IstroSec

Data Sheet

Implementation of Information Security Processes

Information security management specialists from **IstroSec** have many years of experience in information security management both in public administration and in the private sector. From our experience, we know that information security requirements across the different types of organizations vary. Therefore, there is no one-size-fits-all solution to adequately meet all these requirements at a reasonable cost, given the value of the assets.

Our approach toward implementing information security

- Alignment of information security objectives with business objectives and their support
- Risk-based implementation of security controls
- Individual approach
- Leveraging experience with many advanced security incidents during the implementation of security controls

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 are ready to implement information security management processes in accordance with many regulatory 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

Implementation Process

- Identification of all security requirements
- Determining the scope of implementation
- Assessment of existing security measures
- Risk assessment
- Creating an implementation plan
- Implementation of security measures and processes
- Measurement, monitoring, review, and continuous improvement
- Preparation for certification

Why Us?

Experience and knowledge

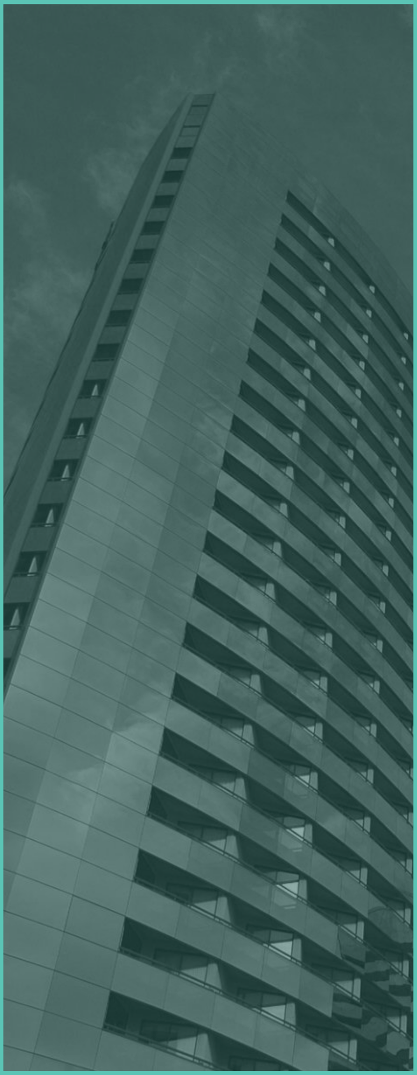
IstroSec specialists have experience in implementing and managing information security according to most information security frameworks. They know the tactics, techniques and procedures of attackers and have the necessary knowledge to implement information security processes into your business processes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

Expertise in management

IstroSec specialists have expertise in information security 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: Medium-sized software development company

Service provided: Implementation of information security management processes

Solution: Implementation of risk management process

Economic software development company needed to implement risk management processes to periodically assess their risks. As the company recently kickstarted their ISO 27001 implementation, they needed to demonstrate their ability to discover, understand and mitigate their information security risks. Therefore, a risk management methodology based on ISO 27005 was developed. After that, the first iteration of risk assessments begun. The list of assets was developed where information assets were identified and valuated. Then, the vulnerabilities and threats relevant to these assets were identified. Information security risks were calculated and those above the acceptable risk threshold were mitigated.

Company type: Essential service provider in telecom sector

Service provided: Implementation of information security management processes

Solution: Gap assessment and implementation of incident management process

Essential service provider according to Slovak Cybersecurity Act needed to fulfill its regulatory obligation to implement processes for cybersecurity incident detection, acquisition and preservation of digital evidence, incident resolution and reporting. Initially, an incident preparedness assessment was performed that uncovered gaps in people, processes and technology needed for incident management. After that, incident response plan and playbooks were designed and implemented. These were then tested by conducting tabletop exercise that further strengthened and validated these processes.