

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.



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

Access Control Project
Priority: 1 03/20/17 - 03/20/17

Description
Information security program should protect information resources that support the critical operations of the organization from unauthorized access, modification, or disclosure. Access controls is the use of administrative, physical, or technical security features to manage how users and systems communicate and interact with other information resources.

Major Activity

- Access control policy and procedures
 - Develop, document, publish, and review
- Account Management
 - Account creation, modification, termination, and removal of information system accounts.
 - Account inventory
 - Privileged Account Management
 - Remote Access
 - Wireless Access
 - Cloud Services Access
 - Mobile Devices
 - Third Party Access
- Access Monitoring
 - Information system accounts
 - Privileged Access
 - Share Accounts
 - Third Party Support

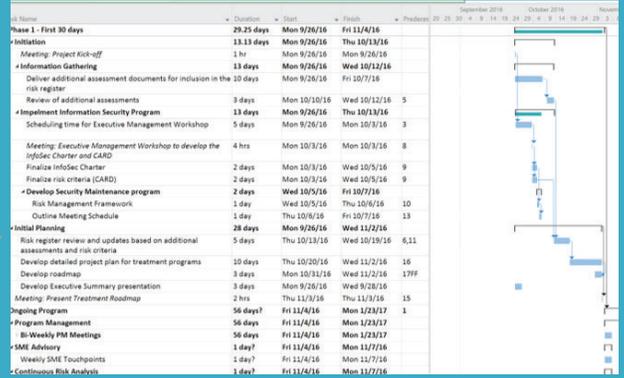
Identified Non-Compliance/Information Security Risk

- 25 - 9.2.3 Management of elevated access rights - Default Domain Administrator and Network accounts have not been changed and are used to gain privileged access.
- 46 - 9.2.3 Management of account authentication information of users - Lack of formal password management for accounts used for hosted services. HR Department stores password written in a notebook for online insurance company access.
- 14 - 9.2.3 Management of privileged access rights - Backup and third party support activities are not formally logged and regularly reviewed.
- 25 - 6.2.1 Mobile device policy - Mobile devices used outside the organization's work space do not use proper controls to avoid unauthorized access to and disclosure of the information stored on the device.
- 41 - 6.2.1 Mobile device controls - Policies and procedures for the use of mobile computing equipment and communication facilities have not been adequately defined and documented. Furthermore, formal mobile management controls are not in place.
- 26 - 6.2.2 Networking - Policies and procedures regarding remote access have not been adequately defined and documented.
- 30 - 9.2.3 Review of user access rights - Access review has not been performed on Choice Website.
- 31 - 9.4.3 Secure Signon procedures - ERP and Factors Edge lacks password complexity.

Remediation Plans, Program Requirements and Action Items

Major Activities Roadmap

Security Maintenance Program Roadmap



Program Plan



Risk Assessments, Audit Findings, Vulnerability Scans

Security Maintenance Program Roadmap



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



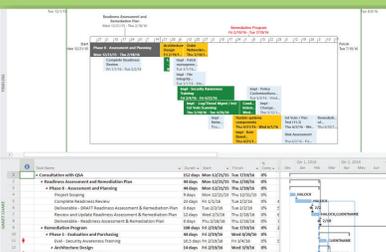
Information Security Group



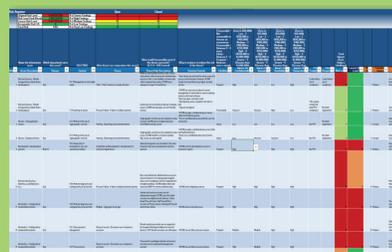
Executive Reporting



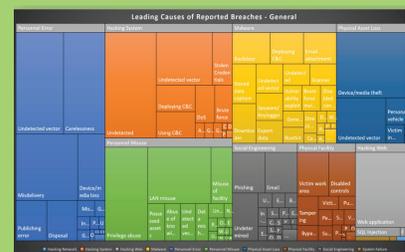
Bi-Weekly Meetings



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




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	<ul style="list-style-type: none"> • Strategic Goal: Ensure an environment of comprehensive security and accountability for personnel, facilities, and products • Information Security Goal: Ensure all vulnerabilities are identified and mitigated.
Measure	Percentage (%) of high ¹³ vulnerabilities mitigated within organizationally defined time periods after discovery
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	
Daily	Performed by: On Date
Controlled Logging Server	Review alerts and logs (Start Logs)
Security Information and Event Management	Review any critical security events
Security Alerts and Logs	Review alerts and logs
Alerts	Identify any new vulnerabilities and assign a Risk Rating
Alerts	Review any critical security issues
Alerts	Review audit logs of antivirus software
Weekly	Performed by: On Date
Maintain and review software	Software updated?
Change Management	Review Audit logs of anti-virus software for missed updates on workstation
Change Management	Review weekly submitted changes
Change Management	Run CIB meeting
Monthly	Performed by: On Date
Patching and Software Updates	Verify vendor supplied critical/security patches are installed within 30 days
Change Management	South Region Change Management Process for out-of-compliance changes
Security Information and Event Management	South Region Monthly Incidents
Quarterly	Performed by: On Date
Discovery Scans	

Scheduled Audit Checkpoints



Evidence Collection Guidance



Controls Compliance Dashboard



Annual Documentation Review

Control	Findings	Control Status	Control Owner	Control Description	Control ID
Information Security Policy	1	Compliant	IT	Information Security Policy	IS-POL-001
Information Security Policy Review	1	Compliant	IT	Information Security Policy Review	IS-POL-002
Information Security Policy Communication	1	Compliant	IT	Information Security Policy Communication	IS-POL-003
Information Security Policy Training	1	Compliant	IT	Information Security Policy Training	IS-POL-004
Information Security Policy Enforcement	1	Compliant	IT	Information Security Policy Enforcement	IS-POL-005
Information Security Policy Monitoring	1	Compliant	IT	Information Security Policy Monitoring	IS-POL-006
Information Security Policy Improvement	1	Compliant	IT	Information Security Policy Improvement	IS-POL-007
Information Security Policy Review	1	Compliant	IT	Information Security Policy Review	IS-POL-008
Information Security Policy Communication	1	Compliant	IT	Information Security Policy Communication	IS-POL-009
Information Security Policy Training	1	Compliant	IT	Information Security Policy Training	IS-POL-010
Information Security Policy Enforcement	1	Compliant	IT	Information Security Policy Enforcement	IS-POL-011
Information Security Policy Monitoring	1	Compliant	IT	Information Security Policy Monitoring	IS-POL-012
Information Security Policy Improvement	1	Compliant	IT	Information Security Policy Improvement	IS-POL-013
Information Security Policy Review	1	Compliant	IT	Information Security Policy Review	IS-POL-014
Information Security Policy Communication	1	Compliant	IT	Information Security Policy Communication	IS-POL-015
Information Security Policy Training	1	Compliant	IT	Information Security Policy Training	IS-POL-016
Information Security Policy Enforcement	1	Compliant	IT	Information Security Policy Enforcement	IS-POL-017
Information Security Policy Monitoring	1	Compliant	IT	Information Security Policy Monitoring	IS-POL-018
Information Security Policy Improvement	1	Compliant	IT	Information Security Policy Improvement	IS-POL-019
Information Security Policy Review	1	Compliant	IT	Information Security Policy Review	IS-POL-020

Annual IT Audit Guidance

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

RISK ASSESSMENT



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 Security Labs

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

Incident Response Hotline: 800-925-0559

www.halock.com

© Copyright 2019 HALOCK Security Labs. All rights reserved.

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.