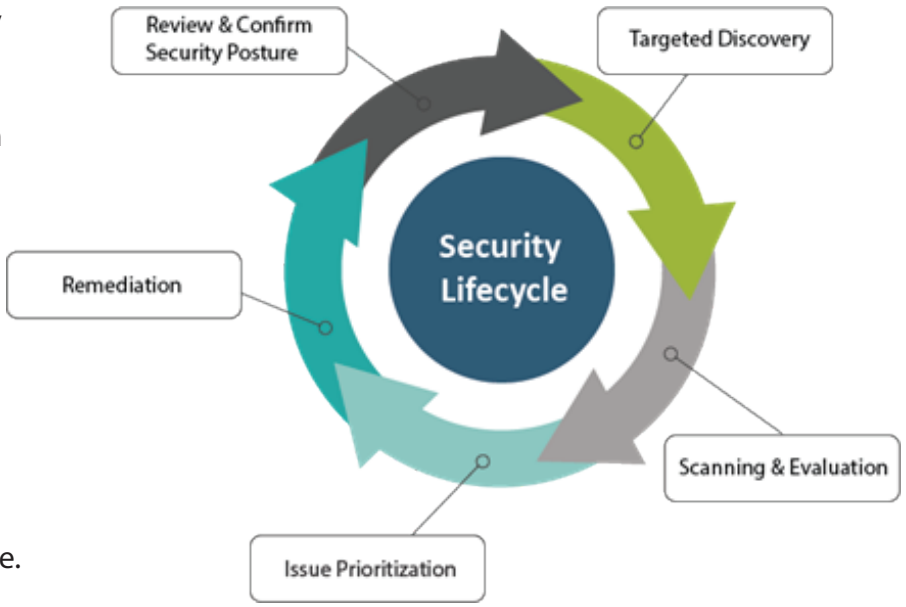
pcis Trusted Security Advisors

Comprehensive Security Vulnerability Assessments

Business technology is a constantly changing and evolving area of any modern organization. This constant progression requires regular investigation and re-evaluation of process, people and security. By adopting a model which recognizes the information security model ensures that critical issues, gaps, and business processes are regularly investigated and adapted to reduce the potential exposure and risk to the organization.

Assessments can take on many names and vary in terms of methodology, rigor and scope. However, the core objective remains consistent - identify and quantify the risks to an organization's technology and information assets.

The risks present within technology and business data has precipitated the need for organizations to become proactive in understanding their security needs. PCIS' Security Vulnerability Assessment provides a wealth of foundational information which helps organizations move decisively towards developing a proactive security posture.



The PCIS Methodology

PCIS considers the relationships between technology and the larger organizational structure as critical information which must be considered as part of any security assessment. Understanging an organization's use of technology, the people who use it, and the business goals it is meant to accomplish create foundations of knowledge used to create a complete understanding of the impact that comprehensive security planning will have.

A Security Vulnerability Assessment happens in two distinct engagements. The Discovery engagement helps create a foundational understanding of the organization. Using this foundational information as a guide, the Assessment engagement is a comprehensive standards-based evaluation of the entire organizations security posture as it relates to people, process and the business technology.

Insight Beyond Basic Measurement

Discovery Engagement

Activity includes focus groups, worksheets, interviews, and capturing data to develop a clear understanding of the organization's people, process and technologies. In evaluating the collected information a detailed Assessment Execution Plan is created. The purpose of this plan is to efficiently guide activity throughout the following Security Assessment engagement. If specific regulatory requirements are a consideration, evaluation tasks designed to meet all regulatory requirements are also defined with the Assessment Execution Plan.

