

# Introduction to Security Auditing

---

**San Francisco ISACA Fall Seminar**

*Carey Carpenter*

*Steve Revesz*

*Deloitte*

*Enterprise Risk Services*

**Deloitte**

*October 4, 2004*



# Agenda

---

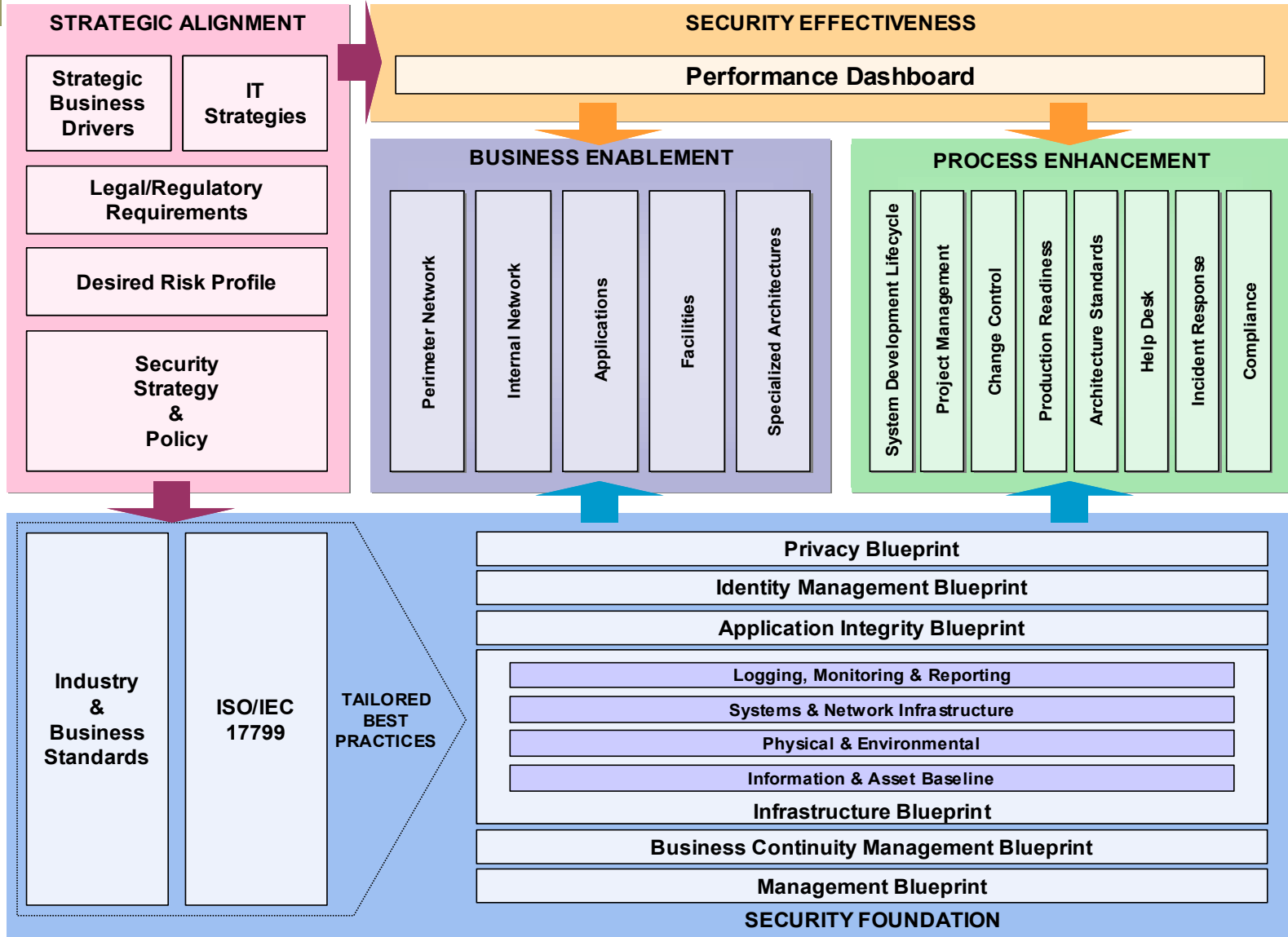
## ● Security Audit Areas

- Security Strategy, Policies and Organization
- User Access Administration
- Secure Systems Development
- Application, Database, Network and Operating System Security
- Intrusion Detection / Prevention Systems
- Emergency Response
- Remote Access and Third Parties
- User Awareness and Training
- Physical Security
- Legal and Regulatory Compliance

## ● Audit Considerations

- Risk Based Audit Approach
- Audit Program Development
- Third Party Security Specialists

# Enterprise Security Architecture





# Security Strategy, Policies and Organization

---

## ● Strategy

- Does the company have a security strategy?
- If so, does it appear to be appropriate?

