

Advanced Active Directory (AD) Auditing and IT Financial Audit Training with Norwegian Experts

Within the framework of the bilateral cooperation agreement with the Office of the Auditor General of Norway, the latest training session with Norwegian experts on IT auditing was held at the Albanian Supreme Audit Institution (ALSAI) from 28 October to 1 November 2024. The main objective of the training was to improve the quality of IT audits at ALSAI, with a particular focus on “Information Security and IT Governance”.

The topics covered during the training are as follow:

Advanced Windows and Active Directory (AD) Auditing:

- Understanding the principles of Windows networks and the Active Directory (AD) Domain System;
- Identifying advanced security risks in the AD Domain System, Windows Servers, and Windows user accounts;
- Using audit software and CIS Benchmarks to audit Windows networks and Active Directory;
- Incorporating audit findings into a comprehensive information security report.

IT Auditing in Financial Systems:

- Understanding the requirements for auditing financial information systems;
 - Practicing financial auditing of ALSAI’s financial systems in accordance with ISSAI 2315.
- The training contributes to enhancing IT audit capacity while also ensuring that ALSAI auditors are equipped with the necessary skills and tools to adapt to the evolving requirements of IT auditing, thereby strengthening the effectiveness and depth of audit practices.



ALSAI’s commitment to developing expertise in Cybersecurity and IT Financial Auditing remains a long-term objective, focused on providing continuous training and improving audit methodologies.

Through the continued cooperation with the Office of the Auditor General of Norway, three additional topics were planned for 2025, which are considered equally relevant to both the institution and its Information Technology auditors.

I. PenTesting of IT Infrastructure.

Pen testing of IT infrastructure is a key process for assessing the security of information technology systems and networks. It aims to identify vulnerabilities and weaknesses that could potentially be exploited by an attacker.

The process involves several key steps:

- Network and vulnerability scanning to identify potential security weaknesses;
- Using automated tools to identify vulnerabilities;
- Exploiting identified vulnerabilities to gain access to systems and simulate a potential attack.

Upon completion of the testing, a detailed report will be prepared to serve as a guide for IT management in addressing identified issues and strengthening security measures. The report will include:

- A description of the identified vulnerabilities;
- The methods used to exploit the vulnerabilities;
- Recommendations for improving security and eliminating vulnerabilities.

Pen testing is an essential component of IT security audits and should be conducted regularly to ensure that IT infrastructure remains protected against potential threats.

II. Phishing Attacks

Phishing is one of the most relevant topics for institutions today, as it concerns not only IT departments but the entire organizational structure. Phishing simulations provide several important benefits for institutions seeking to strengthen their cybersecurity:

- Phishing tests help staff recognize attack tactics and identify suspicious emails. Through training and practical experience, employees become more aware of the risks and learn how to avoid clicking on malicious or suspicious links.
- The tests help identify vulnerabilities and weak points, particularly those related to employees' interaction with email systems and the internet.
- By testing and analyzing staff responses to phishing attacks, institutions can improve their cyber incident response protocols. This is essential to ensure a rapid and effective response in the event of a real attack.
- Awareness and training help reduce the likelihood of a successful phishing attack. The better prepared employees are to recognize and avoid such attacks, the lower the cybersecurity risk to the institution.

III. Auditing Websites and Web Applications

This audit is important for ensuring that online systems are protected against cyber threats and comply with established security standards. The process aims to strengthen the security of websites and web applications, ensuring that users and their data are protected from cyber threats.

The auditors who actively participated in this training used and tested technological tools employed by the Office of the Auditor General of Norway in conducting audits in this area. The participants were: Elira Cukalla, Rodjan Alimerkaj, Klea Saliu, Ardit Alushaj, Anxhela Kostaj, Megi Peza, Arjola Mucaj, Rovenda Deda, and Xhesila Nano.