SANS MANAGEMENT
CYBER LEADER

CURRICULUM

Get the right training to build and lead a world-class security team.

MGT414: SANS Training Program for CISSP® Certification (6 Days)
Need training for the CISSP® exam?

MGT415: A Practical Introduction to Cyber Security Risk Management (2 Days)
Understanding security risk management

MGT433: Managing Human Risk: Mature Security Awareness Programs (2 Days)
Building & leading a security awareness program

MGT512: Security Leadership Essentials for Managers (5 Days)
Leading security initiatives to manage information risk

MGT514: Security Strategic Planning, Policy, and Leadership (5 Days)
Aligning security initiatives with strategy

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud (2 Days)
Building & leading a vulnerability management program

MGT520: Leading Cloud Security Design and Implementation (2 Days)
Building & leading a cloud security program

MGT521: Leading Cybersecurity Change: Building a Security-Based Culture (2 Days)
Leading & aligning security initiatives with culture

MGT525: IT Project Management and Effective Communication (6 Days)
Managing security initiatives & projects

MGT551: Building and Leading Security Operations Centers (2 Days)
Building & leading Security Operations Centers

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems (6 Days)
Auditing a security program & controls

LEG523: Law of Data Security and Investigations (5 Days)
Understanding legal & regulatory requirements

SEC557: Continuous Automation for Enterprise and Cloud Compliance (3 Days)
Using Cloud Security & DevOps Tools to Measure Security & Compliance

SEC440: Critical Security Controls: Planning, Implementing & Auditing (2 Days)
Introduction to Critical Security Controls

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth (5 Days)
Building & auditing Critical Security Controls

RESOURCES

sans.org/cybersecurity-leadership

@secleadership

SANS Security Leadership

SANS

Security Leadership

POSTER

CISO Mind Map

Version 2.5

AND

Vulnerability Management Maturity Model

For Cyber Leaders of Today and Tomorrow

sans.org/cybersecurity-leadership

MGTPS_CISO-VM_v2.5_0221

CISO MIND MAP v. 2.1

Security Operations

- [ ] **Prevention**
  - Data Protection
    - Encryption, PKI, TLS
    - Data Loss Prevention (DLP)
    - User Behavior Analytics (UBA)
    - Email Security
    - Cloud Access Security Broker (CASB)
  - Network Security
    - Firewall, IDS/IPS, Proxy Filtering
    - VPN, Security Gateway
    - DDoS Protection
  - Application Security
    - Threat Modeling
    - Design Review
    - Secure Coding
    - Static Analysis
    - WAF, RASP
  - Endpoint Security
    - Anti-virus, Anti-malware
    - HIDS/HIPS, FIM
    - App Whitelisting
  - Secure Configurations
  - Zero Trust
  - Patch & Image Management
- [ ] **Detection**
  - Log Management/SIEM
  - Continuous Monitoring
  - Network Security Monitoring
  - NetFlow Analysis
  - Advanced Analytics
  - Threat Hunting
  - Penetration Testing
  - Red Team
  - Vulnerability Scanning
  - Web App Scanning
  - Bug Bounties
  - Human Sensor
  - Data Loss Prevention (DLP)
  - User Behavior Analytics (UBA)
  - Security Operations Center (SOC)
  - Threat Intelligence
  - Industry Partnerships
- [ ] **Response**
  - Incident Response Plan
  - Breach Preparation
  - Tabletop Exercises
  - Forensic Analysis
  - Crisis Management
  - Breach Communications

Legal and Regulatory

- [ ] **Compliance**
  - PCI
  - SOX
  - HIPAA/HITECH
  - FFIEC, CAT
  - FERPA
  - NERC CIP
  - NIST SP 800-37 and 800-53
  - NIST 800-61
  - NIST 800-171 (CUI)
  - FISMA and FedRAMP
- [ ] **Privacy**
  - Privacy Shield
  - EU GDPR
  - CCPA
- [ ] **Audit**
  - SSAE 16
  - SOC 2
  - ISO 27001
  - NIST SP 800-53A
  - COSO
- [ ] **Investigations**
  - eDiscovery
  - Forensics
- [ ] **Intellectual Property Protection**
- [ ] **Contract Review**
- [ ] **Customer Requirements**
- [ ] **Lawsuit Risk**

Business Enablement

- [ ] **Product Security**
  - Secure DevOps
  - Secure Development Lifecycle
  - Application Security
- [ ] **Cloud Computing**
  - Cloud Security Architecture
  - Cloud Guidelines
- [ ] **Mobile**
  - Bring Your Own Device (BYOD)
  - Mobile Policy
- [ ] **Emerging Technologies**
  - Internet of Things (IoT)
  - Artificial Intelligence (AI)
  - Machine Learning (ML)
- [ ] **Mergers and Acquisitions**
  - Security Due Diligence

