



Education

# **INFORMATION SECURITY & IT COMPLIANCE**

Eric A Hibbard, Hitachi Data Systems

- The material contained in this tutorial is copyrighted by the SNIA.
  - Member companies and individuals may use this material in presentations and literature under the following conditions:
    - ◆ Any slide or slides used must be reproduced without modification
    - ◆ The SNIA must be acknowledged as 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 nor should be construed as legal advice or opinion. If you need legal advice or legal opinion please contact an attorney.
  - The information presented herein represents the Author's personal opinion and current understanding of the 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.**

## ➤ Information Security & IT Compliance

- ◆ In times past, the sole yardstick of an Enterprise's IT department was business application availability. Today, however, a multitude of both internal and external requirements are applied to IT. IT Policies are now driven by a need for compliance with national and international legislation on data protection and privacy (e.g. HIPPA, Sarbanes-Oxley, EU Data Protection Directive), various standardized and industry-developed security frameworks (e.g. ISO 27002, COBIT, PCI DSS), auditing standards, and even risk management requirements derived from insurance coverage. New IT yardsticks include not only demonstrating compliance to the requirements but also such items as e-discovery response times, intrusion detection tests, and data retention periods.
- ◆ This session will leverage the SNIA Storage Security Best Current Practices (BCPs) addressing data security compliance, understanding risks, and utilizing event logging. Commonly encountered requirements will be identified, and approaches to creating IT Policies and collecting evidence will be described..

# Agenda

- Introduction
  - ◆ Why all this attention?
  - ◆ Security Versus Compliance
- Information Security
- IT Compliance
- SNIA Best Current Practices (BCPs)
- IT Compliance from the Top Down
- Summary

# Why All This Attention?

***“There are more and more of these breaches, because information is money. The more computerized we are the more true that is. It’s not that hard to turn a piece of information into cash, by opening a fake cell phone account or a fake credit card account.”***

Gail Hillebrand

Senior Attorney, Consumers Union

# Why All This Attention?

- Now not only time is money, apparently
- For 100+ years the financial departments of companies have had to:
  - ◆ Follow defined processes
  - ◆ Keep “legal quality” logs of those processes
  - ◆ Have both processes & logs regularly audited by an outside entity
- Because information is now money, the same sort of controls are now applied to the processing of information

# Security Versus Compliance



## Data Security

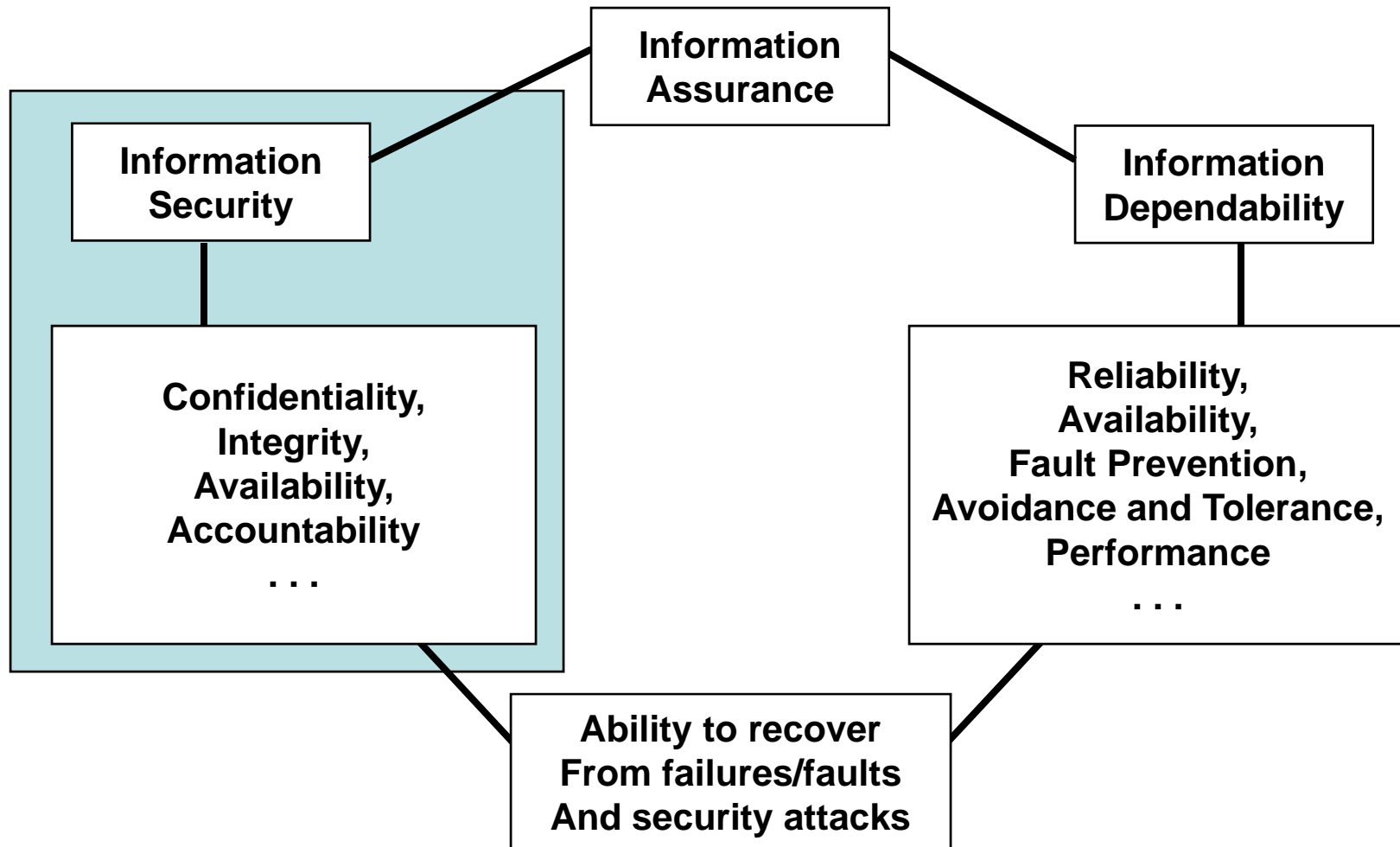
- Proactive
- Defense-in-depth
- Physical, technical and administrative control areas
- Preventive, detective and corrective control types

