

RAC ISSEC



INFORMATION SYSTEM SECURITY EXAMINATION CYCLE

RAC ISSEC je metodika vyvinutá společností RAC za účelem nabídky praktického a provázaného bezpečnostního zkoumání IS, ve všech fázích jeho životního cyklu, přímo v prostorách a na zařízeních zákazníků, včetně penetračního testování přes Internet.

RAC ISSEC se primárně zaměřuje na IT technologie, ale zkoumá bezpečnost jejich implementace a provozu i ve všech ostatních vrstvách bezpečnosti: fyzické, personální, administrativní a zejména organizační (ISMS).

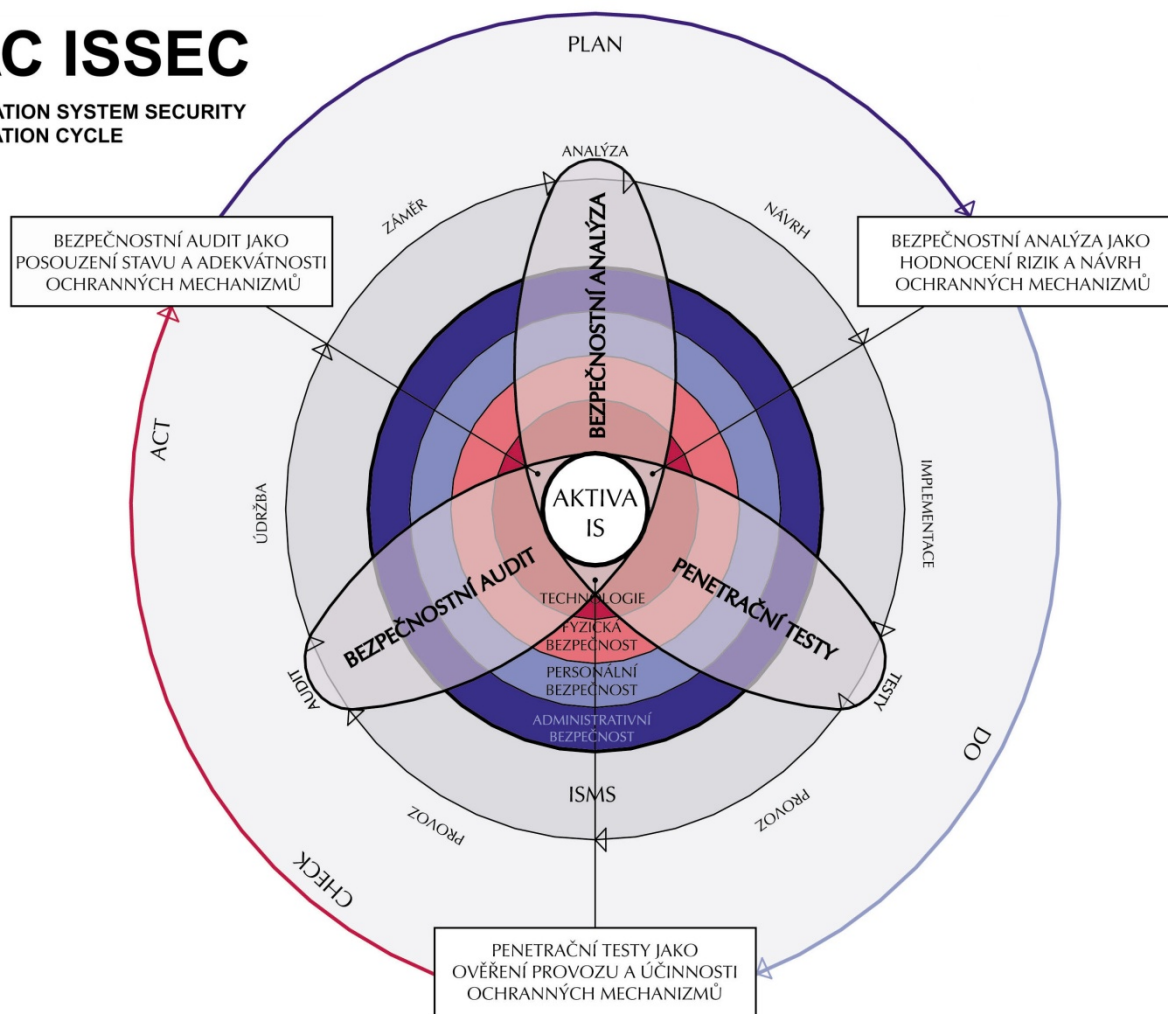
RAC ISSEC je navržena v souladu se standardy ISO/IEC 27002:2005 a ISO/IEC 27001:2005 a slouží jako diagnostický a podpůrný proces pro provádění analýz rizik IS, výběr a implementaci ochranných opatření, bezpečnostní auditu a slouží jako praktická součást a podpora pro zavedení a provoz ISMS v organizacích.

