

# Security Audit



When knowledge of current situation is significant to your decisions...

**Security audit** focuses on and examines current situation of the implementation and configuration of the countermeasures in selected security areas: technological (ICT), physical, personnel and administrative. Identified reality of the countermeasures is compared with selected internal or external criteria, which are acting as the required state.

**Main goals** cover evaluation of the countermeasures' current states and compliance level with the required state based on selected criteria of information security, identification of nonconformities with required state, their documentation and summary.

**Criteria of security audits** can be internal security documentation of the organization (policy, directives and procedures), national/EU legislation, selected external standards, security guidelines, best practices or recommendations of authorities.

## We offer security audits of ICT infrastructure, applications and services, security procedures and management systems (ISMS)

### Security audit of selected areas and procedures of information security

These audits focus on implemented countermeasures of selected security areas (technological, physical, personnel or administrative) within specified scope of the audit (systems, services, applications or complex IS).

#### Technical security audit of selected ICT and its countermeasures (HW, SW, DB, FW, PKI...)

**Goals:** to identify gaps and nonconformities in the application of required countermeasures within selected ICT infrastructure of IS.

**Deliverables:** security check of the design, implementation, operation or configuration of selected scope of ICT infrastructure.

#### Security audit of selected procedures and its countermeasures (Development, BCM, IRH...)

**Goals:** to examine selected procedures in the design, management and operation of IS and identify gaps and nonconformities against selected "Best-practices".

**Deliverables:** security check of application and adherence to defined and required rules, procedures, and responsibilities within scope of organization.

### Complex security audit of the whole IS / ISMS

These audits focus on the complex information security state within the whole organization and its compliance with ISO/IEC 27001:2005 and ISO/IEC 17799:2005 standards for information security management.

#### Complete ISMS audit against ISO 27001:2005 and ISO 27002:2005 (certification by DNV)

**Goals:** complex audit of security management procedures and countermeasures and compliance with requirements of ISO standards for ISMS.

**Deliverables:** to lead the organization through an ISMS pre-certification audit for evaluation of compliance and maturity level of implemented ISMS.

#### Initial ISMS compliance review against ISO 27001:2005 (RAC ISMS C-Audit)

**Goals:** quick basic review of current main security and management procedures and their compliance with key requirements of ISO 27001:2005.

**Deliverables:** efficient information about the current state of information security for initial PLAN phase or for brief review under CHECK phase of ISMS.

### Special types of information security audits

These audits focus on compliance of information security state with selected national / EU legislation and guidelines (personal data protection, classified data protection) or with security standards like BASEL II, ITIL...

#### Information security audit of compliance with BASEL II principles for operation risks

**Goals:** to review current state of IS-operation risk procedures and its compliance with BASEL II.

**Deliverables:** overall review of compliance level with BASEL II principles for operating risks including recommendation for improvement.

#### Audit of personal data or classified data protection against national / EU legislation

**Goals:** to review current state of information security against personal/classified data protection legislation.

**Deliverables:** overall review of compliance level with personal/classified data protection legislation, including recommendation for improvement.