## ● Security Organization

- Is there a separate security organization?
- Is it appropriately staffed with qualified resources?
- What is the reporting relationship? Is the level of authority adequate?

## ● Policies

- Are policies formally documented and ratified?
- Are they current and comprehensive?
- Are they practical?
- Have they been implemented?
- Does they address all constituents (Management, Security, IT, Users)?



# Policies, Procedures, Standards and Guidelines

---

## ● Policy

- Management directive, mandatory in nature.
- Establishes a framework.

## ● Procedures

- Steps or activities to be performed to achieve policy compliance.
- The “How To” of the policy.

## ● Standards and Baselines

- Typically relate to a specific technology.
- Generally should be followed, unless an exception is necessary due to a specific business need.

## ● Guidelines

- Recommendation activities or standards, usually optional but recommended.



# Security Policies Reference

---

- **Information Security Policies Made Easy Version 9, Charles Cresson Wood**
- **ISACA Bookstore \$795.00 (ISACA Members)**
- **More that 1,360 already-written policies including:**
  - Web Pages
  - Firewalls
  - Employee Surveillance
  - Digital Signatures
  - Computer Viruses
  - Encryption
  - Contingency Planning
  - Logging Controls
  - Internet / Intranet
  - Privacy Issues
  - Outsourcing Security Functions
  - Computer Emergency Response Teams
  - Microcomputers
  - Local Area Networks
  - Password Selection
  - Electronic Mail
  - Data Classification
  - Telecommuting
  - Telephone Systems
  - Portable Computers
  - User Training
  - Information Security-Related Terrorism



# User Access Administration

---

- **COBIT: Ensure Systems Security**
- **User Account Management Control Objective**
  - Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.
  - A formal approval procedure outlining the data or system owner granting the access privileges should be included.
- **Management Review of User Accounts**
  - Management should have a control process in place to review and confirm access rights periodically.
  - Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration.
- **Central Identification and Access Rights Management**
  - Controls are in place to ensure that the identification and access rights of users [and] system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

COBIT *Control Objectives*, 3<sup>rd</sup> Edition, Information Systems Audit and Control Foundation (ISACF), July 2000.



# User Access Administration

---

## ● Common Control Concerns

- Informal, Decentralized or Fragmented Process
- User Roles Not Formally Defined
- Inadequate User Access Request Methods
  - Forms Are Too General
  - Requests and Approvals Not Be Documented
  - An Audit Trail Not Maintained
- User Termination Notification Processes Not Effective
- User Removal Processes Not Comprehensive
- Periodic Reviews Not Performed



# Identity Architecture

---

- **Identity Management**

- Authoritative Source
- Identity Repository (such as LDAP)

- **User Provisioning**

- Providing Authorities to the Identities

- **Access Management**

- Mechanism by which Users Gain Access to Provisioned Resources
- Single / Reduced Sign-On

- **Role Based Access Control**

- **Protection of Identifiers**

- Authentication Methods

“Identity Architecture”, Steven J. Ross, *Information Systems Control Journal*, Volume 4, 2003.



# Secure Systems Development

---

- **New systems are developed and implemented in accordance with security requirements.**
- **Systems modifications do not degrade security compliance.**
- **Written policies and procedures should define responsibilities and requirements relevant to systems development.**
- **Software Capability Maturity Model**
  - Based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance process.

The CISSP Prep Guide, Ronald L. Krutz and Russell Dean Vines, Wiley Publishing Inc., 2003.

- **Security Organization and Internal Audit Participation**
  - Can be Consultative or Assessment / Compliance
  - Can Occur throughout the Life Cycle
    - Pre-, Go-Live and Post-Implementation



# Technology Based Security Controls

---

## ● Logical Access Security Levels

- Application
- Database
- Network
- Operating System

## ● Common Control Objectives

- Only authorized users are granted access.
- Access is granted in accordance with assigned job responsibilities.
- User access rights are restricted to enforce an adequate segregation of duties.
- Advanced access rights and sensitive functions are appropriately restricted.
- Security parameters including password controls help to ensure that access is restricted to only authorized personnel.
- Information resources are protected (e.g. file and directory permissions).
- Security events are logged and monitored.



