

SECURITY AUDIT



Making the right decisions means to know reality

Security audit examines and identifies actual state of processes and countermeasures in designated security areas (organizational, administrative, personnel, physical, information and communication systems) and compares it with the determined audit criteria.

Main goals of security audit cover evaluation of the current status of processes and controls as well as compliance level against the required status based on selected criteria of security, identification of nonconformities, their documentation, proposal of recommendations and indications of potential security risks.

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

„ We offer security audits of systems, services, applications, ICT infrastructure and all areas of security controls of information systems as well as audits of organization’s information security or business continuity management systems.”

„We above all conduct security audits in compliance with international standards, internal organization’s documentation and with the best practices.”

Six steps of audit



Audits of information security status

These audits are focused on evaluating current organization’s information security status and its compliance with the requirements of **ISO/IEC 27001:2005 and ISO/IEC 27002:2005** standards for Information Security Management System (**ISMS**) within organizations.

Comprehensive security audit according to ISO/IEC 27001:2005 and ISO/IEC 27002:2005

Goals: an independent evaluation of the current organization’s information security status against the requirements of standards for information security management.

Benefits: the assurance that information security within the organization is managed and improved; competitive advantage and guaranties for partners and clients. Audit can be preparation for obtaining or maintaining ISMS certificate.

ISMS Compliance audit

Goals: an instant overview of the current organization’s information security status from the perspective of the ISMS implementation and operation according to the ISO/IEC 27001:2005 requirements.

Benefits: the significant information for establishing, implementing or developing ISMS; tool and methodology for continuous check of the ISMS status within an organization and its maintenance and improvement.

SECURITY AUDIT

Audits of business continuity status

These audits are focused on evaluating current organization's business continuity status and its compliance with the requirements of **BS 25999-1:2006** and **BS 25999-2:2007** standards for Business Continuity Management System (**BCMS**) within organizations.

Comprehensive audit according to BS 25999

Goals: an independent evaluation of the current organization's business continuity status against the requirements of standards for business continuity management.

Benefits: the assurance that business continuity within the organization is managed and improved; competitive advantage and guarantees for partners and clients. Audit can be preparation for obtaining or maintaining BCMS certificate.

Overview audit of BCMS

Goals: an instant overview of the current organization's information security status from the perspective of the BCMS implementation and operation according to the BS 25999-2:2007 requirements.

Benefits: the significant information for establishing, implementing or developing BCMS; tool and methodology for continuous check of BCMS status within organization and its maintenance and improvement.

Special types of information security audits

These audits are focused on compliance of organization's information security status with selected national or EU legislation (e.g. Act on the Protection of Personal Data, Act on the Protection of Classified Information) and guidelines or with other security standards (BASEL II, ITIL, COBIT, ISM3, ..).

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

Goals: an independent review of the current status of information systems operation risks procedures and its compliance with the BASEL II requirements.

Benefits: an overall review of the compliance level with the BASEL II principles for operating risks including recommendations for improvement.

Audit of Information and Data Protection according to legal, regulatory or organization's requirements

Goals: evaluating organization's compliance in areas like protection of personal data or classified information with the requirements of legislation.

Benefits: an overall review of compliance with the requirements of information and data protection.

Audits of Information Systems Security

These audits are focused on the compliance of security of organization's information systems or their parts in selected security areas (organizational, administrative, personnel, physical, information and communication systems) with required criteria (standards, best practices, organization's policies and guidances, ..). The goal of audits is to assess whether the information systems adequately protect the organization's assets, ensure data integrity and provide reliable and relevant information.



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