## Compliance

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

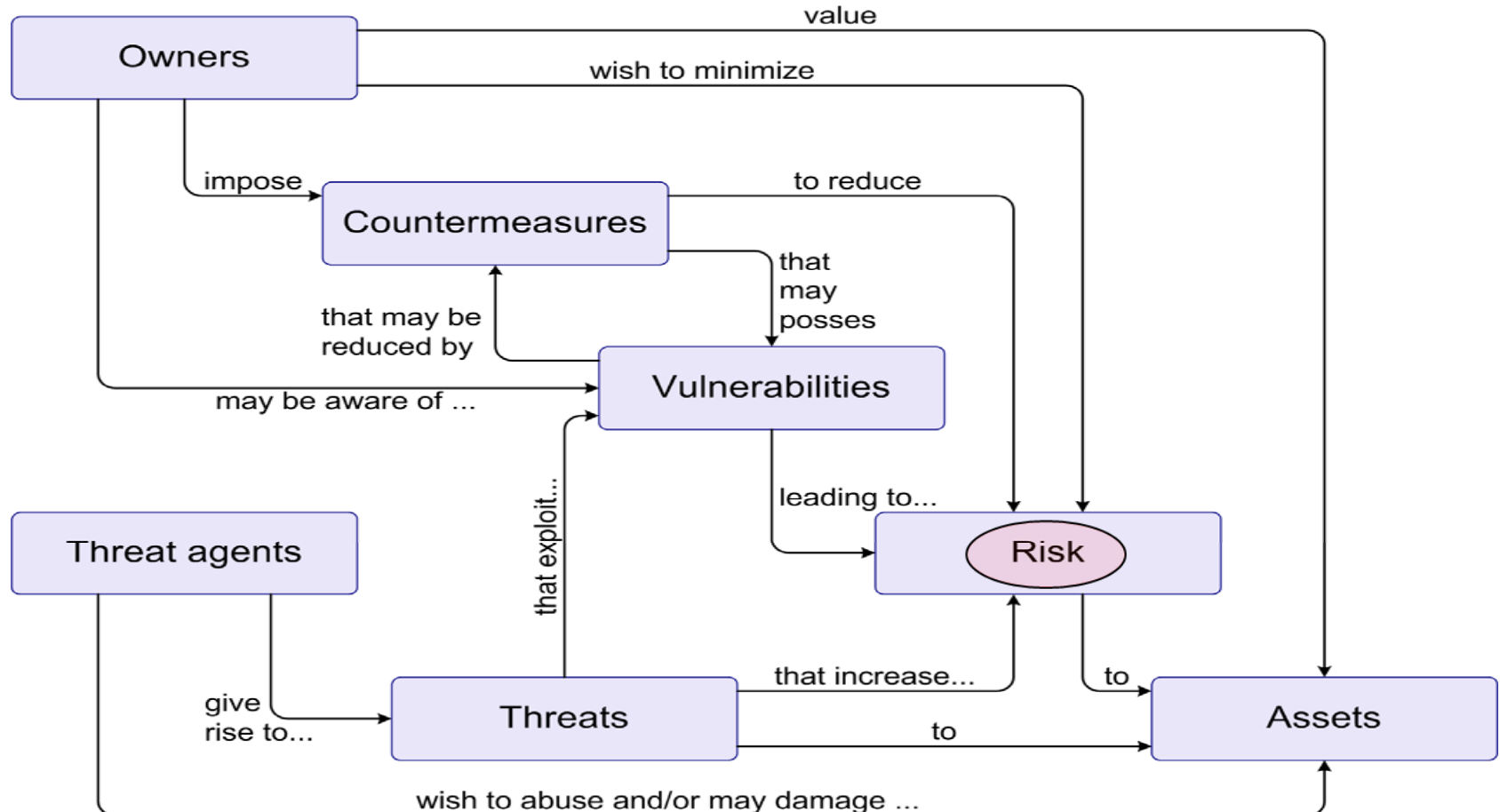
# A Few Words on Information Security

# Information Assurance



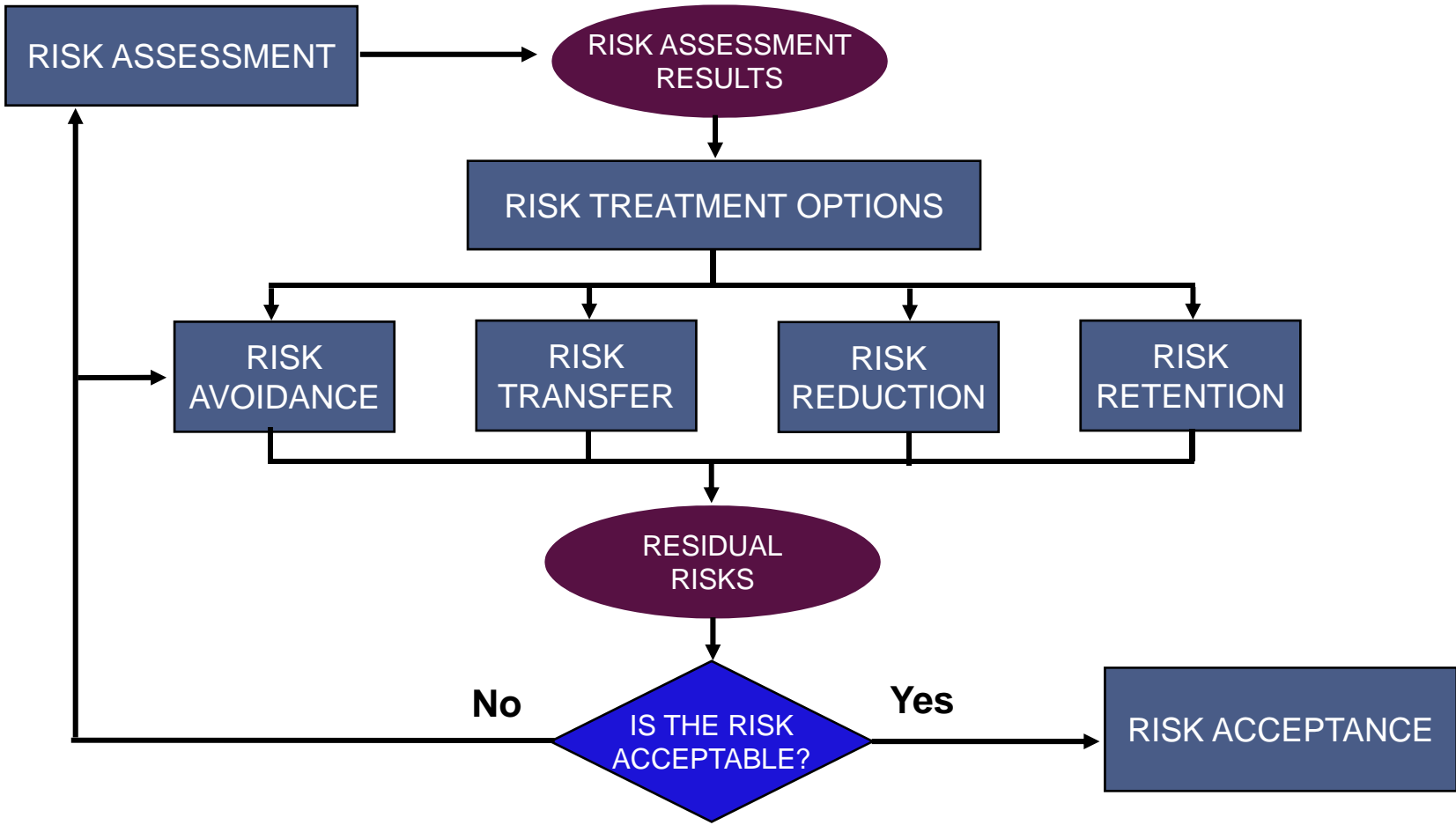
**Source:** *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.

