



Education

# A CISO's View of the Storage Ecosystem

Andrew Nielsen, CISSP, CISA, ISSAP, ISSMP, INAL  
Hitachi Data Systems

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - ◆ Any slide or slides used must be reproduced in their entirety without modification
  - ◆ The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

**NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.**

## ➤ A CISO's View of the Storage Ecosystem

- ◆ This session will appeal to Storage Professionals and those that are seeking a fundamental understanding of what drives the CISO and how they view and interact with the storage ecosystem. The session will help Storage Professionals understand how Security Professionals measure the storage layer and combat risk and threat. Not limited to just Storage Professionals, this session identifies ways for the Security and Storage teams to peacefully co-exist and partner in order to achieve organization goals: generally audit compliance and data confidentiality.

- What is a CISO
- What Drives the CISO
- How the CISO Measures Storage Security
- Security & Storage: Co-existence & Partnership
- Final Thoughts

# What is a CISO?

- CISO = Chief Information Security Officer
- Sometimes confused with CSO
  - ◆ Typically different responsibilities, but sometimes the same
- CISO protects the organizations electronic assets
- Presence of a CISO equates to an elevated importance of security in the organization
- Sometimes also responsible for privacy
- Many hold one or more security certifications
  - ◆ CISSP, CISA, CISM, etc

- Safeguard company assets, IP, and computer systems
- Identify protection goals, objectives and metrics
- Manage, develop, and implement security policy
- Prioritize security initiatives
  - ◆ May have limited budget control, but some influence
- Oversee incident response planning to data breaches
- Interact with the Auditors and sometime Law Enforcement

# What Drives the CISO

## ➤ Compliance

- ◆ SOX, GLBA, HIPPA, etc

## ➤ Survival

- ◆ Average CISO lifespan = 18 months

## ➤ \$\$\$

- ◆ Security Budgets are often flat or shrinking
- ◆ Costs spread across multiple organizations – not just IT
- ◆ Justified via economic impact
- ◆ Organization Alignment is important



