



Cybersecurity Audits



Cybersecurity Audits is a professional service that evaluates your company's IT systems to ensure compliance with cybersecurity regulations and to pinpoint any existing vulnerabilities.

The goals is to identify risks and recommend improvements that help prevent cyberattacks, malware, and data breaches.



Types of Cybersecurity Audits offered by Cloud2Sec:

- Penetration Testing
- Regulatory Alignment
- Compliance Assessment

PENETRATION TESTING

- These are technical tests designed to analyze vulnerabilities and attempt to breach computer systems.
- Goal: Identify weaknesses caused by outdated software and poor security implementations during the production stages.





- ✓ **Cloud environments:** websites, email services, and customer cloud solutions
- ✓ **Local Environments:** wired and Wi-Fi networks, computers and servers, IoT devices, and peripherals
- ✓ **Hybrid:** both environments working together



REGULATORY COMPLIANCE

- These audits are carried out to ensure security policies meet the requirements of ISO27001:2022, ENS, and the EU-NIS2 directive.
- Purpose: To assess the IT environment and draft the necessary Information Security Policies and Procedures.



Regulatory Compliance

- These audits are conducted to ensure compliance with ISO 27001:2022, ENS, and the EU-NIS2 directive.
- Purpose: Identify any non-compliance issues in the systems reviewed, assess them against the client's procedures, and recommend suitable improvements.



Contact

a.marcotulli@enjoynet.es

<https://enjoynet.es>