



Information Security, Compliance Assurance & Risk Management

WHY PENETRATION TESTING ?

Organizations planning for a penetration test have to juggle many competing priorities. They are struggling to become compliant, and stay compliant, with any number of security standards or regulatory targets. Budgetary pressures are ever-present, and organizations need to ensure that penetration tests are performed by a reputable firm, with expert assessors. As a premier security practice, nGuard has helped an extensive portfolio of clients address these challenges.



VULNERABILITY ASSESSMENTS

TASKFORCE RED can assess the overall security of your organization's systems and provide a valuable baseline for determining appropriate safeguards. Periodic assessments are a requirement of many compliance initiatives and verify that new system implementations and changes to existing systems have not introduced new, unmitigated vulnerabilities to the organization. We use a layered approach to security testing, map results to IT controls to identify root causes, remove false positives and, best of all, provide a prioritized remediation road-map based on inter-dependencies and impacts of the findings. In doing so, our clients benefit from highly-effective, yet cost-effective implementation strategies.

RISK ASSESSMENTS:

A risk assessment is a process by which to determine what information resources exist that require protection, and to understand and document potential risks from threats that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets.

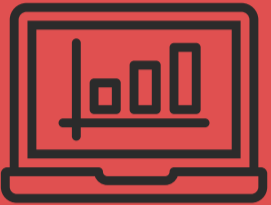


VIRTUAL CISO (VCISO):

When you engage with TASKFORCE RED vCISO services, you gain access to a team of thought leaders in information security compliance, regulations and governance, who will assist in developing, managing and supporting your institution's information security program. Our consultants not only hold advanced security, management and technical certifications, but have successfully assisted hundreds of organizations, (from startups to multi-billion international entities), enhance their information security programs and attain higher levels of assurance and compliance. Only TASKFORCE RED can deliver the professionalism, business acumen and the years of experience that provide the most value to your institution.



Information Security, Compliance Assurance & Risk Management



PENETRATION TESTING & WEB APPLICATION TESTING:

A penetration test, occasionally pentest, is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access). The process

involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Penetration testing of the network perimeter is performed in accordance with an agreed upon Rules of Engagement (ROE) document. Unless requested by client, TASKFORCE RED does not perform denial of service attacks; however, potential denial of service conditions will be identified and actionable findings and recommendations will be delivered in a concise report format.

Web application security reviews are comprised of both comprehensive automated analysis and targeted manual testing techniques. Our testing methodology ensures the uniform detection of common vulnerabilities such as input injection, improper session management, information disclosure and other categories mentioned within the current OWASP Top Ten vulnerability rankings and beyond. All of our deliverables include detailed descriptions, proof-of-concept demonstrations and the perceived risk and remediation effort necessary to successfully address discovered vulnerabilities.

SOCIAL ENGINEERING TESTING:

TASKFORCE RED consultants can help assess the effectiveness of your security awareness training program by attempting to gain access to an organization's systems

through non-technical means. Social engineering is a critical component of an information security assessment as it helps to identify areas of weakness in an organization that can not be addressed through technical solutions such as firewalls and intrusion prevention systems. Our project management approach to social engineering testing ensures our clients benefit from realistic scenarios that closely match the threats to their industry. Furthermore, we provide qualitative results and map the results to internal controls.



PHYSICAL SECURITY TESTING:

The integration of physical security and information security can no longer be overlooked. Not only is physical security a requirement of most compliance initiatives,

it is a requirement of a truly complete information security protection plan. TASKFORCE RED physical security assessment provides this integration by validating existing physical security access controls, providing recommendations for methods to improve integration between physical and information security, and implementing the recommendations.



Information Security, Compliance Assurance & Risk Management



INFORMATION SECURITY POLICY, STANDARD AND PROCEDURES DEVELOPMENT:

Our consultants will help develop a comprehensive set of written information security and data privacy policies that address the specific business and compliance requirements of your company. TASKFORCE RED experts are constantly monitoring

changes in compliance and regulatory requirements, new legislation, and changes in security best practices and can help you maintain the existing policies and procedures to ensure compliance.

INFORMATION SECURITY AWARENESS TRAINING:

awareness and training program that reduces risk and satisfies legal and regulatory requirements. We can work remotely with in-house staff, or deliver hands-on classroom training at your facility.

TASKFORCE RED consultants can help your organization design, develop and deliver an information security



TASKFORCE RED provides the most complete set of penetration testing services available in the industry. With unique assessment services available, our team of credentialed security experts can address penetration testing needs including internet, wireless, database, physical penetration testing, and more.

CALL US NOW

(877) 49-SECURE