# Intrusion Detection / Prevention Systems

---

## ● Intrusion Detection Systems (IDS)

- Signature Based Detection and Protocol and Behavior Anomaly Detection
- Host-Based
  - Watches for processes inside the host and monitor log files and data for suspicious activity.
- Network-Based
  - Examine characteristics of every packet that passes on the network.
- Hybrid

## ● Intrusion Prevention Systems (IPS)

- Take an active role in preventing or responding to an attack.
  - Drop the Traffic
  - Shun (Block Traffic from an Attacker's Host – can result in Denial of Service)
  - Terminate Process

**“Intrusion Detection and Prevention: Security’s One-Two Punch”, Frank Huerta and Barry Cioe, and “The How and Why of Intrusion Detection and Prevention”, Ray Stirbei, *The ISSA Journal*, August 2003.**



# Emergency Response

---

- **Identify Suspicious Activities or Security Breaches**
- **Manage New Security Threats**
  - Blaster Worm
- **NIST Special Publication 800-61, Computer Security Incident Handling Guide**
  - Organizing a computer security incident response capability
  - Establishing incident response policies and procedures
  - Structuring an incident response team
  - Handling incidents from initial preparation through the post-incident lessons learned phase



# Remote Access and Third Parties

---

## ● Remote Access Control Objectives

- Authorization, Authentication, Logging and Monitoring
- Consider strong (2 Factor) authentication methods
- Consider limiting access capabilities to only selected information resources
- Ensure that controls are consistent for remote access

## ● Third Party Access

- 100% of Third Parties with Direct Access should be known and documented
- Written, signed contracts should establish security requirements
  - Unique User Ids for All Users
  - Appropriate Password Controls
  - Termination Notification and Removal Procedures
  - Limit Access to the Minimum Required (Principle of Least Privilege)
  - Design Controls to Monitor and Evaluate Third Party Activities



# User Awareness and Training

---

## ● Successful Security is Not a Technical Solution

- Users Must Be Aware of the Importance of Security
- Users Must Understand their Responsibilities
- It is a Cultural Challenge to View Security as a Business Enabler, Not an Inhibitor
- Control Environment / Tone at the Top / Senior Management Attitude

## ● Awareness and Training Life Cycle

- Design a Program
- Provide Targeted Training
  - Users
  - IT
  - Security Personnel
  - Management
- Raise and Maintain Awareness



# Physical Security

---

- **Physical Access Is Restricted**

- Buildings, Data Centers, Computer Rooms, Network and Telecommunications Equipment
- Personal Computers and Laptops

- **Management Control Objectives**

- Access Approval
- Access Logging and Monitoring
- Termination Notification and Removal Procedures
- Periodic Review



# Legal and Regulatory Compliance

---

- **Legal and Regulatory Pressure is Increasing**

- Sarbanes-Oxley
- HIPAA Privacy Regulations and Security Rules
- Gramm-Leach-Bliley Act
- California Security Breach Information Act (S.B. 1386)
- FDICIA Requirements



# Risk Based Audit Approach

---

- **Perform an Entity Level Security Risk Assessment**
  - Company Objectives
  - Security Threats
  - Level of Vulnerability
  - Areas of Highest Risk
- **Develop and Execute a Risk-Based Audit Plan**
  - Areas Identified as High Risk
  - Areas of Emerging Risk
  - Areas with Known Control Weaknesses
  - Management Requests For Assistance
- **Continue to Monitor and Update the Risk Assessment**
  - Environmental and Organizational Changes



# Audit Program Development

---

- **ISACF COBIT  
(Control Objectives for Information and Related Technology)**
  - Management Guidelines
  - Executive Summary
  - Framework
  - Audit Guidelines
  - Control Objectives
  - Implementation Tool Set
- **ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management**
- **FFEIC Information Technology Examination Handbook InfoBase**
- **HIPAA Privacy Regulations and Security Rules**

## Auditors Sharing Audit Programs

### NEW PROGRAMS ADDED THIS MONTH



1. [Baan Audit Program \(9/1/03\)](#) PDF
2. [Billings for Reinsurance Recoverables ICQ \(9/1/03\)](#) PDF
3. [Budgetary Control ICQ \(9/1/03\)](#) PDF
4. [Creditor Risk Register Template \(9/1/03\)](#) PDF
5. [External Consultants ICQ \(9/1/03\)](#) PDF
6. [JDE One World Security Audit Program \(9/1/03\)](#) PDF
7. [Legal and Government Affairs \(9/1/03\)](#) PDF
8. [Microsoft SQL Server Audit Checklist \(\(9/1/03\) \(contribution required\)](#)
9. [Oracle Audit Checklist \(9/1/03\)](#) PDF
10. [Partnership Agreements \(Education\) ICQ \(9/1/03\)](#) PDF
11. [Power Plant Operations Audit Program \(9/1/03\)](#) PDF
12. [Powerlock Network Security \(9/1/03\)](#) PDF
13. [Sales System Audit Program \(9/1/03\)](#) PDF
14. [Strategic Asset Management ICQ \(9/1/03\)](#) PDF
15. [Wireless LAN Review \(9/1/03\)](#) PDF