# The Security “Big Picture”



**SOURCE:** ISO/IEC 15408-1:2005, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, Common Criteria v2.3, <http://www.iso.ch>

# Risk Treatment Decision-making Process

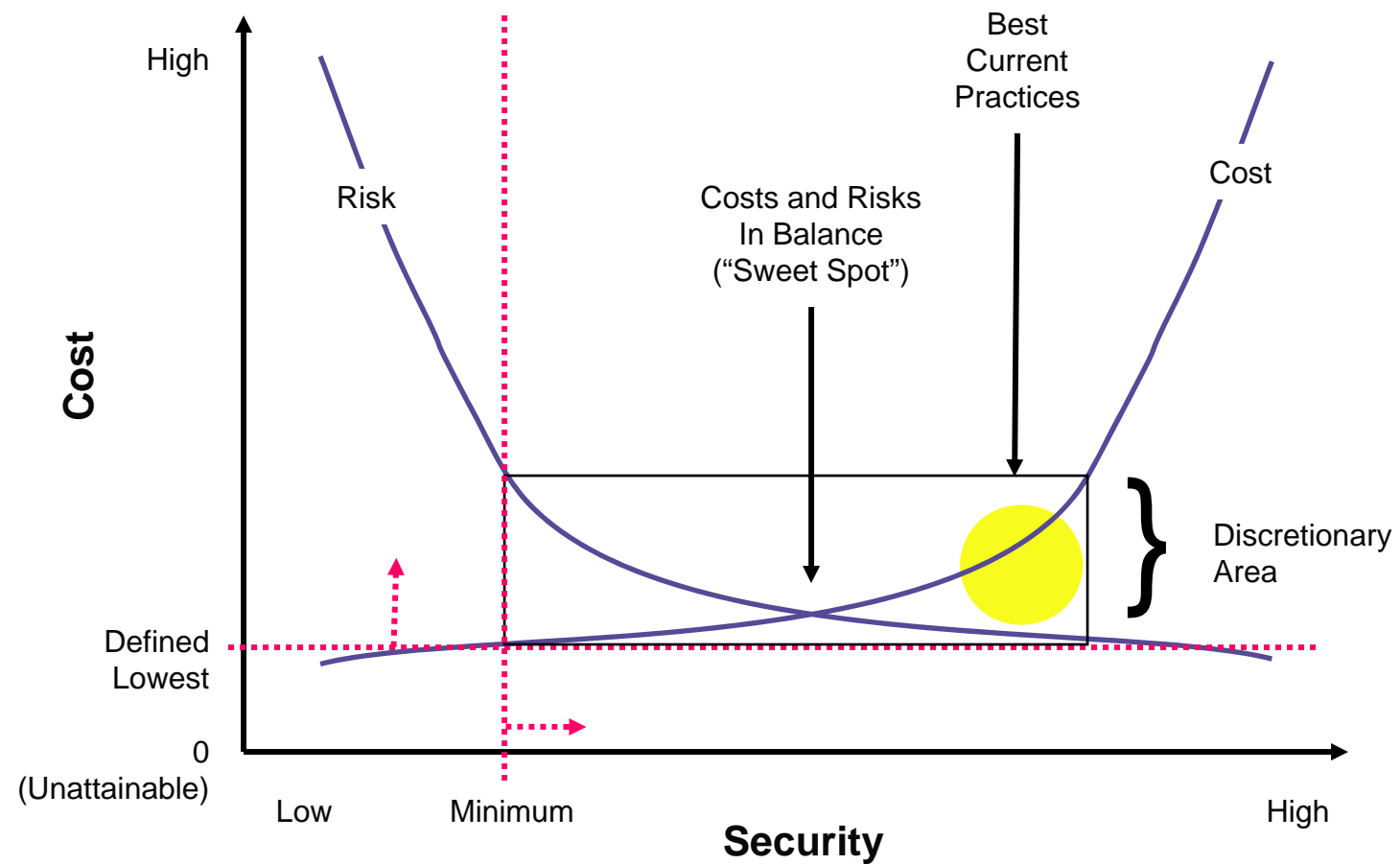


**BASED ON:** ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, <http://www.iso.ch>

# Common Security Frameworks

- ISO/IEC 17799:2005 *The Code of Practice for Information Security Management* & ISO/IEC 27001:2006 *Information Security Management - Requirements*
- IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT) Version 4.0
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission
- Federal Financial Institutions Examination Council (FFIEC)
- National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems (Special Publication 800-53)
- Canadian Institute of Chartered Accountants (CICA), Information Technology Control Guidelines (ITCG)
- UK Office of Government Commerce (OGC), Information Technology Infrastructure Library (ITIL), Security Management

# Balancing Cost & Security



© 1996 – 2000 Ray Kaplan All Rights Reserved

Source: Ray Kaplan, CISSP, *A Matter of Trust*, Information Security Management Handbook, 5<sup>th</sup> Edition. Tipton & Krause, editors.

# IT Compliance

# Definition of Terminology

## Compliance:

The state of being in accordance with the relevant Government authorities and their requirements.

Conformance with a standard, law, or specification that has been clearly defined.

Acting according to company defined policies and procedures.



# 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

# Standard of Care

- **Due Diligence** – responsibility one has to investigate and identify issues
  - ◆ Are the risks managed appropriately
  - ◆ Are the “sensitive” digital assets protected appropriately
  - ◆ Are the “critical” digital assets protected appropriately
- **Due Care** – doing something about the findings from *due diligence*
  - ◆ Risk treatment passes the “giggle” test
  - ◆ Data protection and data security measures are reasonable (i.e., in line with those of peers)
  - ◆ Can we prove that security measures were active at the time of an incident
- **ROI = Risk of Incarceration**

