Security Maintenance Program

PROGRAM DEVELOPMENT | PROGRAM OPERATIONS | SME ADVISORY | AUDIT & COMPLIANCE OVERSIGHT

Risk Assessment: Done
What Now?

You have completed your risk assessment and now have an extensive report of recommended actions to achieve security and compliance. You know what needs to be done, but how do you implement identified requirements?

Maintain Your High Standards. Expand the expertise, support, operations, and analysis to a dedicated Security Maintenance Team.

We've got you covered.

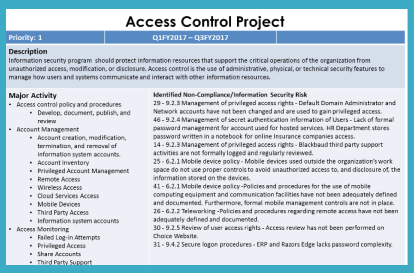
HALOCK®

PLAN

PROGRAM DEVELOPMENT

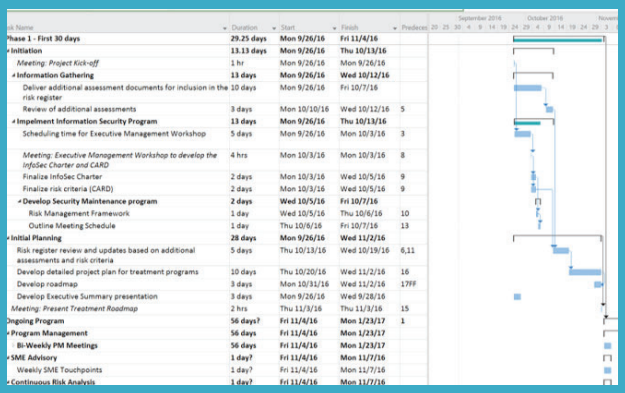
- Organize Risk Treatment options into clearly defined projects
- Arrange the projects into a tactical roadmap
- Define the major project activities, dependencies, benefits, and expected deliverables
- Estimate high-level investment in personnel, skills, resources, timelines, and budgets

Risk Assessments, Audit Findings, Vulnerability Scans



Remediation Plans, Program Requirements and Action Items

Security Maintenance Program Roadmap



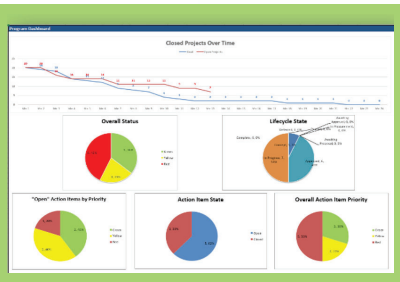
Program Plan

PERFORM

PROGRAM OPERATIONS

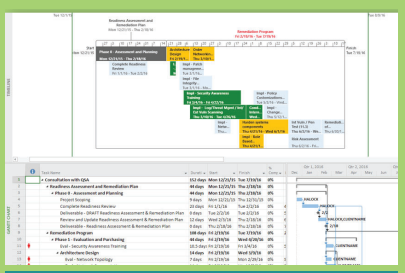
- Establish an Information Security Group (Security Management Team)
- Management of remediation projects
- Update the risk register with new threats and vulnerabilities
- Track the reduction of risk level when risk treatment plans close
- Continuous analysis of threats that are causing reported security breaches in your industry
- Dashboard updates on risk remediation progress
- Regular executive-level presentations providing Security Program updates

Information Security Group

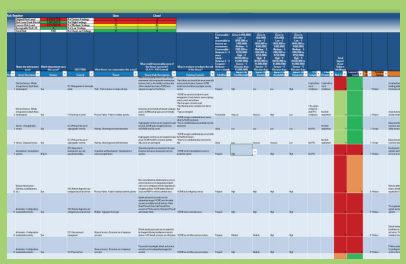


Executive Reporting

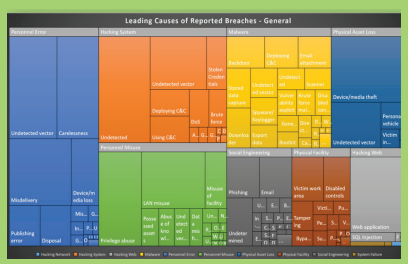
Bi-Weekly Meetings



Project Tracking & Reporting



Risk Register Management



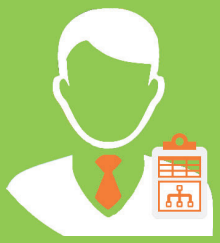
HALOCK Industry Threat Analysis (HIT Index)