Security Culture

- [ ] **Attributes**
  - Perceptions
  - Beliefs
  - Attitudes
  - Behaviors
  - Values
  - Norms
- [ ] **Models & Tools**
  - Fogg Behavior Model
  - Kotter's 8 Step Process
  - Prosci ADKAR Model
  - AIDA Marketing Model
  - Engagement/Culture Surveys

CYBER LEADER

Risk Management

- [ ] **Risk Frameworks**
  - FAIR
  - NIST RMF
  - OCTAVE
  - TARA
- [ ] **Risk Assessment Methodology**
- [ ] **Business Impact Analysis**
- [ ] **Risk Assessment Process**
- [ ] **Risk Analysis and Quantification**
- [ ] **Security Awareness**
- [ ] **Vulnerability Management**
- [ ] **Vendor Risk Management**
- [ ] **Physical Security**
- [ ] **Disaster Recovery**
- [ ] **Business Continuity Planning**
- [ ] **Policies and Procedures**
- [ ] **Risk Treatment**
  - Mitigation Planning, Verification
  - Remediation, Cyber Insurance

Identity & Access Management

- [ ] **Provisioning/Deprovisioning**
- [ ] **Single Sign On (SSO)**
- [ ] **Federated Single Sign On (FSSO)**
- [ ] **Multi-Factor Authentication**
- [ ] **Role-Based Access Control (RBAC)**
- [ ] **Identity Store (LDAP, Active Directory)**

Governance

- [ ] **Strategy**
- [ ] **Business Alignment**
- [ ] **Risk Management**
- [ ] **Asset Management**
- [ ] **Program Frameworks**
  - NIST CSF
  - ISO 27000
- [ ] **Control Frameworks**
  - NIST 800-53
  - CIS Controls
- [ ] **Program Structure**
- [ ] **Program Management**
- [ ] **Communications Plan**
- [ ] **Roles and Responsibilities**
- [ ] **Workforce Planning**
- [ ] **Resource Management**
- [ ] **Data Classification**
- [ ] **Records Management**
- [ ] **Security Policy**
- [ ] **Creating a Security Culture**
- [ ] **Security Training**
  - Awareness Training
  - Role-Based Training
- [ ] **Metrics and Reporting**
- [ ] **IT Portfolio Management**
- [ ] **Change Management**
- [ ] **Board Communications**

Leadership Skills

- [ ] **Business Strategy**
- [ ] **Industry Knowledge**
- [ ] **Business Acumen**
- [ ] **Communication Skills**
- [ ] **Presentation Skills**
- [ ] **Strategic Planning**
- [ ] **Technical Leadership**
- [ ] **Security Consulting**
- [ ] **Stakeholder Management**
- [ ] **Negotiations**
- [ ] **Mission and Vision**
- [ ] **Values and Culture**
- [ ] **Roadmap Development**
- [ ] **Business Case Development**
- [ ] **Project Management**
- [ ] **Employee Development**
- [ ] **Financial Planning**
- [ ] **Innovation**
- [ ] **Marketing**
- [ ] **Leading Change**
- [ ] **Customer Relationships**
- [ ] **Team Building**
- [ ] **Mentoring**

Based on CISO MindMap by Rafeeq Rehman
@rafeeq_rehman http://rafeeqrehman.com Used with permission.