# It's Simple, Right?



# It's Simple, Right?

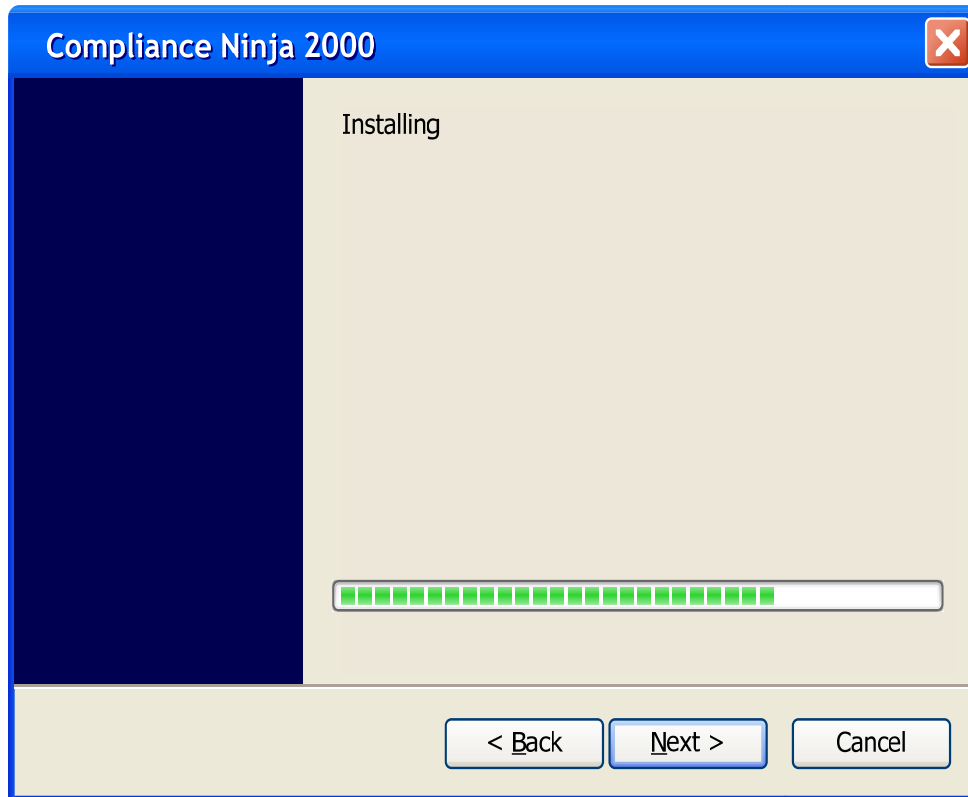
Compliance Ninja 2000

Choose your regulation.

