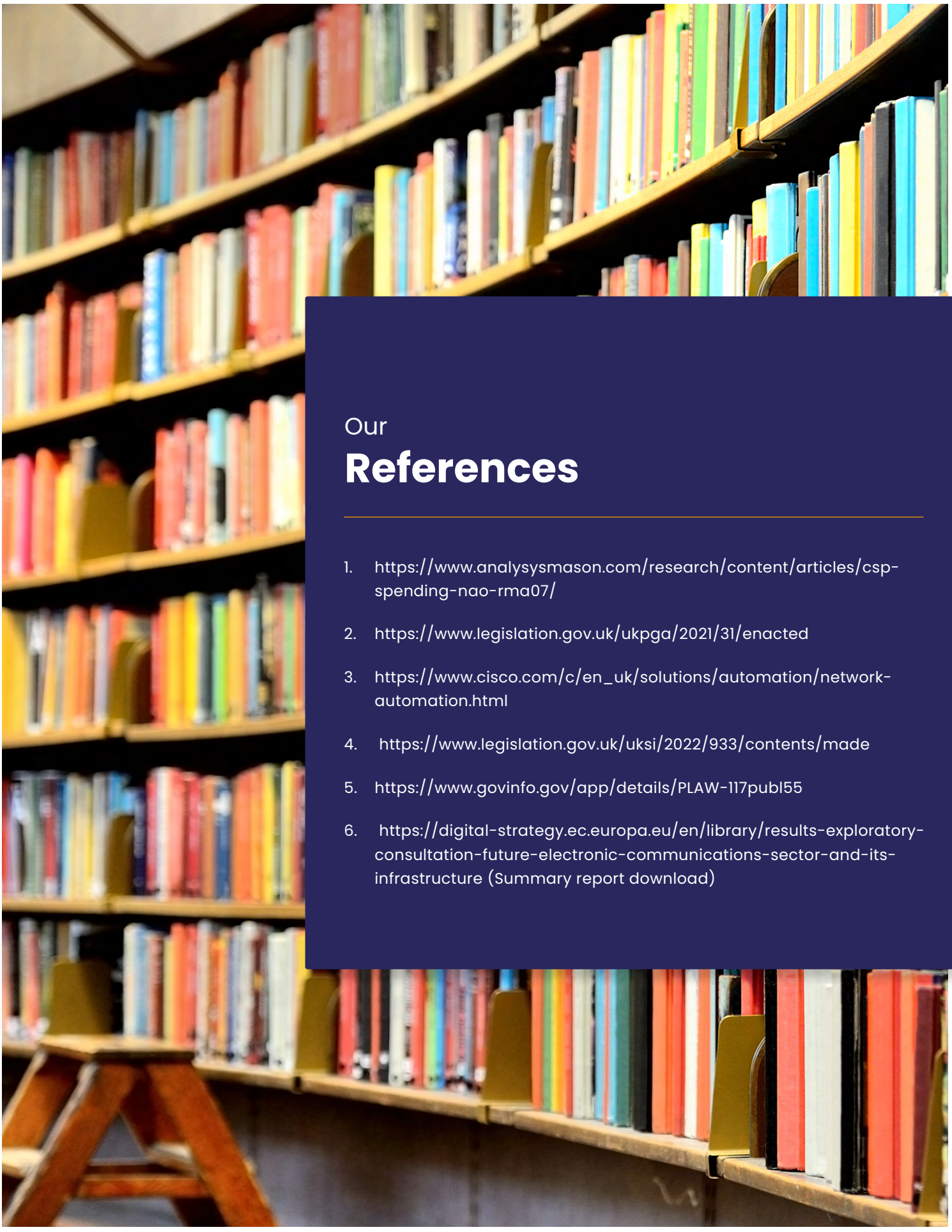
We Are CORTEX offer proven, network-hardened solutions that enable CSPs to navigate automation journeys – and to ensure compliance with regulation that require significant internal transformation, and which are accelerating the transition to fully automated networks and operations.

With We Are CORTEX, you can easily show how you have complied with relevant regulations and legislation – all changes are captured, and strict version and access control is maintained in line with best-practice for IT governance and regulatory compliance. Changes can be tracked to users – with visibility of the complete change history – ensuring that you align with authorised personnel.

Our simple, OPEX-based model means you only pay for what you use, with clear annual licensing costs. We allow you to focus your budgets and resources where they matter - and adapt to skills shortages by making the best use of your teams. Automate with We Are CORTEX and ensure compliance with acts such as the TSA, eliminate operational friction, accelerate service delivery, and enhance network performance.

Efficient, fast, successful.

©2023 CORTEX Ltd.



Our
References

1. https://www.analysysmason.com/research/content/articles/csp-spending-nao-rma07/
2. https://www.legislation.gov.uk/ukpga/2021/31/enacted
3. https://www.cisco.com/c/en_uk/solutions/automation/network-automation.html
4. https://www.legislation.gov.uk/uksi/2022/933/contents/made
5. https://www.govinfo.gov/app/details/PLAW-117publ55
6. https://digital-strategy.ec.europa.eu/en/library/results-exploratory-consultation-future-electronic-communications-sector-and-its-infrastructure (Summary report download)

©2023 CORTEX Ltd.



Get in touch to

Start a conversation today!

Hopefully, we have inspired some new ways of thinking about automation that could benefit your CSP.

Clearly, there is more that could be said, and your CSP will have specific automation requirements. We would be delighted to discuss these in more detail with you and help your automation journey.

Get in touch to start a discussion today!

Thanks for reading.

©2023 CORTEX Ltd.

WE ARE CORTEX

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