Vulnerability Management Maturity Model

		LEVEL 1 **Initial**	LEVEL 2 **Managed**	LEVEL 3 **Defined**	LEVEL 4 **Quantitatively Managed**	LEVEL 5 **Optimizing**
Prepare	**Policy & Standards**	Policy and standards are undocumented or in a state of change.	Policy and standards are defined in specific areas as a result of a negative impact to the program rather than based on a deliberate selection of best practices or standards from recognized frameworks.	Policy and standards have been carefully selected based on best practices and recognized security frameworks and are updated as needed to fulfill the program's mission. Employees are made aware of standards and training on requirements is available.	Adherence to defined policy and standards is tracked and deviations are highlighted. Training of personnel on requirements is required at least annually.	Automated, proactive controls enforce policy and standards and provide input to regular updates and training requirements.
	Context	Contextual data (e.g., asset details, ownership, relationships) are available from multiple data sources with varying degrees of accuracy.	There is a central repository of contextual data that has some data for most systems and applications.	The central repository requires that certain contextual information be tracked and updated for each system and that it is based on program needs.	Reports show compliance with contextual information requirements and processes are in place to identify non-compliant, missing, or retired systems and applications.	Automated or technology-assisted processes and procedures exist to both create and remove systems and applications and associated attributes from the central repository, or data are correlated and reconciled with other systems that contain information about tracked systems and applications.
Identify	**Automated**	Infrastructure and applications are scanned ad-hoc or irregularly for vulnerability details, or vulnerability details are acquired from existing data repositories or from the systems themselves as time permits.	The process, configuration, and schedule for scanning infrastructure and applications is defined and followed for certain departments or divisions within the organization. Available technology may vary throughout the organization.	There are defined and mandated organization-wide scanning requirements and configurations for infrastructure and applications that set a minimum threshold for all departments or divisions. Technology is made available throughout the organization through enterprise licensing agreements or as a service.	Scanning coverage is measured and includes the measurement of authenticated vs. unauthenticated scanning (where applicable), the types of automated testing employed, false positive rates, and vulnerability escape rates.	Scanning is integrated into build-and-release processes and procedures and happens automatically in accordance with requirements. Scanning configurations and rules are updated based on previous measurements.
	Manual	Manual testing or review occurs when specifically required or requested.	Manual testing or review processes are established and some departments and divisions have defined requirements.	Manual testing or review occurs based on reasonable policy-defined requirements that apply to the entire organization and is available as a service where not specifically required by policy.	Deviations from manual testing or review requirements are tracked and reported.	Manual testing or review processes include focused testing based on historical test data and commonalities or threat intelligence.
	External	External vulnerability reports and disclosures are handled on a case-by-case basis.	Basic vulnerability disclosure policy (VDP) and contact information published, but backend processes and procedures not documented.	More comprehensive VDP in place, along with terms and conditions for external vendors and security researchers, that outlines rules of engagement, tracking, and feedback processes.	Compliance with VDP and terms and conditions is tracked and measured and information is used to streamline processes and evaluate vendors and researchers.	A mature external testing and research program is in place with specific goals and campaigns that may only be available to specific vendors or researchers.
Analyze	**Prioritization**	Prioritization is performed based on CVSS/Severity designations provided by identification technology or indicated in reports.	Prioritization also includes analysis of other available fields such as whether or not exploits or malware exist or confidence scores.	Prioritization includes correlation with the affected asset, asset group, or application to account for it's criticality in addition to the severity designation. This may require light to moderate customization depending on architecture and design.	Generic threat intelligence or other custom data, which may require additional products or services, are leveraged to perform prioritization.	Company-specific threat intelligence, or other information gathered from the operating environment, is leveraged to preform prioritization. This information may require human analysis or more extensive customization.
	Root Cause Analysis	Root cause analysis is performed based on out-of-the-box information such as standard remediation/patch reports or other categorized reports (e.g., OWASP Top 10 category).	Data are lightly customized to apply less granular or more meaningful groupings of data than CVE, CWE, or Top 10 identifiers to facilitate root cause analysis.	Data are also identified, grouped, and/or filtered by department or location to enable identification of location- or group-based deficiencies. This may require light to moderate customization depending on architecture and design.	Data are also identified, grouped, and/or filtered by owner or role. This may require more extensive customization and ongoing maintenance.	An executive dashboard is in place and includes the highest-risk root cause impediments, exclusions, project cost projections, etc. This will require more detailed analysis and customization to become meaningful and should integrate with existing executive business intelligence tools.
Communicate	**Metrics & Reporting**	Simple, point-in-time operational metrics are available primarily sourced from out-of-the-box reports leveraging minimal customization or filtering.	Filtered reports are created to target specific groups or prioritize findings. Specific divisions or departments have defined their own reporting requirements, including both program and operational metrics, and generate and release the corresponding reports at a defined interval.	Reporting requirements, including all required program, operational, and executive metrics and trends, are well-defined and baseline reports are consistent throughout the organization and tailored or filtered to the individual departments or stakeholders.	Reports and metrics include an indication of compliance with defined policy and standards, treatment timelines, and bug bars. Correlation with other security or contextual data sources allows for more meaningful grouping, improves accuracy, and allows for identification of faulty or inefficient design patterns.	Custom reporting is available as a service or via self-service options, or feedback is regularly solicited and reports are updated to reflect changing needs. Automated outlier and trend analysis along with exclusion tracking is performed to identify high/low performers and highlight systemic issues/successes.
	Alerting	Alerting is either not available or only available within security-specific technologies.	Integrations exist and alerts are being sent for specific divisions or departments or for users of specific non-security technologies already being leveraged by some stakeholders.	Alerting is available for most stakeholders in their technology of choice.	Visibility and both timing and detail of response to alerts is measured and tracked.	Data are analyzed to develop a standard or automated response to alerts for common issues that can be tied to a common response.
Treat	**Change Management**	Changes related to vulnerability management activities pass through the same workflow as any other change.	Some changes related to vulnerability management activities have a custom workflow or are treated as standard changes.	Most changes related to vulnerability management activities follow a custom workflow or are treated as standard changes.	Changes related to vulnerability management activities along with success rates are tracked. Timing is also measured for different stages of the change or subtasks related to the change.	Metrics from vulnerability management change activities are used to modify requirements or streamline future change requests. At least some standard changes are automated.
	Patch Management	Patches are applied manually or scheduled by admins and end-users.	There is a standard schedule defined and technology is available for some divisions or departments or for some platforms to automate patch testing and deployment.	All departments are required to patch within a certain timeframe and technologies are available to assist with testing and applying patches for all approved platforms.	Patch management activities are tracked along with compliance with remediation timelines and the success rate.	Data from patch management activities, security incidents, and threat intelligence are used to right-size remediation timelines and identify process or technology changes.
	Configuration Management	Configuration requirements are not well-defined and changes are either applied manually or the automatic application of configurations is only available for a subset of platforms.	Configurations are defined for some divisions or departments or for specific platforms.	Configurations are defined for all supported platforms and technologies are available to automate or validate configuration changes for all platforms.	Deviations from configuration requirements and associated service impacts are measured and tracked.	Data from the configuration process along with security incidents and threat intelligence are leveraged to strengthen or relax requirements as needed.