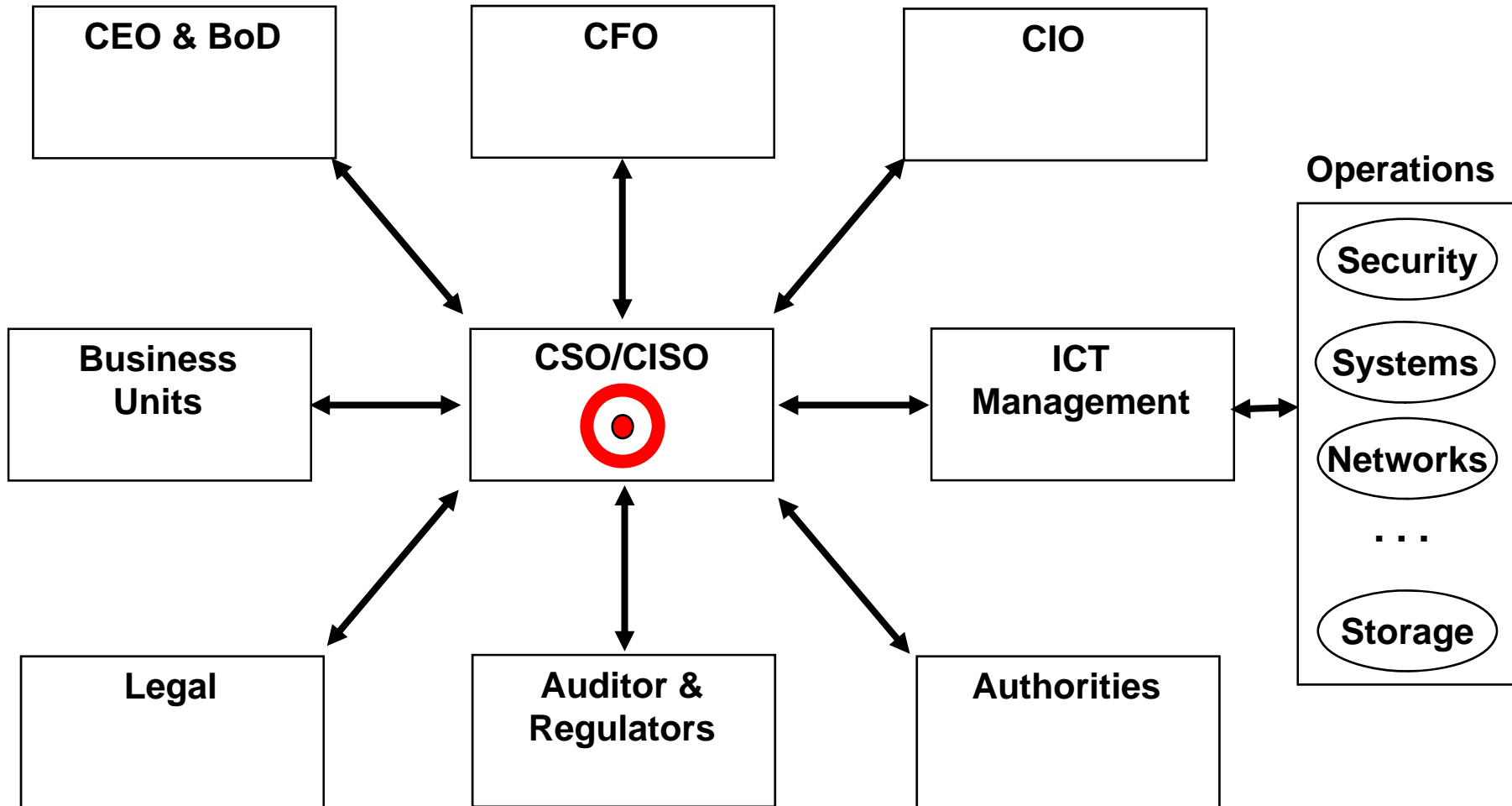
## Data Security

- Proactive
- Defense-in-depth
- Physical, technical and administrative control areas
- Preventive, detective and corrective control types

## Compliance

- Reactive
- Accountability
- Traceability
- Monitoring & Reporting
- Risk Management
- **Often the driver for security**

# Dynamic Tension



# Regulatory Drivers (Sample Domestic US)

- Sarbanes-Oxley (SOX) Act
- Gramm-Leach-Bliley Act (GLBA)
- Securities Exchange Act (SEC) Rules 17a-3 and 17a-4
- California Data Security Act (SB 1386/AB 1950)
- Health Insurance Portability & Accountability Act (HIPAA)
- DOE 10 CFR 600.153 Retention & Access Requirements for Records
- U.S. Patriot Act
- International Trafficking in Arms Regulations (ITAR)
- Food & Drug Administration (FDA): Title 21 CFR Part 11
- Homeland Security Information Sharing Act (HSISA)
- New York Reg. 173

# Regulatory Drivers (Sample International)

- European Union Data Protection Directive of 1995
- Basel Capital Accord (Basel II)
- EU Directive on Telecommunication Privacy
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australia: Commonwealth Privacy Act 1988
- Japanese Protection for Personal Information Act
- UK: Data Protection Act 1998
- New Zealand: Privacy Act 1993