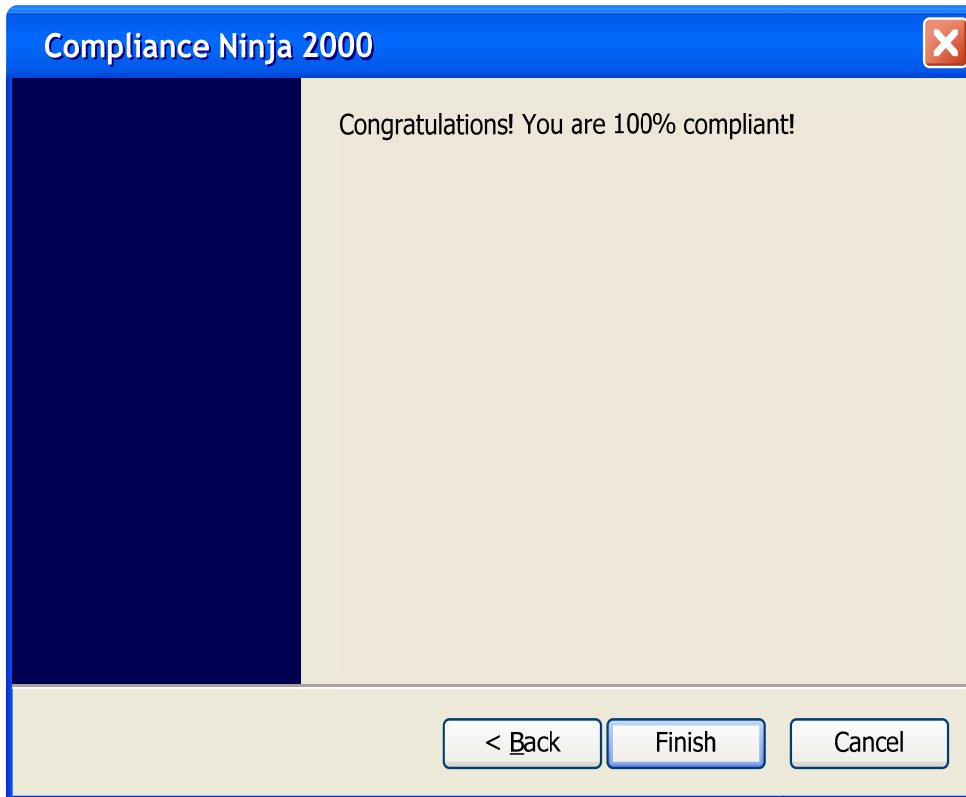
- HIPAA
- GLBA
- Sarbanes-Oxley

< Back   Next >   Cancel

# It's Simple, Right?



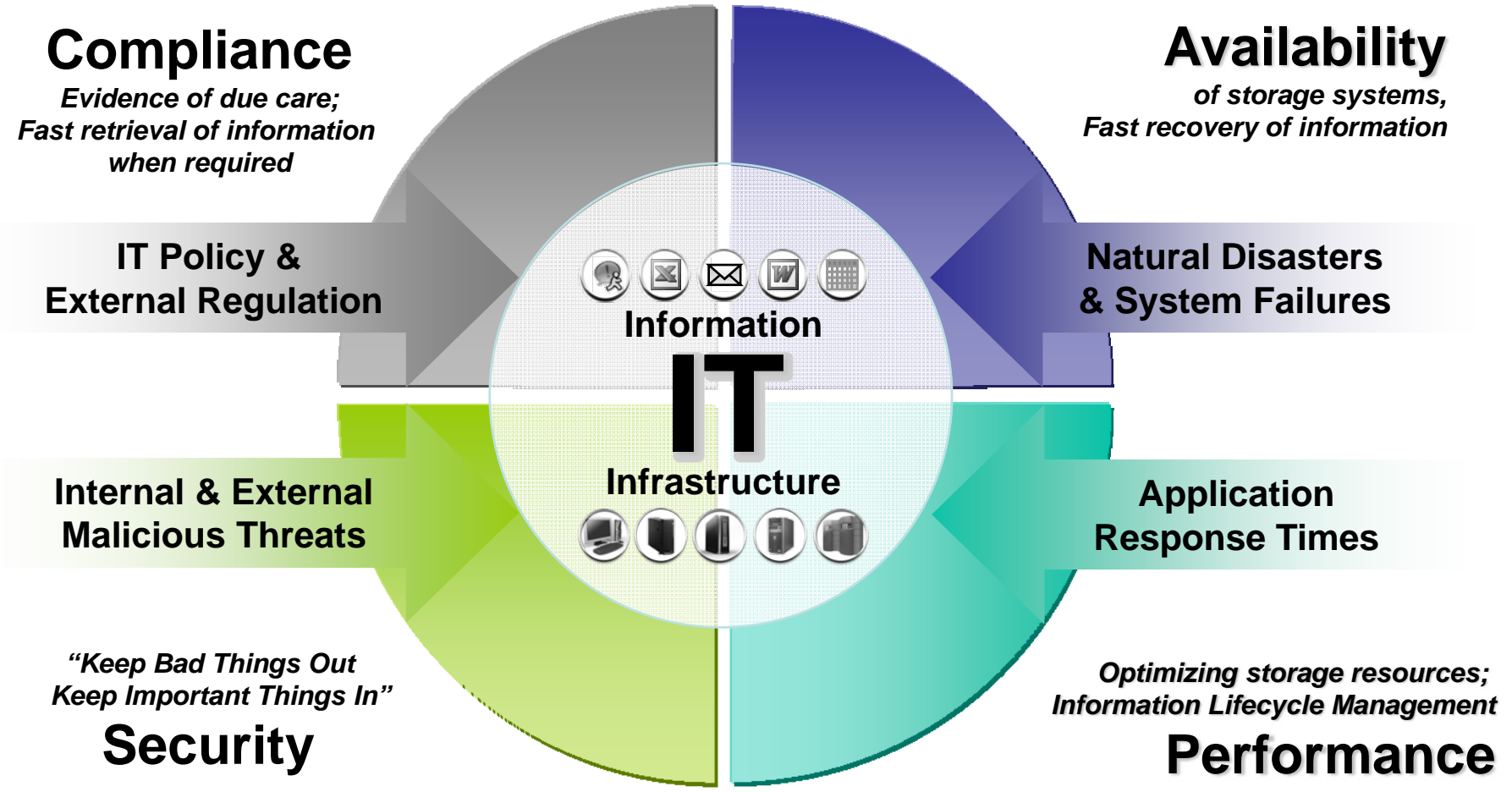
# Too Good to be True



# Not That Simple!

- Cannot be as simple as installing a single piece of software
  - ◆ Although automation is a key part of making this problem tractable
- The entire IT infrastructure has to be addressed
- Education & training is a must
- Defined and repeatable processes are the key
- And compliance is only one part....

# .... Of The 4 Dimensions of IT Risk



# Approach

- IT compliance doesn't have to be driven by legal & government requirements
  - ◆ There's value in IT being able to demonstrate compliance to existing company procedures
  - ◆ IT risk management in general can be as well be driven by internal business requirements as externally
- Existing standards & audit guidelines can be used as a basis for IT risk management activities
  - ◆ SNIA has developed Best Current Practices (BCPs) on that basis
  - ◆ Creating controls & processes NOW based on those definitions will likely save you considerable time & effort in the future

# **SNIA Technical Proposal – Storage Security Best Current Practices (BCPs)**

# BCPs Background

- Storage Security BCPs available from
  - ◆ [http://www.snia.org/forums/ssif/programs/best\\_practices/](http://www.snia.org/forums/ssif/programs/best_practices/)
- BCPs created from review of existing standards definitions
  - ◆ ISO/IEC 27001 & 27002 (formerly 17799)
  - ◆ ISACA Audit Guidelines
  - ◆ FFIEC Information Technology Examination Handbook
  - ◆ PCI Security Standards Council's Data Security Standard
- In many cases there's existing information on how specific legal & government requirements map to these documents
  - ◆ Thus they define a set of “common approaches”
  - ◆ This view “from the top down” will be addressed in last section of the tutorial

# Storage Security BCP Structure

- Core (applicable to all storage systems)
  - ◆ General Storage Security
  - ◆ Storage System Security
  - ◆ Storage Management Security
- Technology-specific
  - ◆ Network Attached Storage
  - ◆ Block-based IP Storage
  - ◆ Fibre Channel Storage
  - ◆ Encryption for Storage
  - ◆ Key Management for Storage
  - ◆ Long-term Information Security

# Relevant BCPs

- BCPs described in more detail in the following slides
  - ◆ General Storage Security
    - › Address Data Security Compliance
  - ◆ Storage System Security
    - › Understand the Exposures
    - › Utilize Event Logging
- Other BCPs that have some relevance
  - ◆ General Storage Security
    - › Implement Appropriate Service Continuity
  - ◆ Storage Management
    - › Tightly Control Access and Privileges

# Address Data Security Compliance

## ➤ Accountability

- ◆ No shared accounts, uses roles when possible
- ◆ Log all attempted (successful and unsuccessful) management events and transactions

## ➤ Traceability

- ◆ Ensure logged event/transaction data contains sufficient application and/or system detail to clearly identify the source & a user
- ◆ When appropriate, treat log records as evidence (chain of custody, non-repudiation, authenticity, etc.)

## ➤ Risk Management

- ◆ Enumerate and classify the information assets
- ◆ Perform risk assessments & analysis
- ◆ Implement risk treatment (avoid, transfer, reduce, or accept)
- ◆ Regularly test controls and review processes

# Address Data Security Compliance

- Detect, Monitor, and Evaluate
  - ◆ Monitor the audit logging events and issue appropriate alerts
- Information Retention & Sanitization
  - ◆ Implement appropriate data retention, integrity & authenticity measures
  - ◆ Sanitize data upon deletion, repurposing or decommissioning of hardware
- Privacy
  - ◆ Consider both data and metadata (e.g., search results)
    - › Assume a least privilege posture whenever possible
  - ◆ Prevent unauthorized disclosure
- Legal
  - ◆ Ensure that the use of data deduplication does not conflict with data authenticity requirements
  - ◆ Ensure data and media sanitization mechanisms do not violate preservation orders
  - ◆ Ensure proper chain of custody procedures are followed when evidentiary data

# Understand the Exposures

## ➤ Perform Vulnerability Assessments

- ◆ Perform security scans against the elements of the storage ecosystem to understand the security posture of the technology
  - › Use known default passwords, test field & service accounts
- ◆ Maintain awareness of advertised vulnerabilities in platforms supporting management applications

## ➤ Maintain Security of Systems

- ◆ Install security patches and fixes in a timely fashion
- ◆ Consider upgrading applications/software when end-of-life products contain exploitable, but unpatchable vulnerabilities

## ➤ Monitor for Zero-day Events

- ◆ Integrate intrusion detection/prevention technology

# Utilize Event Logging

- Include Storage Systems & Devices in Logging Policy
  - ◆ Policy should include evidentiary expectations (authenticity, chain of custody) how & when retained etc.
- Employ External Event Logging
  - ◆ Collect events from all sources in a single repository
  - ◆ Use a common, accurate time source
  - ◆ Log events to one, and preferably multiple, external servers (preferably syslog).
  - ◆ Log events on a transactional basis (no buffering)

# Utilize Event Logging

- **Ensure Complete Event Logging**
  - ◆ Log both in-band and out-of-band activity
  - ◆ Log many kinds of events
    - > Good list of suggestions in the BCPs
  - ◆ Each entry should include:
    - > Timestamp (date and time)
    - > Severity level (
    - > Source of the log entry (distinguishing name, IP address, etc.)
    - > Description of the event
- **Use automation to correlate audit log records to identify significant security events**

# IT Compliance from the Top Down

# From Regulations to ...

Regulation

**SOX 404(a)(2)** [The Commission shall prescribe rules requiring each annual internal control report, which shall]...contain an assessment, at the end of each most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Framework

**COBIT DS5.19** Malicious Software Prevention, Detection and Correction - Malicious software, management should establish a framework of detective and corrective control measures, and occurrence response and reporting.

