

Overview Risk Analysis (CRAMM Express)

Goals: an instant risk assessment of the most important threats and vulnerabilities on selected sample of data asset, representing the whole Information System.

Benefits: in very fast and effective way obtaining significant information for decision and preparation of Detailed Risk Assessment.

Detailed Risk Assessment (CRAMM Expert)

Goals: a comprehensive risk analysis and evaluation on detailed assets by breaking down the analyzed IS scope; selection of countermeasures, review of their current status and recommendations for risk elimination.

Benefits: the first part of the initial PLAN phase of every security project which includes implementation of ISMS (Information Security Management System).

Business Impact Analysis (BIA)

Goals: to identify potential business impacts in case of critical assets unavailability in various time frames and disaster conditions as well as to recommend effective preventive countermeasures.

Benefits: specification of Business Continuity Management (BCM) requirements and selection of the optimal Strategies for BCM and Disaster Recovery Planning (DRP).

Vulnerability Analysis

Goals: to identify and evaluate vulnerability of systems and applications, security of internal and external equipments or to conduct penetration testing.

Benefits: the part of the vulnerability management process and security supervision; the significant information from an internal and external penetration testing.

Technical Security Analysis (RAC ISSEC)

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

Benefits: the evaluation of effectiveness of design, implementation or operations of ICT systems; the specification of risk analysis or penetration testing results.

GAP analysis

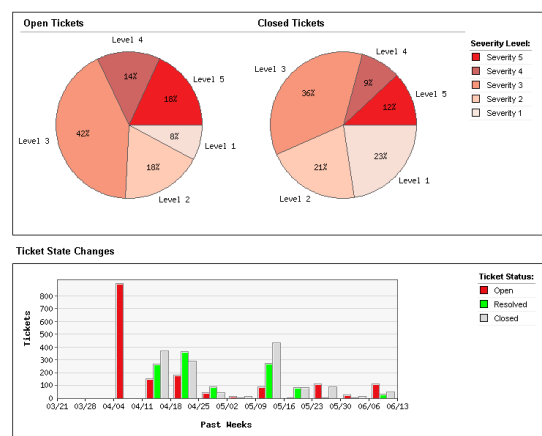
Goals: to identify gaps of the current information security status against the selected international standards (e.g. ISO/IEC 27001:2005, ISO/IEC 27002:2005, BASEL II,) and to recommend required controls.

Benefits: the significant information for selection and implementation of controls according to the given security standard for compliance or certification audit.

Digital Forensic Analysis (RAC CFI)

Goals: to identify and document causes and history of the security incidents, to analyze the course of security incidents as well as to document range of the impact of incidents for collection of evidence for investigation.

Benefits: digital forensic analysis and investigation of security incidents and crime caused by using information technology and services.



Risk Analysis Consultants, s. r.o.
Španělská 2
120 00 Prague 2
Czech Republic
+420 221 628 400
rac@rac.cz
www.rac.cz

Risk Analysis Consultants is a Czech based professional provider of information security services and solutions. We have assisted organizations from government and commercial sectors in protecting their information since 1995. We are the only firm exclusively specialized in the information security field in the Czech market, and one of the few in Europe as well as the world.



QR code RAC