# Most Critical Security Issues

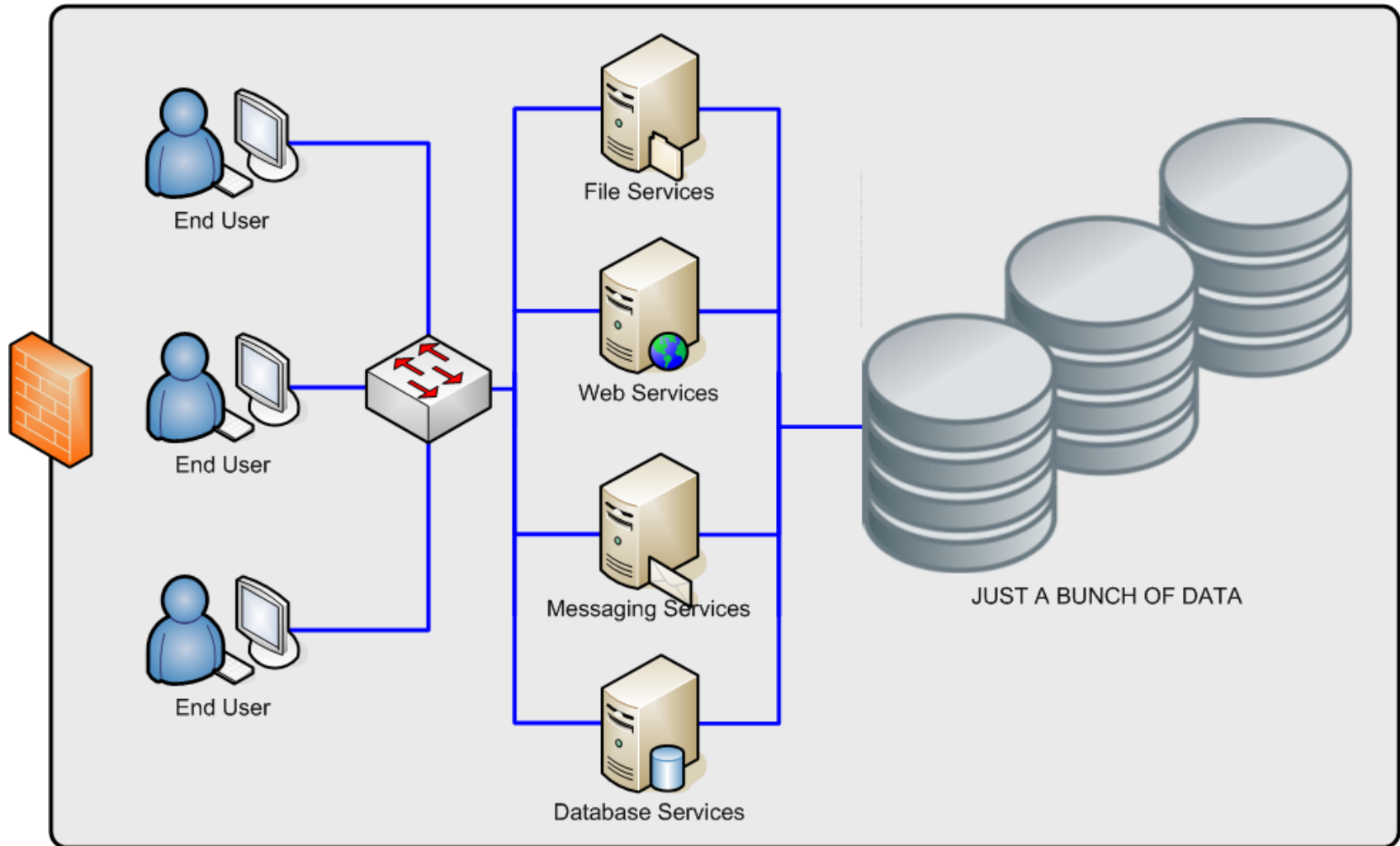
## (2008 CSI/FBI Top 10)

1. Viruses and Worms
2. Insider Abuse (e.g. Internal Network Security)
3. Unauthorized Access
4. Laptop Theft
5. Denial of Service / Instant Messaging Abuse – Tied
6. Bots
7. Theft/Loss of Customer Data
8. System Penetration
9. Financial Fraud
10. Misuse of Web Applications