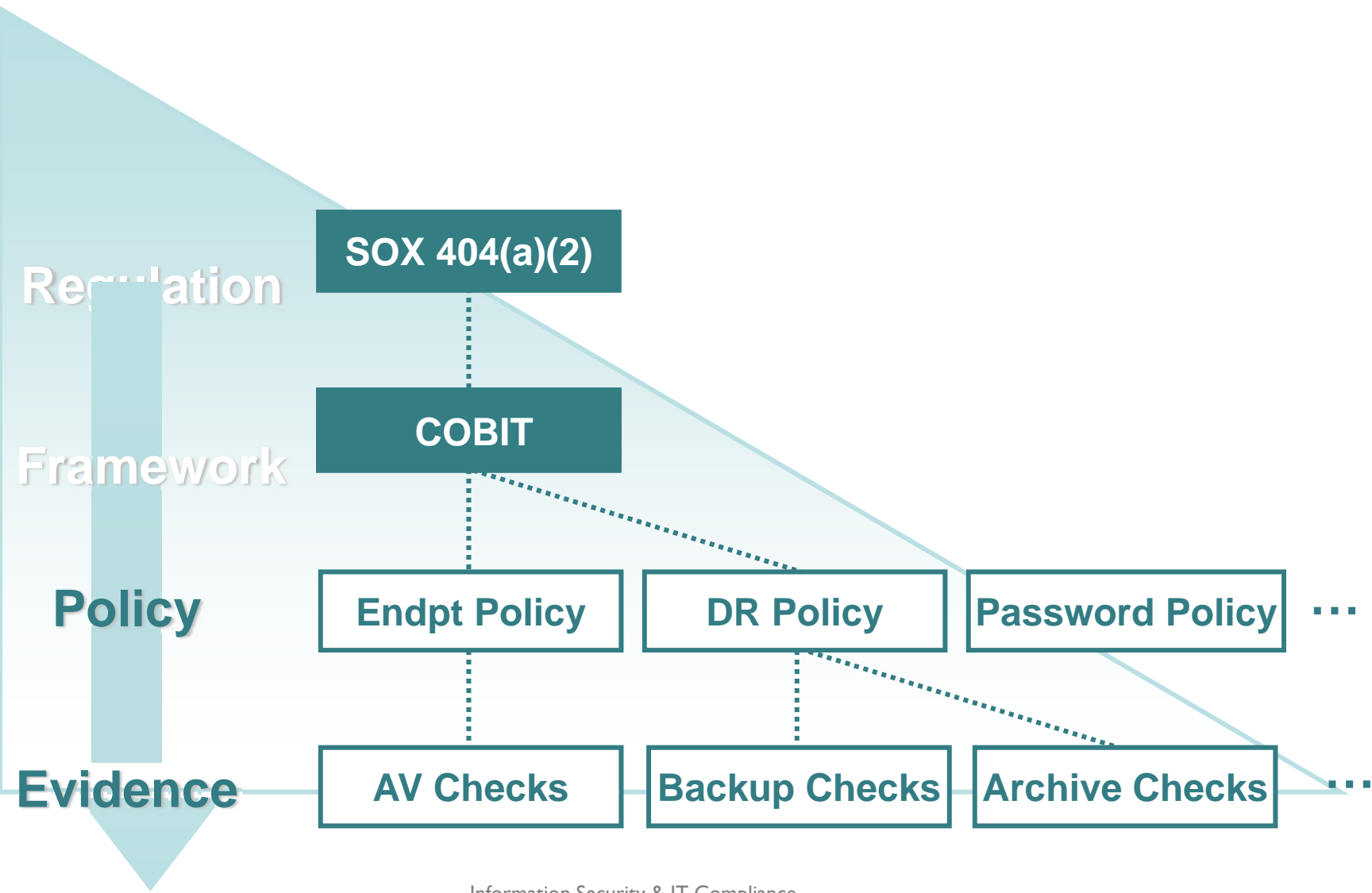
Policy

**Endpoint Protection Malware Policy**  
**Endpoint Policy** Software Is Installed  
Software Is Running  
Anti-Virus & Firewall Software Is Up To Date