### A. MANAGEMENT AND FINANCIAL AUDIT PROGRAMS

1. [3rd Party Construction Contracts \(Word\)](#) PDF
2. [401 K Plan Audit Program](#)
3. [401K Loan Audit Program](#) W PDF
4. [403B Retirement Plan](#)
5. [A/E Design Price Audit Program](#)



# NIST Computer Security Special Publications

Address <http://csrc.nist.gov/publications/nistpubs/> Go

- [News & Events](#)
- [Federal News](#)
- [Security Events](#)

- [Services For the:](#)
- [Federal Community](#)
- [Vendor](#)
- [User](#)

- [Links & Organizations](#)
- [Academic](#)
- [Government](#)
- [Professional](#)
- [Additional Links](#)

- [General Information](#)
- [Site Map](#)
- [Virus Information](#)

[Search CSRC](#)



[Search Vulnerability Archive](#)

Enter vendor, software, or keyword



**SP 800-48** Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, **November 2002**

[Adobe Acrobat .pdf file](#) (1,050,853 bytes)  
[Zipped .pdf file](#) (797,896 bytes)

**SP 800-47** Security Guide for Interconnecting Information Technology Systems, **September 2002**

[Adobe Acrobat .pdf file](#) (745,484 bytes)  
[Zipped .pdf file](#) (516,275 bytes)

**SP 800-46** Security for Telecommuting and Broadband Communications, **September 2002**

[Adobe Acrobat Reader file pdf](#) (3,869,074 bytes)  
[Zipped .pdf file](#) (2,207,382 bytes)

**SP 800-45** Guidelines on Electronic Mail Security, **September 2002**

[Adobe Acrobat Reader .pdf file](#) (1,123,602 bytes)  
[Zipped .pdf file](#) (1,043,103 bytes)

**SP 800-44** Guidelines on Securing Public Web Servers, **September 2002**

[Adobe Acrobat Reader .pdf file](#) (2,234,418 bytes)  
[Zipped .pdf file](#) (2,121,759 bytes)

**SP 800-43** Systems Administration Guidance for Windows 2000 Professional



# Third Party Security Specialists

---

- **Specialist Knowledge of Specific Technologies and Audit Techniques**
  - Applications, Databases, Networks, Operating Systems
  - Security Technologies Including Firewalls, IDS/IPS
  - Attack & Penetration Vulnerability Assessments
- **Use of Automated Assessment Tools**
  - Experience in Benefits and Risks
  - Software Licensing Considerations



# Selected Resources

---

- Information Systems Audit and Control Association [www.isaca.org](http://www.isaca.org)
- IT Governance Institute [www.ITgovernance.org](http://www.ITgovernance.org)
- SANS (SysAdmin, Audit, Network, Security) Institute [www.sans.org](http://www.sans.org)
- International Information Systems Security Certification Consortium, Inc. [www.isc2.org](http://www.isc2.org)
- Auditors Sharing Audit Programs [www.auditnet.org](http://www.auditnet.org)
- MIS Training Institute [www.misti.com](http://www.misti.com)
- NIST (National Institute of Standards and Technology) Computer Security Resource Center [csrc.nist.gov](http://csrc.nist.gov)
- Federal Financial Institutions Examination Council's (FFIEC) [www.ffiec.gov](http://www.ffiec.gov)
- International Organization for Standardization [www.iso.org](http://www.iso.org)
- HIPAA Final Privacy Rules [www.access.gpo.gov/su\\_docs/fedreg/a001228c.html](http://www.access.gpo.gov/su_docs/fedreg/a001228c.html)
- The CISSP Prep Guide, Ronald L. Krutz and Russell Dean Vines, Wiley Publishing Inc., 2003.



# Contact Information

---

**Carey Carpenter**

**Deloitte**

**Enterprise Risk Services**

**50 Fremont Street**

**San Francisco, CA 94105**

**Desk/Voicemail 415.783.5290**

**Cellular 415.602.7605**

**Fax 415.783.9130**

**E-Mail [ccarpenter@deloitte.com](mailto:ccarpenter@deloitte.com)**

**Steve Revesz**

**Deloitte**

**Enterprise Risk Services**

**50 Freemont Street**

**San Francisco, CA 94105**

**Desk/Voicemail 415.783.4311**

**Cellular 415.706.2779**

**Fax 415.783.9844**

**E-Mail [srevesz@deloitte.com](mailto:srevesz@deloitte.com)**