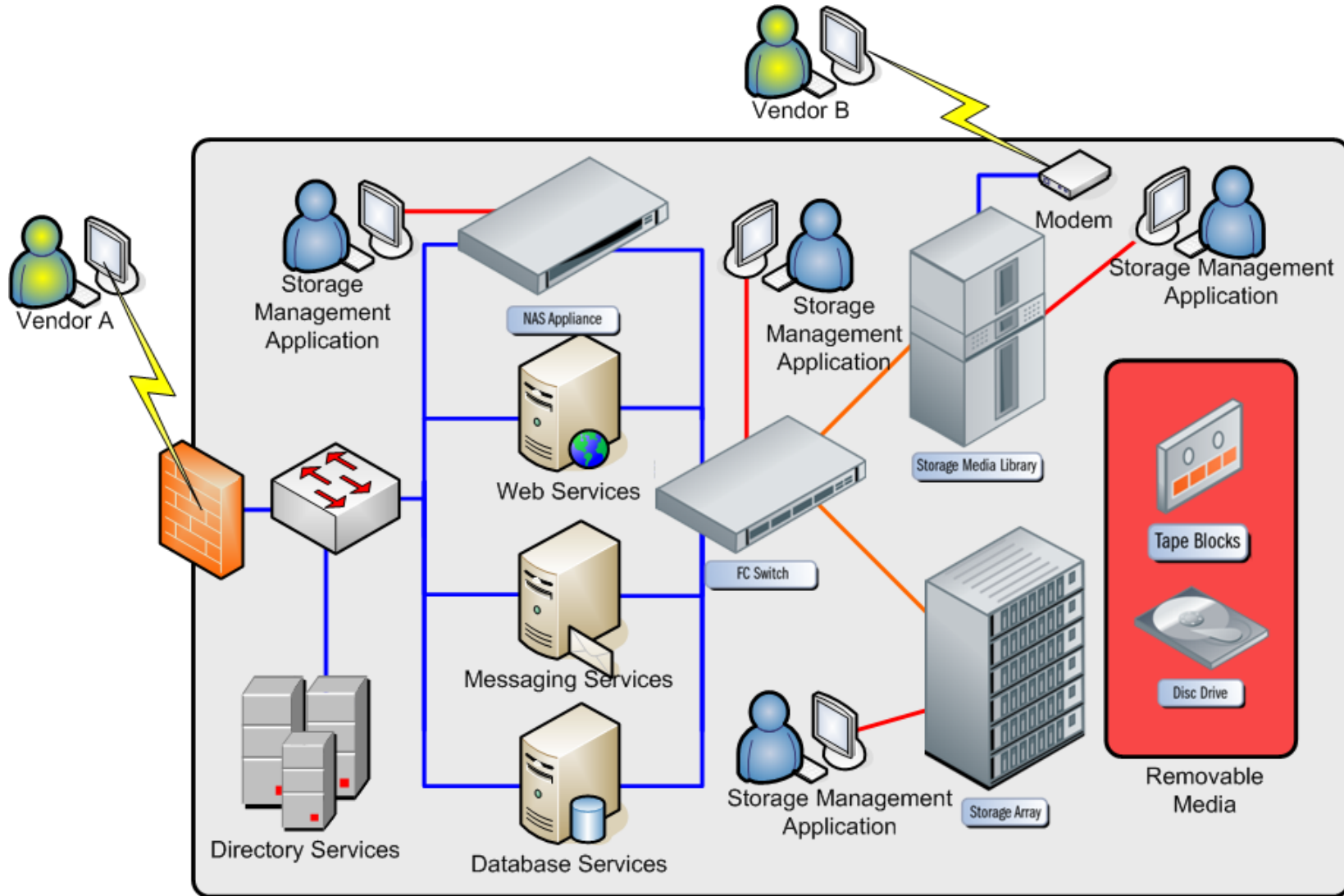
**SOURCE:** Computer Security Institute, “2008 CSI Computer Crime & Security Survey,” © 2008 by CSI, <http://www.gocsi.com>

# How the CISO Views Storage Security

# What the CISO used to see



# What the CISO sees now



# Possible Storage Attack Vectors

- **Embedded Operating Systems**
  - ◆ Security by obscurity is no longer an option
- **Storage Management Applications**
  - ◆ Web Apps, Java, Etc
- **Hosts Connected to the Fabric**
  - ◆ OS attacks
- **Removable Media**
  - ◆ Lost/Stolen Media (HDDs, Tapes, etc)
- **People**
  - ◆ Vendors requiring remote access for maintenance, etc.

