Alcatel-Lucent Enterprise Security Assessment Services for regulation compliance

Ensuring the security of network infrastructure is paramount for any organization aiming to protect itself from today's increasingly sophisticated cyber threats and to comply with regulations such as the NIS2 Directive.

These elements of cyber security must be assessed according to regulations and your business needs:

- **Risk assessment**: Must be properly performed by a certified body to catch all cyber security environment risks and vulnerabilities
- **Network topology**: Must be structured so any device can see only the devices associated with its business to avoid allowing attackers to move easily among devices
- **Misconfigurations and outdated software**: Must be addressed to avoid vulnerabilities that attackers can exploit
- **Network access**: Must be tightly controlled so unauthorized entities cannot slip in undetected, posing significant risks
- **Data encryption**: Must be encrypted to safeguard against interception and theft, especially when transmitted across networks
- **Endpoint security**: Must be protected against threats like phishing and ransomware so the laptops and accessories, smartphones and IoT devices that your team uses every day are not open to unauthorized access and widespread malware infections
- **IT and OT integration**: Must be analyzed deeply to avoid issues that may arise from interconnected infrastructures
- **Mitigation plan**: Must be in place as a clear, actionable plan so your team can quickly contain, understand and recover from incidents, minimizing downtime and business impact

By focusing on the critical areas, companies develop a comprehensive cybersecurity strategy that safeguards their organization against various threats while ensuring operational resilience and compliance.

Alcatel-Lucent Enterprise network infrastructure is at the heart of your cyber environment. It must be properly designed, configured and managed to ensure the underlying security of your entire ecosystem.

Focusing on these key areas fortifies your organization against the numerous cyber threats in today's digital world. By remaining proactive and informed, you can maintain a resilient network security posture that protects your organization and its valuable data assets.

ALE Security Assessment Services

Ensuring state-of-the-art security across your network infrastructure is a combination of product features, configurations and best practices that ALE designed and proposes through this service.

The ALE Security Assessment service evaluates your network performance and security. We provide state of the art visibility on configurations and implementations on ALE equipment so you can prepare to apply for a security audit with a certified body to ensure compliance with regulations such as NIS2.

Check your initial situation

Depending on the maturity of your network's security, you may need guidance, information and a defined action plan.

With our preliminary free workshop with an ALE expert or with the preliminary questionnaire on our web portal, we help you understand the effort required for a full network assessment.

You need to secure and optimize your preparations before you submit to a **security audit**. You must be able to **target the right aspects with the best practices and align expectations and obligations** with your own business to benefit from a straightforward path to security compliance.

Get a full assessment on your network

One of our experts analyzes your network topology, configurations, features usage, integrations and potential internal and external vulnerabilities. We identify performance issues, optimization needs and best practices to be applied to comply with your obligations.

Get a report with an improvement plan description

From that analysis, our expert consolidates conclusions, warnings and issues within a **single report**, incorporating recommendations and best practices. We present that report to your teams and make sure you understand your level of exposure and risk.

Run the improvement plan to reach security compliance

The **improvement plan description** is part of the report delivered by our expert. It shows the path to state-of -the-art security configurations and compliance. Steps and activities are recommended and described, which can be delivered by a Business Partner or ALE. Executing the improvement plan, within a dedicated project, ensures you get the true value of our expertise in network performance and security and you comply with regulations.

Revisit your security policy

Performing the improvement plan is essential, but that is not the end of the story. You need to **regularly reassess your security policy** as cyber threats, your business and regulations evolve. ALE will recommend a pace for regular partial and complete reassessments.

Understand your security posture's impact on your business

Get detailed descriptions and clarifications on configuration issues and vulnerabilities from our network topology analysis.

Secure your network to protect your business

Get prepared to align your network with ALE vendor recommendations, state-of-the-art security features, best practices and recommendations.

Ensure regulation compliance and be ready for a cybersecurity audit

Align your network, within a dedicated project, with applicable regulations, and make sure your network topology and configurations meet regulatory requirements.

The contribution of your ALE network infrastructure to your entire cyber security is vital and can consist of the following elements:

- A **robust network infrastructure**
- A **structured architecture** where layers and separations are fully designed, implemented and tested
- A **Zero-Trust policy implementation** where no device connection can happen without a dedicated approval path
- An updated release management and **state-of-the-art configurations**
- An event detection and notifications to administrators
- An integration with a Security Information and Event Management platform (SIEM)
- **Staff training and awareness** programs on network usage and management
- An adherence to industry standards for compliance

For more information, visit our Professional and Managed Services page.

Alcatel·Lucent Enterprise