

Security Analysis



When impression is not enough and knowledge of the reality is essential...

Security analysis breaks down an analyzed object to its basic elements and focuses on assessment of their internal vulnerabilities, external threats and implemented countermeasures of the analyzed object in selected areas of information security: technological (ICT), physical, personnel and administrative.

Main goals cover identification of existing vulnerabilities and potential threats affecting analyzed object, assessment of risks and possible negative impacts to analyzed object and related infrastructure or organization and recommendation of countermeasures for risk elimination or reduction to an acceptable level.

Objects of security analysis include either dedicated computer systems or LAN/WAN infrastructure, subsystems or complex IS, its data, applications and services.

We offer various types of security analyses of the IS and ICT according to the customer's requirements, using international methodologies and standards

Analyses for security planning purposes:

During planning or improving of information security, analysis should focus on complex risk assessment in all parameters of information security: confidentiality, integrity and availability. Appropriate risk treatment plan should be established with selection of countermeasures for reduction of risk to an acceptable level.

Initial/Basic risk analysis (CRAMM Express)

Goals: quick risk assessment of the most important vulnerabilities and threats on selected sample data asset, representing the whole IS.

Deliverables: base input for decision and preparation of detailed risk assessment (very fast and efficient).

Detailed risk assessment (CRAMM Expert)

Goals: complex risk analysis and evaluation on detailed asset break down of analyzed IS scope; selection of countermeasures, review of their current state and recommendation for risk elimination.

Deliverables: basic part of initial PLAN phase of every security project, including implementation of ISMS (Information Security Management System).

Business impact analysis (BIA)

Goals: to identify potential negative business impacts in case of critical asset unavailability in various time frames and disaster conditions; to recommend effective preventive countermeasures - BCM process.

Deliverables: specification of availability requirements and selection of optimal BCM (Business Continuity Management) for DRP (Disaster Recovery Planning).

Analyses for security operation purposes:

During operating, monitoring and checking of the state of information security, analyses should focus on functionality and failures of selected countermeasures (controls) or on investigation of security incidents and breaches of security controls in various areas like technological, physical, personnel or administrative security.

Technical security analysis (RAC ISSEC)

Goals: to identify and evaluate vulnerabilities in design, implementation or configuration of ICT systems/services and to recommend countermeasures.

Deliverables: evaluation of security effectiveness in design, implementation or operation of ICT systems.

GAP analysis (RAC Questor + Q-Module)

Goals: to identify gaps of current information security state against selected international standards (e.g. ISO/IEC 27002:2005, ISO/IEC 27001:2005, BASEL II, ...) and to recommend missing controls.

Deliverables: base input for selection and implementation of missing controls of selected security standard for compliance or certification audit.

Computer forensic analysis (CFI)

Goals: to identify and document cause and history of the security incidents analyzing ICT systems and services; to document range of impact of incidents for collection of evidence for investigation.

Deliverables: expert forensic analysis and investigation of security incidents and crime caused using information technology and services.