# How the CISO Measures Storage Security

- Security is primarily concerned with protecting data
  - ◆ Everywhere and by Everyone
- The CISO (and his team) have limited understanding of Storage Ecosystems
- Storage components are now expected to integrate with the infrastructure
- Storage Managers (and staff) are expected to comply with all organizational security policies
- GOAL: Stay Out of the Headlines
- THE OTHER GOAL: Avoid Incarceration

# Security Frameworks

- CISO's use them to help them keep an eye on all the things they need to worry about.
- Frameworks are usually the source of internal security checklists
- Popular Security Frameworks:
  - ◆ ISO 27001
  - ◆ Federal Information Security Management Act (FISMA)
  - ◆ And many other industry relevant ones as well

# Evaluation of the Storage Ecosystem

## ➤ Secure Management Interfaces

- ◆ Accountability and Traceability
- ◆ Explicit Access Controls
- ◆ Separation of Duties

## ➤ Entitlement Review

- ◆ Who has access to what?
- ◆ Creation/Modification/Removal of Access
- ◆ Can it be managed centrally (Directory Services)

## ➤ Monitoring & Reporting

- ◆ Audit Logging
- ◆ Security Information Event Management

## ➤ Proprietary Operating Systems

- ◆ Vulnerability Management
- ◆ Vendor Security Patching

## ➤ Management Applications

- ◆ Can they integrate with existing infrastructure for:
  - > Authentication
  - > Authorization

## ➤ Maintenance Access

- ◆ HTTPS, Dial-Up, VPN
- ◆ Customer Controlled Access
- ◆ Traceability of Access and Actions Taken

# **Security & Storage: Co-existence & Partnership**

- Storage is an important element of the defense-in-depth security strategy
- Storage is now part of an organization's compliance objectives
- Storage security measures are no longer a checkbox
- Storage does not become the source of audit surprises (i.e., negative findings)

# Final Thoughts

- The weak link in the security chain is most often the human element. **Security IS a people problem!**
- Manage the risks **or** mitigate the consequences
- A holistic approach to security includes the people, the organization, governance, process and, **lastly**, technology.
- Expectations of the security program - keeping the organization out of trouble and out of the headlines, while doing it for as little money possible
- Implementing firewalls and hardening systems are not enough

- Please send any questions or comments on this presentation to SNIA: [tracksecurity@snia.org](mailto:tracksecurity@snia.org)

**Many thanks to the following individuals  
for their contributions to this tutorial.**

**- SNIA Education Committee**

**Eric Hibbard, CISSP, CISA, ISSAP, ISSEP**

**Larry Hofer, CISSP**

## ➤ SNIA Security Technical Work Group (TWG)

- ◆ **Focus:** Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
- ◆ [http://www.snia.org/tech\\_activities/workgroups/security/](http://www.snia.org/tech_activities/workgroups/security/)

## ➤ Storage Security Industry Forum (SSIF)

- ◆ **Focus:** Marketing collateral, educational materials, customer needs, whitepapers, and best practices for storage security.
- ◆ <http://www.snia.org/ssif>

- ISO/IEC 27000 Series ([www.iso.org](http://www.iso.org)) – Information security management systems
- COBIT® v4.0 ([www.isaca.org/cobit](http://www.isaca.org/cobit)) – Control Objectives for Information and related Technology
- COSO ([www.coso.org](http://www.coso.org)) – Enterprise Risk Management — Integrated Framework
- FFIEC ([www.ffiec.gov](http://www.ffiec.gov)) – FFIEC Information Technology Examination Handbook
- NIST/CSD Computer Security Resource Center ([csrc.nist.gov/publications/nistpubs](http://csrc.nist.gov/publications/nistpubs)) – Security standards for U.S. Government
- CICA ([www.cica.ca](http://www.cica.ca)) – Information Technology Control Guidelines (ITCG)
- ITIL ([www.itil.co.uk](http://www.itil.co.uk)) – ITIL Security Management

# Additional Sources of Security Information

- The CERT® Coordination Center, <http://www.cert.org>
- The SANS (SysAdmin, Audit, Network, Security) Institute, <http://www.sans.org>
- The Center for Internet Security (CIS), <http://www.cisecurity.org>
- Information Security Forum (ISF) – The Standard of Good Practice for Information Security, <http://www.isfsecuritystandard.com>
- Open Information Systems Security Group (OISSG), <http://www.oissg.org>
- Open Web Application Security Project (OWASP), <http://www.owasp.org>