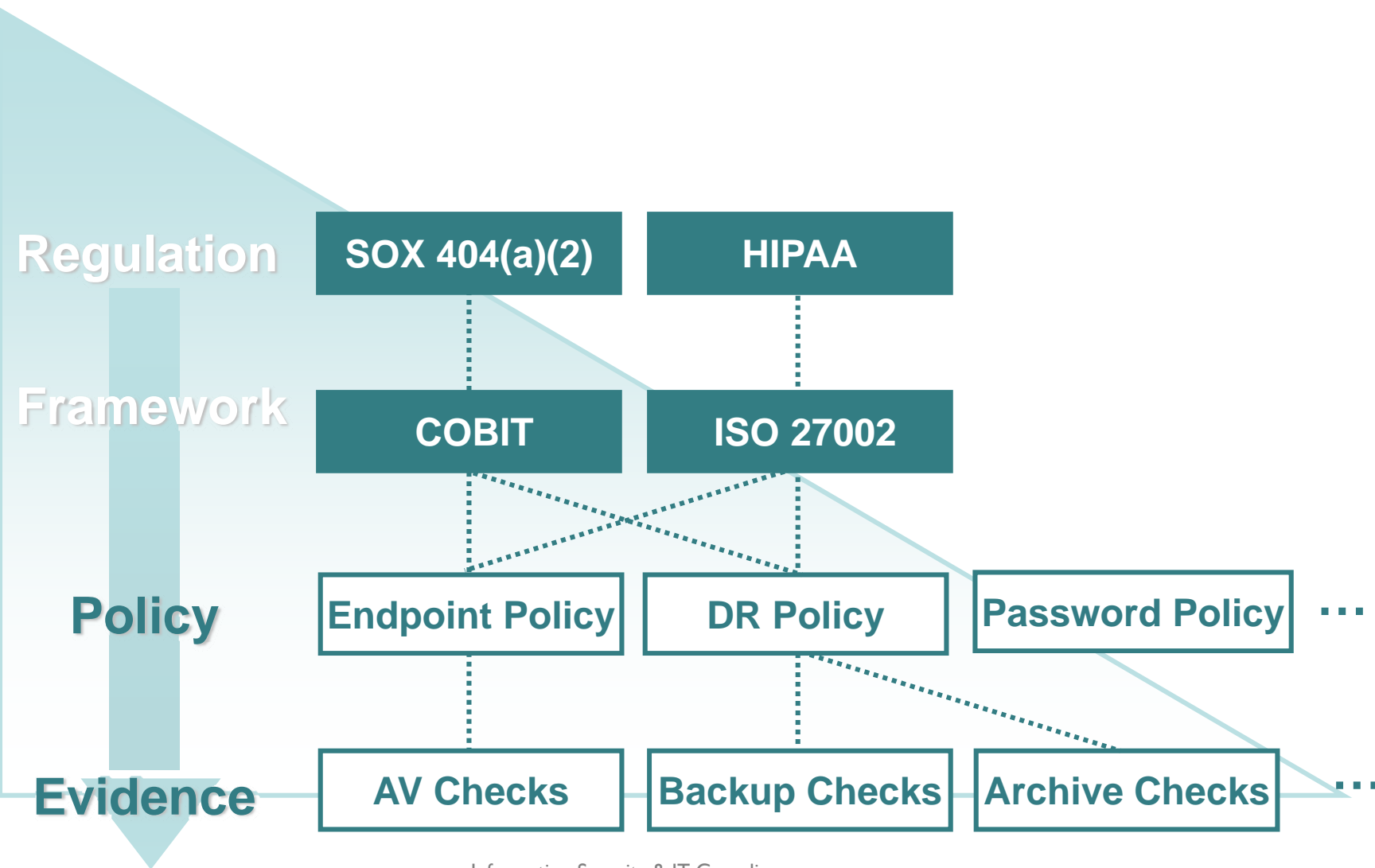
**AV Checks**

Evidence

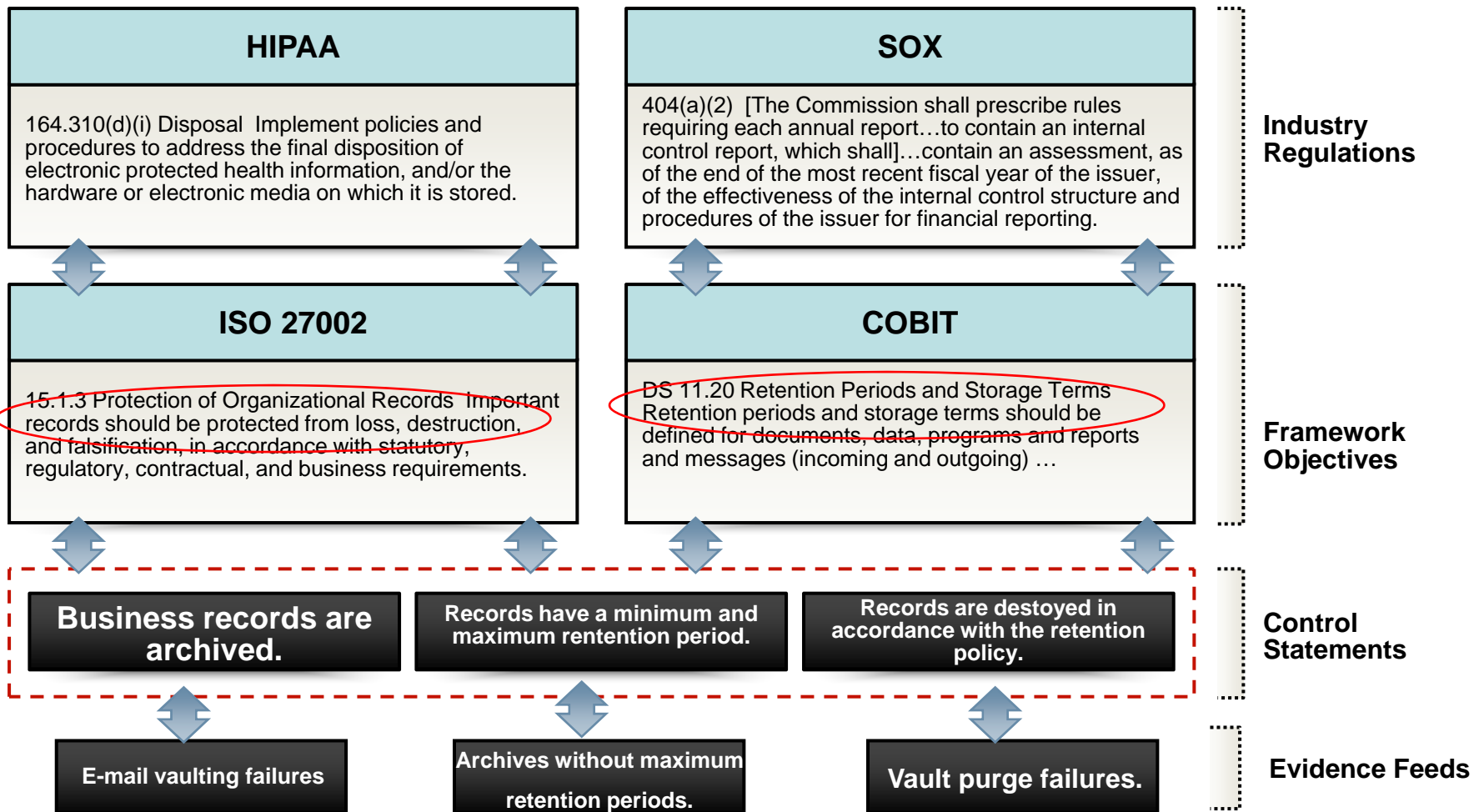
# ... Multiple Policies that ...



# Show Coverage across Regulations



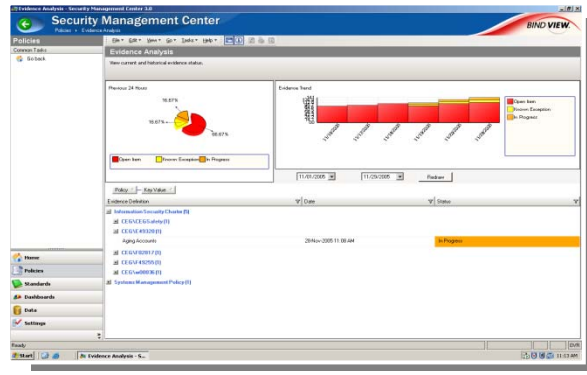
# Map Policies to IT controls - Archiving



# Management of IT Compliance

Regulation

- SOX View
- HIPAA View
- COBIT View
- ISO 27002 View



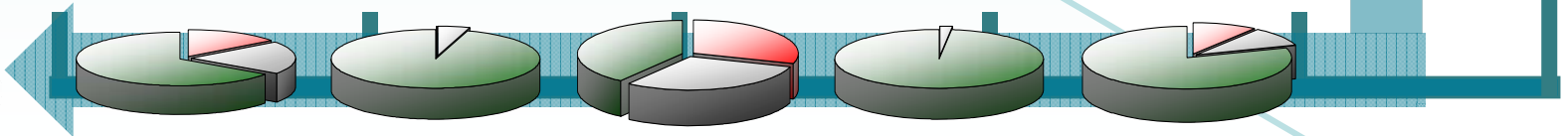
Framework



Policy

- NAC
- Archive
- Backup
- Anti-Virus
- Usr Access
- Sys Config ...