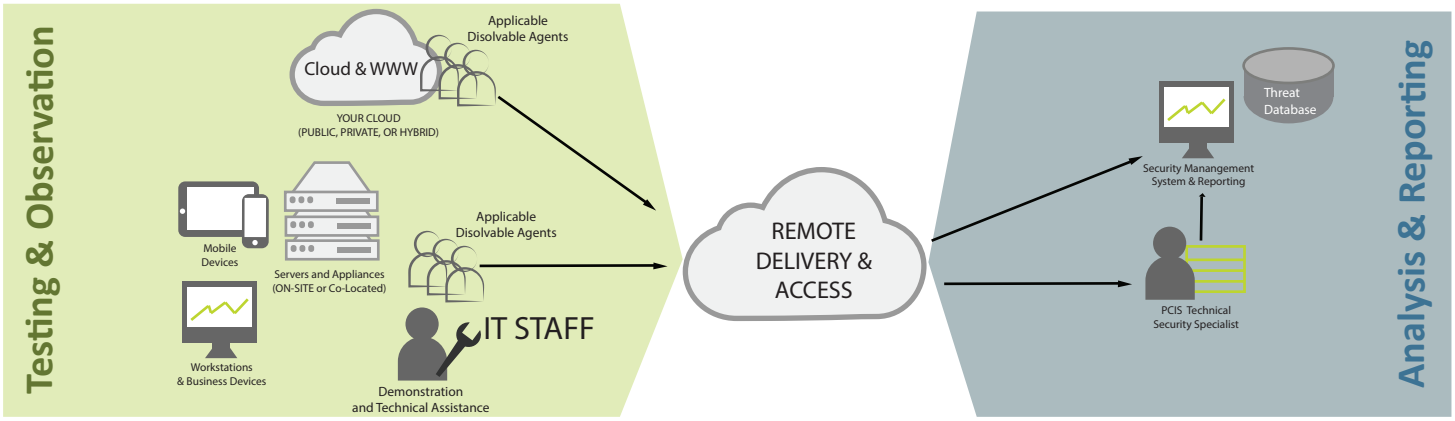
Assessment Engagement

Assessment activities are conducted within the contexts defined within the Discovery engagement, these include:

- Information sharing (verbally, visual demonstrations and documentation)
- Observing (configuration and execution of policies)
- Scanning for vulnerabilities using software-supported and manual tests
- Reviewing of organizational security policy and technical documentation

For most organizations, Assessment activities can be completed remotely, minimizing the need for on-site scheduling and demands on their internal resources.

REMOTE ASSESSMENT ACTIVITY



Reporting and Creating a Comprehensive Security Posture

The final Assessment Report provides a statement of measured and observed facts relating to an organization's current security state, relative to the baseline Centre for Internet Security framework and other standards if required. The Assessment Report provides recommendations for prioritization and actions required for remediation of the observed IT and/or web application security vulnerabilities. Included are detailed technical reports outlining found vulnerabilities, and evaluations of observed organizational practice and policy as it relates to the Centre for Internet Security Top 20 controls.

pcis Trusted Security Advisors

Security Vulnerability Assessment Reports

Discovery Engagement

Report Delivered	What's Included	Standard	Optional
Assessment Execution Plan	• Client Information Worksheet • SWOT Analysis • Execution Plan & Strategy • Organizational Technology & Data Maps	●	

Assessment Engagement

Report Delivered	What's Included	Standard	Optional
Security Assessment Executive Summary	• Methodology & Activity Review • Summaries of Findings • Critical Task & Future Planning Recommendations	●	
IT Vulnerability Technical Report	• Detailed Vulnerability Findings • Explanations & Theory • Remediation Instructions	●	
High Priority Patches	• Listing of High Priority Patches to be applied	●	
Vulnerability Scorecard	• Overview of technical security performance	●	
Compliance Scorecard (Windows Systems)	• Overview of applicable systems configuration compliance with CIS/SANS top 20 Security Controls	●	
Web Application Technical Report (per application)	• Detailed OWASP Vulnerability Findings • Explanations, Theory and Test Output • Remediation Instructions		●
PCI Vulnerability Scan Report	• PCI DSS v3.0 Compliant Vulnerability Technical Report including defined threat assignments		●
PCI Self-Assessment Questionnaires	• PCI DSS Vendor Self-Assessment Questionnaires (Version 3)		●
Quarterly Delta Reports	• Delta Reports with trending analysis (with previously generated data)		●