

DoIT Service Catalog

Service: IT Security Assessments.

General information: IT Security Assessments consist of three types, Risk, Vulnerability and Physical. Normally they are done in sequence in order to better assist agency in understanding their IT Security concerns.

Purpose: Protection of the IT assets requires periodic testing and review by a third party. The Office of Information Security (OIS) can provide a resource to perform this service.

Scope: The Information Security Assessment Team is composed of five (5) computer security professionals. These individuals are trained in various security domains to cover the wide range of required assessment skills. The Risk Assessment reviews the internal controls that are in place. The Vulnerability assessment verifies the strength and depth of technical security measures in place. The Physical Security Assessment reviews basic physical security and environmental controls.

Features: Security controls covered in all three types of assessments include review of internal PSP's, interviews with employees, on site visit for testing and evaluation of information systems, servers, network connectivity, wireless connections, and a final report provided to the agency management..

Usage: Services are provided to all state agencies and can be accessed Monday through Friday between the operational hours of 7:00AM to 6:00PM.

Value Proposition: Services provided by DoIT's Office of Information Security are assessed into each agency's budget therefore; there are no additional charges involved. In most organizations the IT staff has the responsibility to ensure the continued operating of the agency's business. Some agencies do not have the staff to conduct periodic reviews of existing security controls OIS can provide this service as a disinterested third party in testing procedures or plans with out knowing what the resulting outcome is suppose to look like, thus providing an more realistic appraisal of the situation.

Future Plans: OIS is increasing the coordination with state agencies to offer assessment services to provide a baseline report identifying the current security posture of an agency and recommendations to reduce the risks of identified vulnerabilities and weaknesses of their existing information security controls.

Options and Features		
Options /Choices	Cost	Notes
Security Risk Assessment	No charge beyond the assessment paid to DoIT	The agencies' internal IT data controls and procedures will be compiled read and reviewed. All business functions must be considered as they relate to the IT infrastructure, data storage, data transport as well as the sensitivity of the data (Classification). These policies/controls will be compared to IT best practices and accepted system standards
Technical Vulnerability Assessment	No charge beyond the assessment paid to DoIT	A technical vulnerability assessment encompasses a variety of different areas. Generally anything that contains, or transport data, requires a vulnerability test. A vulnerability assessment is typically conducted after a "Risk Assessment" is completed. When conducting a vulnerability assessment, minor penetration testing will be conducted to better help in discovering flaws inherent in the system. The depth of the vulnerability test is dependent on the classification and the legal requirements of the data
Physical Security Assessment	No charge beyond the assessment paid to DoIT	A physical security assessment encompasses a variety of different areas. Generally system that contains, or transports data requires a physical security assessment and typically is conducted after a Risk and Vulnerability is completed. The depth of the physical security assessment is dependent on the classification and the legal requirements of the data. Physical security assessments include five main categories, structure and perimeter, access control and CCTV, Power, HVAC/environmental controls, supporting utilities, and Life safety

Access: Services can be requested though a letter to the administrator of the Department of Information Technology.