Evidence



# Focus On IT Controls

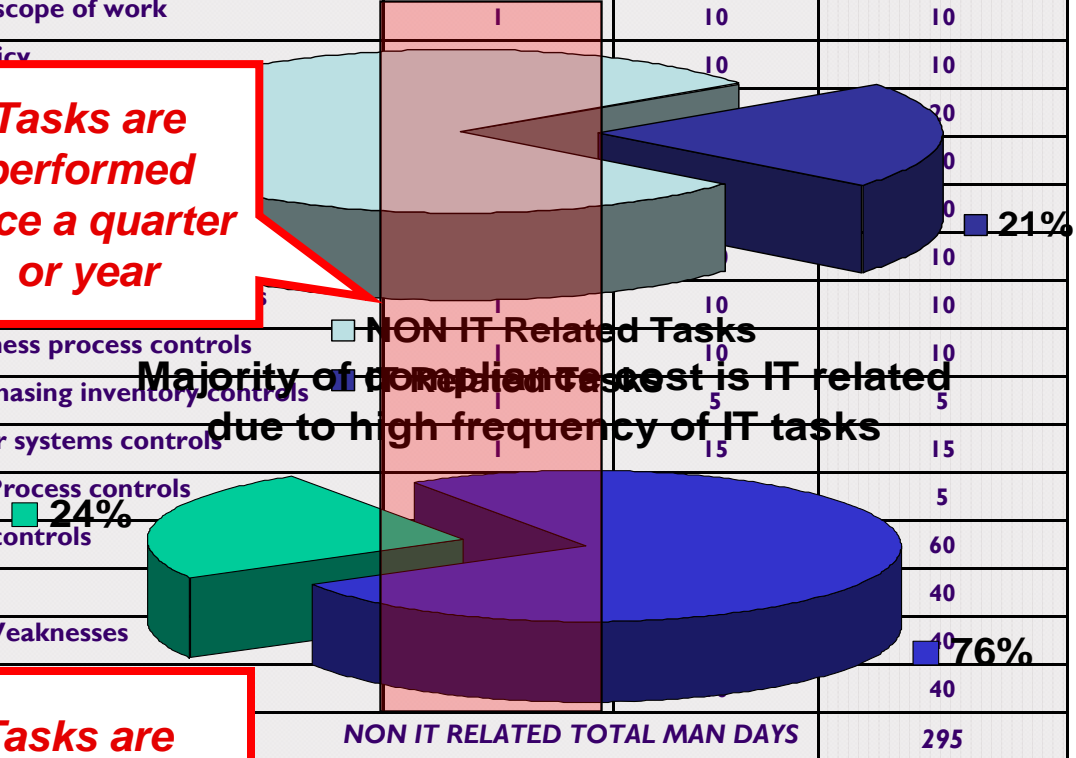
TYPE	TASKS	FREQUENCY / YEAR	COST (Days)	TOTAL COST / YEAR (Days)
NON IT Related	Create compliance scope of work	1	10	10
	Establish/review policy	1	10	10
	Project Management	1	20	20
	Design/Review	1	20	20
	Design/Review	1	20	20
	Design/Review	1	10	10
	Design/Review	1	10	10
	Design/Review business process controls	1	10	10
	Design/Review purchasing inventory controls	1	5	5
	Design/Review other systems controls	1	15	15
	Design/Review HR Process controls	1	5	5
	Implement/update controls	1	60	60
	Test controls	1	40	40
	Evaluate Material Weaknesses	1	40	40
	Submit Executive Summary	1	40	40
<b>NON IT RELATED TOTAL MAN DAYS</b>				<b>295</b>
IT Related	Design/Review	4	10	40
	Run It Controls	52	10	520
	Disseminate	52	2	104
	Remediation	52	5	260
	<b>IT RELATED TOTAL MAN DAYS</b>			

Majority of compliance tasks are not related to IT

Tasks are performed once a quarter or year

Majority of compliance cost is IT related due to high frequency of IT tasks

Tasks are performed every week



# Key to success – Frequent Auditing

## MORE FREQUENT AUDITING TRANSLATES INTO BETTER SECURITY AND COMPLIANCE RESULTS

Success Factors	Leaders (10%)	The Rest (90%)
Freq of internal audits	21 days	8 Months
IT time on compliance	33%	24%
IT budget on security	10.4%	7.0%
# of overall deficiencies	20	40
# of significant deficiencies	2	13

Leaders are ~6x better because they do more audits...  
 ...But they spend ~50% more because of lack of automation

Source: ITpolicycompliance.com

# The reality – the To Do List

- Assess your industry sector's regulatory requirements
  - ◆ In collaboration with corporate legal & the business units
- Define, document, and disseminate policies
  - ◆ Utilize software and/or templates to create policies
  - ◆ Maximize commonality across all business units
- Implement and manage controls
  - ◆ Map policies to IT Controls
  - ◆ Use as much automation as possible today
    - Ad hoc tools & spreadsheets end up costing more money!
- Audit and improve process in a controlled environment
  - ◆ Start with self-audits before external ones
- Report results and demonstrate compliance internally or to external auditors

# Final Thoughts

# Summary

- IT Risk Management is an essential component of business effectiveness
  - ◆ More than Information Security
  - ◆ More than Compliance (both internal & external)
  - ◆ A process, not a project
  - ◆ Requires a holistic approach to managing the entire IT infrastructure
  - ◆ Education & training are key aspects
  - ◆ Logging all relevant information is vital
- The process **MUST** have a significant degree of automation to be tractable
  - ◆ Single approach across an entire enterprise
  - ◆ Start with few most important controls first and build over time
  - ◆ Use common tools rather than ad hoc ones
  - ◆ Exploit efficiencies of scale

# Security Framework Sources

- 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 **SNIA**

- 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>

- 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, ISSMP, ISSEP  
Andrew Nielsen, CISSP, CISA, ISSAP, ISSMP  
Chris Parker  
Larry Hofer CISSP  
Ray Kaplan, CISSP**

**Frank Bunn  
Roger Cummings  
Blair Semple, CISSP-ISSEP  
Chris Lionetti**