Cloud Vulnerability Management Roadmap

Level 1 Cloud infrastructure and applications are managed the same as on-premise technologies.

Level 2 Some modifications have been made to processes to account for cloud architecture and design differences. Some cloud management technologies are being leveraged.

Level 3 All processes have been analyzed, and where needed, tailored for the cloud, and cloud management technologies are broadly leveraged to account for cloud risks.

Level 4 Metrics, alerts, and reports include cloud-specific data and risks as well as compliance with cloud-specific requirements.

Level 5 Data from cloud monitoring are used to update images and code used to provision resources and applications in the cloud.

Cloud Vulnerability Management Responsibility Model

Infrastructure as a Service – Customer responsible for everything except physical network configuration and physical security.

Platform as a Service – Customer still responsible for secure configuration via exposed settings, IAM , proper configuration of virtualized network security controls, third-party assurance, and all application code, third-party libraries, or data deployed to platform. Customer not responsible for configuration of platform not available through APIs, OS and software patching, or physical security.

Software as a Service – Customer still responsible for secure configuration via exposed settings, IAM, proper configuration of virtualized network security controls, custom code, and third-party assurance. Customer not responsible for out-of-the-box code, OS and software patching, physical security.

Identification by Enterprise/Cloud Service Type

Environment/Service Type	Infra Vuln Scanning	Config Scanning	SAST	DAST	IAST/RASP	Pen Testing	Code Review	Component Analysis	Alternative Identification	Cloud/Service Analysis
Enterprise	A*	A	A	A*	?	A*	A	A	A	?
Infrastructure as a Service	P*	P	A	A*	?	A*	A	A	A	A
Platform as a Service	U	U	A	A*	U	A*	A	P	A	A
Software as a Service	U	U	P	?*	U	?*	P	P	A	?

A = Available
P = Partially Available
U = Unavailable
? = Depends on Provider/Technology
* = Permission Required

Vulnerability Management Metrics

Contextual measures and metrics are not explicitly related to VM operations or VM program governance, but measure data quality and availability in related processes and technology that can be leveraged to more effectively manage vulnerabilities or calculate risk.

Operational measures and metrics are usually derived directly from the processes and/or tools utilized to operate the VM program and may be correlated with contextual measures or metrics to provide additional clarity or to enable more meaningful grouping.

Program metrics are higher-level metrics meant to gauge the effectiveness and influence the direction of the VM program and its underlying policy.

Executive metrics are simple and directional representations of risk or other data points which highlight specific VM program needs requiring executive and/or board support or funding.

Metrics Examples

Contextual

- Percentage of assets with ownership revalidated in the last 90 days
- New assets identified, but not in inventory by month
- Process delays due to missing inventory, tags, or attributes

Operational

- Vulnerability aging (i.e., conforming, nearing due date, past due)
- Total, new, closed, and reopened vulnerability counts by *
- Request for change/security incidents on assets with critical vulnerabilities

Program

- Percentage of assets tested by identification type and business unit
- Vulnerability counts and mean time to resolution over time
- Mean time to exploit correlated with current remediation timelines

Executive

- High-level risk score with visual indication of trend by business unit
- Top three most vulnerable technologies
- Top three reasons for exclusion requests