IstroSec

Data Sheet

Information security audit

Information systems security audit is a key element in the process of ensuring and verifying compliance with security requirements. It is a tool to verify that security measures are adequate, effective, and work as expected. It is also a way to ensure continuous improvement and to adjust the security controls to a dynamically changing environment and security threats.

IstroSec auditors adhere to the following principles:

- Impartiality, independence and objectivity
- Due diligence and professional care
- Confidentiality and non-disclosure
- Risk-based approach
- Professional ethics
- Competence and professional development

Why IstroSec?

Combined experience of more than 70 years

Access to experts in all domains of information security, including penetration testers, forensic analysts, malware analysts, trainers and more

Systematic improvement of information security according to frameworks enriched with the experience of IstroSec experts with advanced security incidents

Ensuring compliance with security standards and legislation - IstroSec experts have been operating in public administration (NIS Directive, GDPR and others) as well as in the private sector (ISO 27001, NIST, HIPAA and others)

> *We perform internal security audits according to many legislative and normative requirements*

- ISO / IEC 27001 and ISO / IEC 27002
- NIST Cybersecurity Framework
- IASME
- 69/2018 Coll. - Cyber Security Act
- Act on Information Technologies in Public Administration
- GDPR
- HIPAA
- FISMA

IstroSec performs external audits according to Act no. 69/2018 Coll. on Cyber Security and on Amendments to Certain Laws. Our certified auditors meet the qualification requirements set by NBU Decree no. 436/2019 Coll. on the audit of cyber security and the auditor’s knowledge standard.

An internal audit from IstroSec will allow you to:

- Prepare for an external or certification audit
- Fulfillment of regulatory obligations and requirements of standards regarding conduct of internal audit
- Identify non-conformities between the current state and security requirements
- Identify opportunities for improvement
- Prioritize security investments

European Cybersecurity Company.
Threat Intelligence. Incident Response. Cyber Advisory.

www.istrosec.com

We follow these steps when performing audits

Planning

- Determining the subject and scope, and identification of audit objectives
- Pre-audit
- Identification of information sources

Audit conduct

- Documentation review
- Interviews with personnel
- Collection and evaluation of evidence

Reporting

- Audit evaluation
- Final report creation
- Presentation of results
- Follow-up and evaluation of corrective actions

We provide these types of audits

Audit of the information security documentation

Examining the adequacy and effectiveness of information security documentation will make it possible to identify gaps in information security management. The security documentation consists mainly of security strategies, policies, guidelines, procedures, manuals, but also of records on the operation of the information security system. In addition to the high-level documentation, we will also review asset management, risk management, information classification schemes, access control and any other security documentation.

Audit of processes

Within the information security system, many processes take place, such as third party risk management or information security incident management process. Our auditors examine how these processes work and assess the extent to which internal and external requirements are met. During interviews with the staff responsible for these processes, the current state will be reviewed. Then, it will be assessed whether these processes are clearly defined, documented and whether all stakeholders know their role. As part of the final audit report, we will also provide recommendations for resolving the identified gaps.

Audit of compliance with a standard

This type of audit aims to examine the extent to which the requirements of security standards and legislation are met. The scope of the audit heavily depends on the standard of reference. As part of the compliance audit, auditors examine internal policies, documented procedures, and various records demonstrating that the security system is operating as intended.

Technical security audit

This type of security audit examines the security configurations of servers, endpoints, network and security devices. The hardening of equipment and the implementation of technical security measures are also examined. As part of audit activities, auditors focus on security logs, firewall rules, encryption, backup and other aspects of the information security.

Why Us?

Experience and knowledge

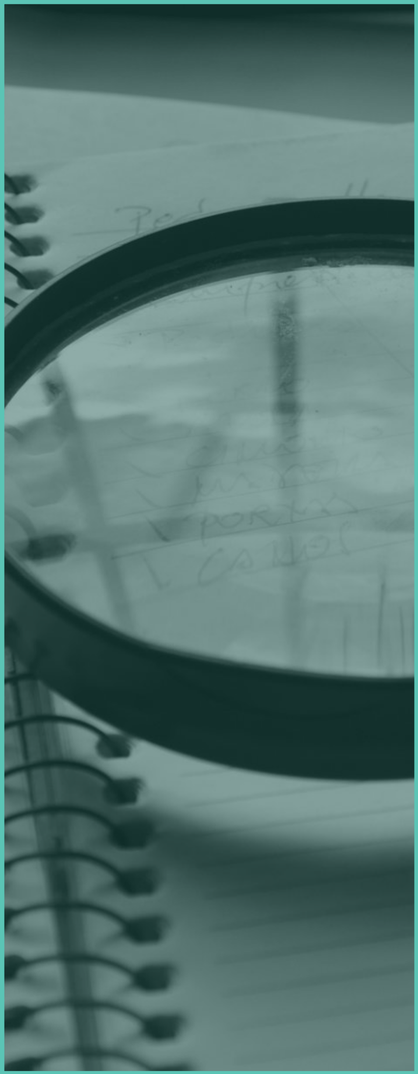
IstroSec specialists have experience in implementing, managing and auditing information security according to most information security frameworks. They know the tactics, techniques and procedures of attackers and have the necessary knowledge to implement information security processes into your business processes effectively and smoothly.

Expertise in audit

IstroSec specialists have expertise in information security auditing, management, and many other areas, such as incident response, forensic analysis, and world-class malware analysis, which they have repeatedly demonstrated while dealing with state sponsored cyber-attacks, attacks on Fortune 500 organizations, as well as the participation of four IstroSec experts in the winning team of LockedShields 2016 exercise.

Certified professionals

IstroSec experts are also holders of internationally recognized certificates in these areas. We hold certificates such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) and more.



Case Studies

Company type: Logistics services provider

Service provided: Information security audit

Solution: Internal audit of compliance with the ISO 27001 standard

The company providing logistics and shipping services needed to perform an internal audit of the information security management system. The company recently implemented the ISO 27001 standard, and it was necessary to demonstrate that it has an independent and effective internal audit function. As the company did not have an internal auditor, the company decided to outsource this function. Therefore, an internal methodology for conducting audits was developed and an audit program for the next three years was designed. Subsequently, the first iteration of the internal audit in accordance with ISO 27001 commenced. The internal documentation was reviewed, employees were interviewed, evidence was collected and analyzed, and the findings were subsequently evaluated. The audit findings, together with the recommendations, were summarized in the final audit report. Several discrepancies with the standard and several opportunities for improvement were identified.

Company type: Software development company

Service provided: Information security audit

Solution: Technical security audit

The software development company needed to verify the effectiveness of its network security features and their compliance with current security standards. Therefore, a comprehensive technical audit of the configuration of firewalls, intrusion prevention systems (IPS), web application firewalls and proxy servers was performed. Firewall rules, logging, patch management and hardening of network and security devices were examined. The final report contained a prioritized list of findings together with recommendations for their mitigation.