

INFORMATION SECURITY ARCHITECTURE: AN INTEGRATED APPROACH TO SECURITY IN THE ORGANIZATION, SECOND EDITION

INFORMATION SECURITY ARCHITECTURE

Why an Architecture?
Client/Server Environments
Overview of Security Controls
The Strategic Information Technology (IT) Plan
Summary
Getting Started

SECURITY ORGANIZATION / INFRASTRUCTURE

Learning Objectives
The Security Organization
The Executive Committee for Security
The Chief Information Officer
The Chief Financial Officer
The Security Officer
The Security Team
Security Coordinators or Liaisons
Departmental Management
Network and Application Administrators
Human Resources
Legal Counsel
Help Desk
Audit
System Users
Centralized versus Decentralized Security Administration
Information and Resource Ownership
The Strategic Information Technology (IT) Plan
Chapter Summary
Getting Started: Project Management
Starcross, Inc.
Enterprise wide Information Security Architecture
Business Need
Approach, Scope, and Deliverables
Key Milestones
External Security Systems (ESS) Engagement Team
Engagement Management
Change Management Approach
Deliverables
Notes

SECURITY POLICIES, STANDARDS, AND PROCEDURES

Introduction
Learning Objectives
The Information Security Policy
Information Security Policy Acknowledgment Form
Network Usage Policy
E-Mail Policy
Internet Policy
Internet Risk
Process for Change
Security Standards

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/721>

Standards Organizations
Security Procedures
Chapter Summary
Getting Started
Notes

SECURITY BASELINES AND RISK ASSESSMENTS

Information Security Assessment: A Phased Approach
High-Level Security Assessment (Section I)
Assessing the Organization of the Security Function
Assessing the Security Plan
Assessing Security Policies, Standards, and Procedures
Assessing Risk-Related Programs
Security Operations (Section II)
Security Monitoring
Computer Virus Controls
Microcomputer Security
Compliance with Legal and Regulatory Requirements
Computer Operations (Section III)
Physical and Environmental Security
Backup and Recovery
Computer Systems Management
Problem Management
Application Controls Assessments
Access Controls
Separation (or Segregation) of Duties
Audit Trails
Authentication
Application Development and Implementation
Change Management
Database Security
Network Assessments.
Emergency Response
Remote Access
Gateways Separating the Corporate WAN and Lines of
Business
Current and Future Internet Connections
Electronic Mail and the Virtual Office
Placement of WAN Resources at Client Sites
Operating System Security Assessment
Windows NT
Telecommunications Assessments
Summary

SECURITY AWARENESS AND TRAINING PROGRAM

Program Objectives
Employees Recognize Their Responsibility for Protecting the
Enterprise's Information Assets
Employees Understand the Value of Information Security
Employees Recognize Potential Violations and Know Who
to Contact
The Level of Security Awareness among Existing Employees
Remains High
Program Considerations
Effectiveness Is Based on Long-term Commitment of
Resources and Funding
Benefits Are Difficult to Measure in the Short Term

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/721>

Scoping the Target Audience
Effectively Reaching the Target Audience
Security Organizations
Summary
Getting Started - Program Development

COMPLIANCE

Level One Compliance: The Component Owner
Level Two Compliance: The Audit Function
Level Three Compliance: The Security Team
Line of Business (LOB) Security Plan
Enterprise Management Tools
Summary

PITFALLS TO AN EFFECTIVE ISA PROGRAM

Lack of a Project Sponsor and Executive Management Support
Executive-Level Responsibilities
Executive Management's Lack of Understanding of Realistic Risk
Lack of Resources
The Impact of Mergers and Acquisitions on Disparate Systems
Independent Operations throughout Business Units
Discord Between Mainframe versus Distributed Computing Cultures
Fostering Trust in the Organization
Mom-and-Pop Shop Beginnings
Third-Party and Remote Network Management
The Rate of Change in Technology
Summary
Getting Started

COMPUTER INCIDENT / EMERGENCY RESPONSE

Introduction
Learning Objectives
CERT®/CC
CSIRT Goals and Responsibilities
Reactive Services
Alerts and Warnings
Incident Handling
Vulnerability Handling
Artifact Handling
Incident Response Handling Methodology
Reporting
Incident Classification
Triage
Identification
Incident Analysis
Incident Response
Incident Response Coordination
Key Organizations
Containment
Eradication
Recovery
Notification
Development of the CSIRT
Issues in Developing a CSIRT
Funding

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/721>

Management Buy-In
Staffing and Training
Policy Development
Legal Issues
Re-evaluation of CSIRT Operations
Chapter Summary
Getting Started
Notes

CONCLUSION

APPENDIXES

Information Security Policy
Information Security Policy Acknowledgment Form
Network Computing Policy
E-Mail Security Policy
Internet Policy
Security Lists
Security Standards and Procedures Manual Table of
Anti-Virus Update Procedure
Security Assessment Workplan
Applications Security Assessment
Network Security Assessment Workplan
Windows NT Assessment Workplan
Telecommunications Security Assessment Workplan
Computer Incidence/Emergency Response Plan
Sample Line of Business Security Plan
Intrusion Checklist