PERFORM

SME ADVISORY

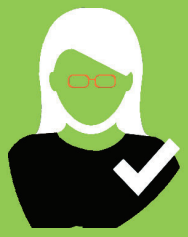
Support your team through a fractional Full Time Equivalent (FTE) to address needs for:

- Engineering personnel
- Governance personnel
- Audit personnel
- Compliance personnel
- Experienced practitioners for remediation optimization
- Executive Engagement



Project Manager

Risk Manager



Security Auditor

Security SME

CISA Certified Information Systems Auditor® An ISACA® Certification

CISM Certified Information Security Manager® An ISACA® Certification

PMI PMP®

LEAD AUDITOR ISO 27001 Information Security Management System

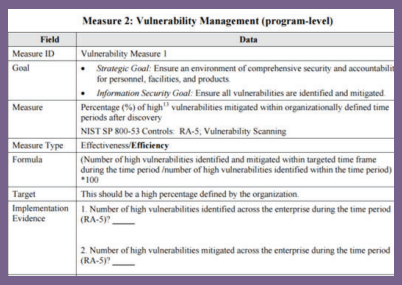
PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP®

MAINTAIN

AUDIT & COMPLIANCE OVERSIGHT

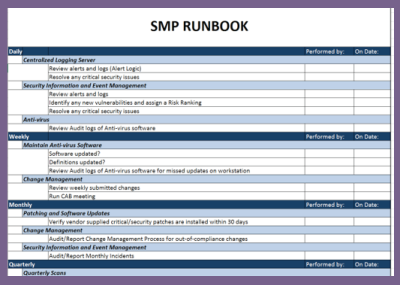
- Guidance for incorporating measures and metrics into individual control development
- Develop a high-level audit plan
- Integrate audit findings into the Risk Register to evaluate the effectiveness of controls
- Prepare for internal and external audits



Measure 2: Vulnerability Management (program-level)

Field	Data
Measure ID	Vulnerability Measure 1
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountabili for personnel, facilities, and products • *Information Security Goal:* Ensure all vulnerabilities are identified and mitigated.
Measure	Percentage (%) of high[1] vulnerabilities mitigated within organizationally defined time periods after discovery NIST SP 800-53 Controls: RA-5; Vulnerability Scanning
Measure Type	Effectiveness/**Efficiency**
Formula	(Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. Number of high vulnerabilities identified across the enterprise during the time period (RA-5)? ____ 2. Number of high vulnerabilities mitigated across the enterprise during the time period (RA-5)? ____

Audit Plans



SMP RUNBOOK

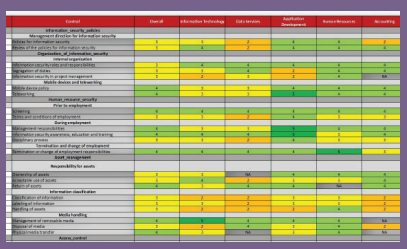
		Performed by:	On Date:
Daily			
Centralized Logging Server			
	Review alerts and logs (Alert Logic)		
	Resolve any critical security issues		
Security Information and Event Management			
	Review alerts and logs		
	Identify any new vulnerabilities and assign a Risk Ranking		
	Resolve any critical security issues		
Anti-virus			
	Review Audit logs of Anti-virus software		
Weekly		Performed by:	On Date:
Maintain Anti-virus Software			
	Software updated?		
	Definitions updated?		
	Review Audit logs of Anti-virus software for missed updates on workstation		
Change Management			
	Review weekly submitted changes		
	Run CAB meeting		
Monthly		Performed by:	On Date:
Patching and Software Updates			
	Verify vendor supplied critical/security patches are installed within 30 days		
Change Management			
	Audit/Report Change Management Process for out-of-compliance changes		
Security Information and Event Management			
	Audit/Report Monthly Incidents		
Quarterly		Performed by:	On Date:
Quarterly Scans			

Scheduled Audit Checkpoints

Evidence Collection Guidance

Controls Compliance Dashboard

Annual Documentation Review



Annual IT Audit Guidance

AFTER YOUR RISK ASSESSMENT - TO BE CONTINUED ...SECURELY.

Plan

Remediation efforts
Oversight process
Audit measures

Perform

Program operations
SME advisory
Threat analysis

Maintain

Continuous risk analysis
Oversight
Effectiveness testing

SECURITY PROGRAM ADD-ONS

Solutions / Safeguards

Penetration Testing
End-Point Protection
Next Gen Firewall
Malware Protection
Log/Threat Management
Vulnerability Scanning
Threat-Based Security Architecture Review & Analysis
Security Engineering Services
Compromise Assessment
Security Threat Management
Technology/Resell Partners

Quick Start Packages

Policies and Procedures
Security Awareness Training/Program
Business Continuity/DR
Change Management
Vulnerability Management
& More

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

www.halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.