RAC ISSEC

Každý typ bezpečnostního zkoumání má svůj účel, přednosti a omezení. Pouze kombinací těchto zkoumání ve správném rozsahu a posloupnosti a souhrnné interpretaci získáme ucelený obraz o zkoumaném objektu z různých pohledů a vypovídající, komplexní podklady pro rozhodování.

RAC ISSEC

INFORMATION SYSTEM SECURITY EXAMINATION CYCLE



Bezpečnostní analýza

Zkoumá zranitelnosti, hrozby a rizika ve zvolených vrstvách bezpečnosti a navrhuje potřebná protiopatření.

Bezpečnostní audit

Porovnává aktuální stav bezpečnosti s požadovaným a definovaným stavem a zjišťuje míru dosažené shody.

Penetrační testování

Simuluje reálné útoky, detekuje zranitelnosti a proěřuje funkčnost bezpečnostních mechanismů.

Přínos zákazníkům

Maximálním respektování jejich potřeb, cílů a prostředí. Vzhledem k použití individuálně sestavené kombinace analýzy, testování a auditu jsou zkoumané objekty podrobně posuzovány z různých hledisek. Zkoumají se zranitelnosti a potencionální hrozby, stávající opatření, jejich účinnost, odolnost a soulad s požadavky a doporučeními.

Integrace takto získaných výsledků zaručuje nadstandardní úroveň závěrů a především kvalitu návrhů na zlepšení zabezpečení citlivých systémů a dat.

Příklad základních typů zkoumání RAC ISSEC:

Vlastnosti zkoumání	Bezpečnostní ANALÝZA	Penetrační TESTOVÁNÍ	Bezpečnostní AUDIT
Účel použití	Vyhledat a identifikovat maximum existujících zranitelností a potencionálně možných hrozeb a navrhnout optimální a efektivní protiopatření.	Otestovat funkčnost stávajících protiopatření a jejich odolnost proti možným typům útoků z vnějšího / vnitřního prostředí. Identifikace dostupných a využitelných zranitelností přes stávající opatření.	Identifikovat reálný stav ochranných opatření, ověřit jejich soulad s požadovaným / definovaným stavem, případně porovnat s doporučením externích vzorů.
Omezení použití	Nevhodné pro simulaci a testování odolnosti vůči útokům na systém. Nezkoumá soulad vůči interním požadavkům ani externím doporučením a vzorům.	Nelze identifikovat veškeré existující zranitelnosti, protože jsou chráněny stávajícími opatřeními, která se mění v čase. Nezkoumá soulad vůči interním požadavkům ani externím doporučením a vzorům.	Nezkoumá zranitelnosti a hrozby citlivých systémů, ani odolnost ochranných opatření proti útokům, ale zkoumá aktuální stav těchto ochrann. opatření z hlediska souladu s požadavky, doporučeními a vzory.
Potřebné vstupní podmínky	Zkoumaný objekt přístupný lokálně i vzdáleně z interního segmentu sítě s vypnutými IDS systémy, firewally apod.	Zkoumaný objekt testovaný vzdáleně přes Internet, případně z interních LAN/WAN segmentů s funkčními IDS a ochrannými systémy.	Zpravidla lokální přístup k instalaci, dokumentaci a nastavení technologických ochranných opatření, k interní bezpečnostní dokumentaci a především k interní legislativě, definující požadovaný stav bezpečnostních mechanismů.
Poskytované výstupy	Podrobný výpis nalezených a identifikovaných zranitelností a hrozeb, návrh optimálních protiopatření, a doporučení pro změnu stávajících.	Protokol o průběhu penetračního testování s výpisem nalezených, dostupných zranitelností a doporučených protiopatření.	Zpráva o výsledcích auditu obsahující zdokumentovaný aktuální stav, míru souladu s požadovaným nebo vzorovým doporučeným stavem.



Risk Analysis Consultants, s. r.o.
 Španělská 2
 120 00 Praha 2
 Česká republika
 +420 221 628 400
 rac@rac.cz
 www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.



QR kód RAC