CALIAN™
Confidence. Engineered.

Cybersecurity Assessments

Using industry security standards and regulations to assess an organization's controls and maturity.

INDUSTRY ASSESSMENTS

ENTERPRISE RISK ASSESSMENT (ERA)

VULNERABILITY ASSESSMENTS & PENETRATION TESTING

TECHNICAL ASSESSMENTS

Industry Assessments

The Payment Card Industry Data Security Standard (PCI-DSS)

A set of security standards formed by Visa, MasterCard, Discover Financial Services, JCB International, and American Express.

Personal Health Information Protection Act (PHIPA)

In addition to regulating custodians of health information, it also regulates individuals who receive health information from them.

Personal Information Protection and Electronic Documents Act (PIPEDA)

An individual's right to control how their personal information is handled in the private sector is protected by these principles.

General Data Protection Regulation (GDPR)

Using appropriate technical and organizational measures is required by the GDPR for the secure processing of personal data.

Enterprise Risk Assessment (ERA)

Review an organization’s security posture from top to bottom including security operational controls, policies and procedures and map to industry leading standards such as NIST and ISO27001. ERA deliverables include:

- Maturity score mapping
- Identifcation of organizational security gaps
- Propose a high-level transition plan with priorities to move from the current state to the “ideal” to-be state
- Provide a multi-year roadmap for successful completion of projects.

Vulnerability Assessments & Penetration Testing

Our award-winning testing process involves an ethical hacker who fully scrutinizes your environment while attempting to breach data.

01 **PLANNING AND RECONNAISSANCE**

Identifying the scope of a test, as well as the systems to be addressed and the testing methods to be used.

02 **ANALYSIS**

The results of the penetration test are then compiled into a report detailing specific vulnerabilities, sensitive data that was accessed, and the amount of time it remained in the system undetected.

03 **SCANNING**

Inspecting an application's code to estimate the way it behaves while running. It is followed by inspecting an application's code in a running state.

04 **GAINING ACCESS**

Attacks such as cross-site scripting, SQL injection, and backdoors are used in this stage to uncover a target's vulnerabilities.

Technical Assessments

Identify potential security gaps and how to fix them. It is an excellent way to see how your cybersecurity strategy will fare in the real world.

External

To gain initial access to the target network, all possible attack vectors are analyzed from the adversary's perspective and all necessary hacking techniques are executed.

Internal

Validating the effectiveness of internal security controls and evaluating the risk of a compromised system in an organization.

Credential

A valid domain credential used in an internal security assessment to infiltrate mission-critical segments of the network via any LAN point or WiFi.

Work Station

Obtaining local access to the provided laptop or workstation; if successful, obtaining administrator privileges. Then using this machine to test installing unauthorized software and bypassing internal security controls.

Choose a suitable security assessment at the right time in accordance with your current business requirement.