Chapter 1 The Principles of Auditing 1

Security Fundamentals: The Five Pillars

- Assessment
- Prevention
- Detection
- Reaction
- Recovery

Building a Security Program

- Policy
- Procedures
- Standards

Security Controls

- Administrative Controls
- Technical Controls
- Physical Controls
- *Preventative Controls*
- *Detective Controls*
- *Corrective Controls*
- *Recovery Controls*

Managing Risk

- Risk Assessment 1
- Risk Mitigation 1
- Risk in the Fourth Dimension

How, What, and Why You Audit

- Audit Charter
- Engagement Letter
- Types of Audits
- *Security Review*
- *Security Assessment*
- *Security Audit*
- The Role of the Auditor
- Places Where Audits Occur
- *Policy Level*
- *Procedure Level*
- Control Level
- The Auditing Process
- Planning Phase: Audit Subject, Objective, and Scope
- Research Phase: Planning, Audit Procedures, and Evaluation Criteria
- Data Gathering Phase: Checklists, Tools, and Evidence

- Data Analysis Phase: Analyze, Map, and Recommend
- Audit Report Phase: Write, Present, and File the Audit Report
- Follow-Up Phase: Follow up, Follow up, Follow up!

Chapter 2 Information Security and the Law

- IT Security Laws
- Hacking, Cracking, and Fraud Law
- Intellectual Property Laws
- Digital Millennium Copyright Act
- Economic Espionage Act
- CAN-SPAM Act of 2003
- State and Local Laws
- Reporting a Crime
- Regulatory Compliance Laws
- SOX
- HIPAA
- *Privacy Rule*
- *Security Rule*
- *Transactions and Code Sets Standard Rule*
- *Identifiers Rule*
- *Enforcement Rule*

Chapter 3 Information Security Governance, Frameworks, and Standards 61

Understanding Information Security Governance

- People: Roles and Responsibilities
- Information Security Governance Organizational Structure
- *Board of Directors*
- *Security Steering Committee*
- *CEO or Executive Management*
- *CIO/CISO*
- *Security Director*
- *Security Analyst*
- *Security Architect*
- *Security Engineer*
- *Systems Administrator*
- *Database Administrator*
- *IS Auditor*
- *End User*
- Spotting Weaknesses in the People Aspect of Security

Process: Security Governance Frameworks

- COSO
- *Control Environment*
- *Risk Assessment*
- *Control Activities*
- *Information and Communication*
- *Monitoring*
- COBIT
- ITIL

Technology: Standards Procedures and Guidelines

- ISO 27000 Series of Standards
- NIST
- Center for Internet Security
- NSA
- DISA
- SANS
- ISACA
- Cisco Security Best Practices

Chapter 4 Auditing Tools and Techniques

Evaluating Security Controls

Auditing Security Practices

Testing Security Technology

Security Testing Frameworks

- OSSTMM
- ISSAF
- NIST 800-115
- OWASAP

Security Auditing Tools

- Service Mapping Tools
- *Nmap*
- *Hping*
- Vulnerability Assessment Tools
- *Nessus*
- *RedSeal SRM*
- Packet Capture Tools
- *Tcpdump*
- *Wireshark/Tshark*
- Penetration Testing Tools
- *Core Impact*
- *Metasploit*
- BackTrack

Chapter 5 Auditing Cisco Security Solutions

Auditors and Technology

Security as a System

Cisco Security Auditing Domains

- Policy, Compliance, and Management
- Infrastructure Security
- Perimeter Intrusion Prevention
- Access Control
- Secure Remote Access
- Endpoint Protection
- Unified Communications

Defining the Audit Scope of a Domain
Identifying Security Controls to Assess
Mapping Security Controls to Cisco Solutions
The Audit Checklist

Chapter 6 Policy, Compliance, and Management

Do You Know Where Your Policy Is?
Auditing Security Policies
Standard Policies

- Acceptable Use
- Minimum Access
- Network Access
- Remote Access
- Internet Access
- User Account Management
- Data Classification
- Change Management
- Server Security
- Mobile Devices
- Guest Access
- Physical Security
- Password Policy
- Malware Protection
- Incident Handling
- Audit Policy
- Software Licensing

Electronic Monitoring and Privacy
Policies for Regulatory and Industry Compliance
Cisco Policy Management and Monitoring Tools

- Cisco MARS
- Cisco Configuration Professional
- Cisco Security Manager
- Cisco Network Compliance Manager

Chapter 7 Infrastructure Security

Infrastructure Threats

- Unauthorized Access
- Denial of Service

- Traffic Capture
- Layer 2 Threats
- Network Service Threats

Policy Review 1

Infrastructure Operational Revie

- The Network Map and Documentation
- *Logical Diagrams*
- *Physical Diagrams*
- *Asset Location and Access Requirements*
- *Data Flow and Traffic Analysis*
- Administrative Accounts
- Configuration Management
- Vulnerability Management
- Disaster Recovery
- Wireless Operations

Infrastructure Architecture Review

- Management Plane Auditing
- *Cisco Device Management Access*
- *Syslog*
- *NTP*
- *Netflow*
- Control Plane Auditing
- *IOS Hardening*
- *Routing Protocols*
- *Protecting the Control Plane*
- Data Plane Auditing
- *Access Control Lists*
- *iACLs*
- *Unicast Reverse Path Forwarding*
- Layer 2 Security
- xii Network Security Auditing
- *VTP*
- *Port Security*
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *IP Source Guard*
- *Disable Dynamic Trunking*
- *Protecting Spanning Tree*
- *Switch Access Controls Lists*
- *Protect Unused Ports*
- Wireless Security
- *Wireless Network Architecture*
- *Cisco Adaptive Wireless Intrusion Prevention System*
- *Protecting Wireless Access*

