

RAC ISSEC



INFORMATION SYSTEM SECURITY EXAMINATION CYCLE

RAC ISSEC is a methodology developed by RAC that offers practical and interconnected Information System (IS) security examinations during every phase of the IS lifecycle, directly at the customer's site and on their systems, including Internet penetration testing.

RAC ISSEC focuses on IT technologies, examining the security of their implementations and operations as well as all other security layers: physical, personal, administrative and organizational (ISMS).

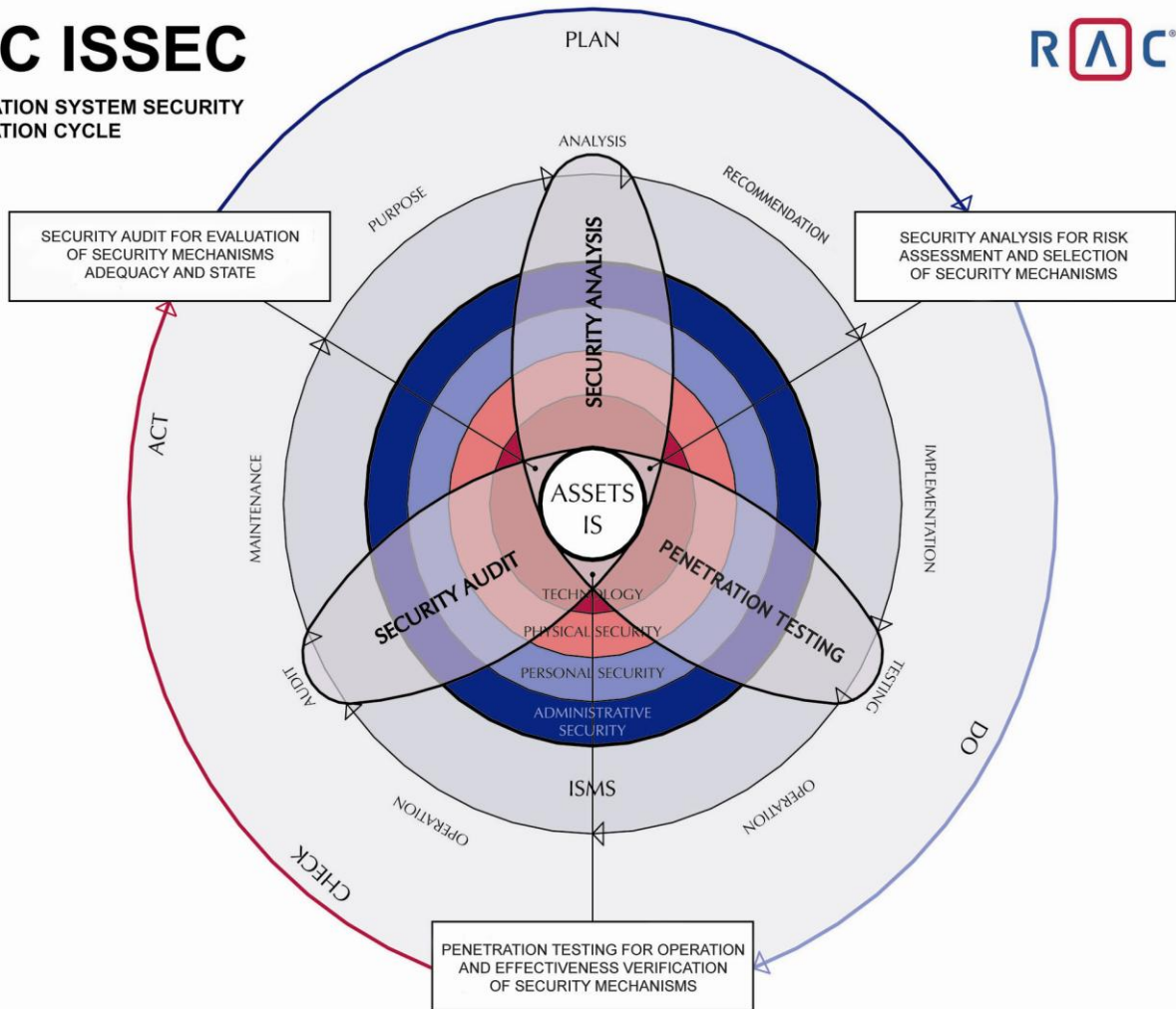
RAC ISSEC is designed in compliance with the ISO/IEC 27002:2005 and ISO/IEC 27001:2005 standards. It is used as a diagnostic tool and supportive process for IS risk analysis, selection of controls and implementations, security testing and audits as well as its use as a practical part of the ISMS implementation and operation within the organizations.

RAC ISSEC

Each type of the security examination has its purpose, advantages and limitations. A compact picture about object under examination from different sights and comprehensive data for decision making can be obtained only by combination of these examinations in right scope, order and general interpretation.

RAC ISSEC

INFORMATION SYSTEM SECURITY EXAMINATION CYCLE



(C) 2003, Risk Analysis Consultants, All Rights Reserved

SECURITY IS A CONTINUOUS PROCESS

Security analysis

Assesses the vulnerabilities, threats and risks in the selected security layers, and designs the required security controls.

Security audit

Compares the current security status with a set of standards and examines their level of compliance.

Penetration testing

Simulates real-world attacks, detects vulnerabilities and tests the functionality of the security mechanisms.

Benefits for clients

Maximum respect of the clients' needs, objectives, and environment. Objects under examination are assessed from the different standpoints due to using individually set up combination of analyses, testing, and audit. The vulnerabilities and potential threats, current arrangements, their effectiveness, resilience as well as conformity with requirements and recommendations are examined. An integration of results obtained this way ensures above standard level of conclusions and especially quality of proposals on improvement of security sensitive systems and data.

An example of basic types of RAC ISSEC examinations:

Feature examinations	Security Analysis	Penetration Testing	Security Audit
Purpose	Look up and identify a maximum of existing vulnerabilities and potential threats as well as suggesting optimal and effective countermeasures.	Test functionality of current countermeasures and their resilience against possible attacks from outer / inner environments. Identify available and exploitable vulnerabilities over current countermeasures.	Identify current status of security countermeasures, examining their conformity with required / defined status, and eventually compare with the recommendations of standards.
Limitation	Not suitable for simulation and testing resilience against attacks on systems. Do not examine conformity with internal needs, external recommendations or standards.	It is impossible to identify all existing vulnerabilities, because they are protected by current countermeasures, which are being changed in time. Do not examine conformity with internal needs, external recommendations or standards.	Do not examine vulnerabilities and threats of critical systems nor resilience of security countermeasures against attacks.
Input conditions	Objects under examination accessible locally and remotely from internal network segments with switched off IDS systems, firewalls, etc.	Objects under examination testing remotely over the Internet, eventually from internal LAN/WAN segments with operational IDS and protective systems.	Generally local access to installations, documentations and settings of security countermeasures as well as internal security documentations and legislations defining desired security status.
Outputs	Detailed report of found and identified vulnerabilities and threats, proposal as well as recommendations for countermeasures.	Protocol on the penetration testing process with listing of found and available vulnerabilities as well as recommended countermeasures.	Report on the audit results containing documented current status, degree of conformity with required security status.



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 and as well as the world.



QR code RAC