- *Wireless Service Availability*
- *Rogue Access Point Detection*
- General Network Device Security Best Practices

Technical Testing

- Router Testing
- Switch Testing
- Wireless Testing

Chapter 8 Perimeter Intrusion Prevention

- Perimeter Threats and Risk
- Policy Review

Perimeter Operations Review

- Management and Change Control
- Monitoring and Incident Handling

Perimeter Architecture Review

- What Are You Protecting?
- Perimeter Design Review
- *Logical Architecture*
- *Physical Architecture*
- *What Is the Risk?*
- *Good Design Practices*

Auditing Firewalls

- Review Firewall Design
- *Simple Firewall*
- *Screening Router and Firewall*
- *Firewall with*
- *Firewall with DMZ and Services Network*
- *High Availability Firewall*
- IOS Firewall Deployment
- Review Firewall Configuration
- *Firewall Modes of Operation*
- *Firewall Virtualization*
- *Filtering Methods*
- *Network Address Translation*
- *Secure Management*
- *Logging 256*
- *Other Configuration Checks*
- Review Rule Base
- *Cisco Firewall Rule Basics*
- *Rule Review*
- *Rule Optimization*
- *The ASA Modular Policy Framework and Application Inspection*

IOS Zone-Based Firewall 263

Auditing IPS

- How IPS Works
- Review IPS Deployment
- Review IPS Configuration
- *Protect the Management Interface*
- *Administrative Access and Authentication*
- *NTP Configuration*
- *Signature Updates*
- *Event Logging*
- Review IPS Signatures
- *Signature Definitions*
- *Event Action Rules*
- *Target Value Rating*
- *IOS IPS*

Network Security Auditing

Technical Control Testing

- Firewall Rule Testing
- Testing the IPS
- *Conducting an IPS Test*
- *Reviewing the Logs*

Chapter 9 Access Control

Fundamentals of Access Control

- Identity and Authentication

Access Control Threats and Risks

Access Control Policy

Access Control Operational Review

- Identity Operational Good Practices
- Authorization and Accounting Practices
- Administrative Users
- Classification of Assets

Access Control Architecture Review

- Identity and Access Control Technologies
- Network Admission Control
- *NAC Components*
- *How NAC Works*
- *NAC Deployment Considerations*
- *NAC Posture Assessment*
- Identity-Based Networking Services
- *Deployment Methods*
- NAC Guest Server
- NAC Profiler

Technical Testing

- Authentication and Identity Handling

- Posture Assessment Testing
- Testing for Weak Authentication

Chapter 10 Secure Remote Access

Defining the Network Edge
VPN Fundamentals
- Confidentiality
- *Symmetric Encryption*
- *Asymmetric Encryption*
- Integrity
- Authentication and Key Management
- IPsec, SSL, and dTLS
- *IPsec*
- *Secure Socket Layer*
- *Datagram Transport Layer Security (dTLS)*

Remote Access Threats and Risks
Remote Access Policies
Remote Access Operational Review
- VPN Device Provisioning
- Mobile Access Provisioning
- Mobile User Role-Based Access Control
- Monitoring and Incident Handling

Remote Access Architecture Review
- Site-to-Site VPN Technologies
- *Easy VPN*
- *IPsec and Generic Router Encapsulation (GRE)*
- *Dynamic Multipoint VPN (DMVPN)*
- *Multi Protocol Label Switching (MPLS) and Virtual Routing and*

Forwarding (VRF) VPNs
GETVPN
Mobile User Access VPN
IPsec Client
Clientless SSL VPN
Cisco Secure Desktop
SSL Full Tunneling Client
VPN Network Placement
VPN Access Controls
Site-to-Site Access Controls
Mobile User Access Controls
Remote Access Good Practices
Technical Testing
- Authentication
- IPsec 351

- SSL
- Site-to-Site Access Control Testing
- Mobile User Access Control Testing
- Monitoring and Log Review

Chapter 11 Endpoint Protection
Endpoint Risks
Endpoint Threats

- Malware
- Web-Based Threats
- *Social Networking and Web 2.0*
- E-Mail Threats
- Data Loss Threats

Policy Review 368
Endpoint Protection Operational Control Review

- Current Threat Intelligence 370
- Vulnerability and Patch Management
- Monitoring and Incident Handling
- Security Awareness Program

Endpoint Architecture Review

- Cisco Security Intelligence Operations
- *SensorBase*
- *Cisco Threat Operations Center*
- *Dynamic Update Function*
- Web Controls 376
- *Web Security Appliance*
- *ASA*
- *IPS*
- *CSA*
- E-Mail Controls
- *E-Mail Policy Enforcement*
- *E-Mail Authentication*
- Data Loss Prevention
- *Web*
- E-Mail
- *Client*
- *Patch Management*
- Monitoring
- *Web*
- *E-Mail*
- *MARS*

Technical Testing

- Acceptable Use Enforcement

- Malware Detection and Quarantine
- SPAM, Phishing, and E-Mail Fraud
- Encryption
- Patch Management and Enforcement
- Data Loss Prevention Testing
- Detection and Response