Education

INFORMATION SECURITY & IT COMPLIANCE

Frank Bunn, Symantec
Roger Cummings, Symantec

SNIA Legal Notice

- 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.

Abstract

- 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, along with a host of metrics. IT Policies are now driven by a need for compliance with national and international legislation on information security (e.g. HIPPA, Sarbanes-Oxley), various standardized and industry-developed regulatory frameworks (e.g. ISO 17799, COBIT), auditing standards, and even risk management requirements derived from insurance coverage. IT metrics 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 describe SNIA Best Practices 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 that enable appropriate metrics to be used to demonstrate compliance will be described.

Notice

- The authors are NOT attorneys, and nothing in this presentation is intended to be nor should be construed as legal advice or opinion. If you need legal advice or a legal opinion, please contact an attorney
- The information presented herein represents the authors' personal opinion and current understanding of the issues involved. The authors, Symantec, and SNIA do NOT assume any responsibility or liability for damages arising out of any reliance on or use of this information

Agenda

- Introduction
  - Why all this attention?
  - It's simple, right?.....
  - Not that simple!
  - The four dimensions of IT Risk Management
  - Terminology
  - Approach
- SNIA-developed 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."

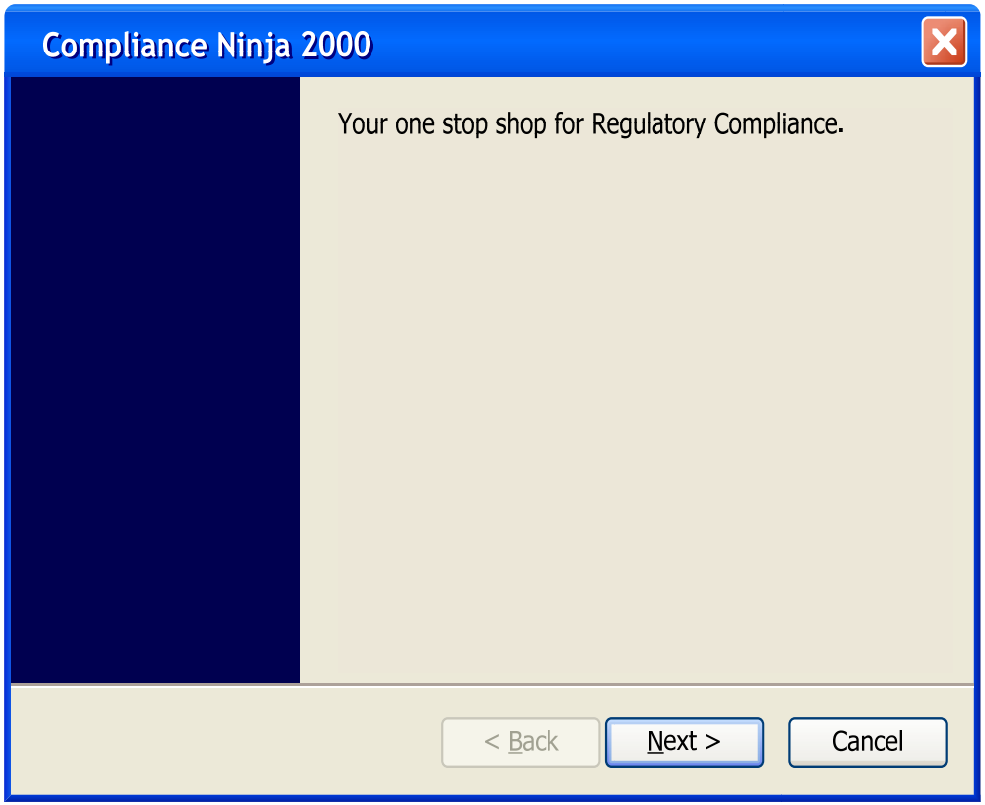
Gail Hillebrand

Senior Attorney, Consumers Union

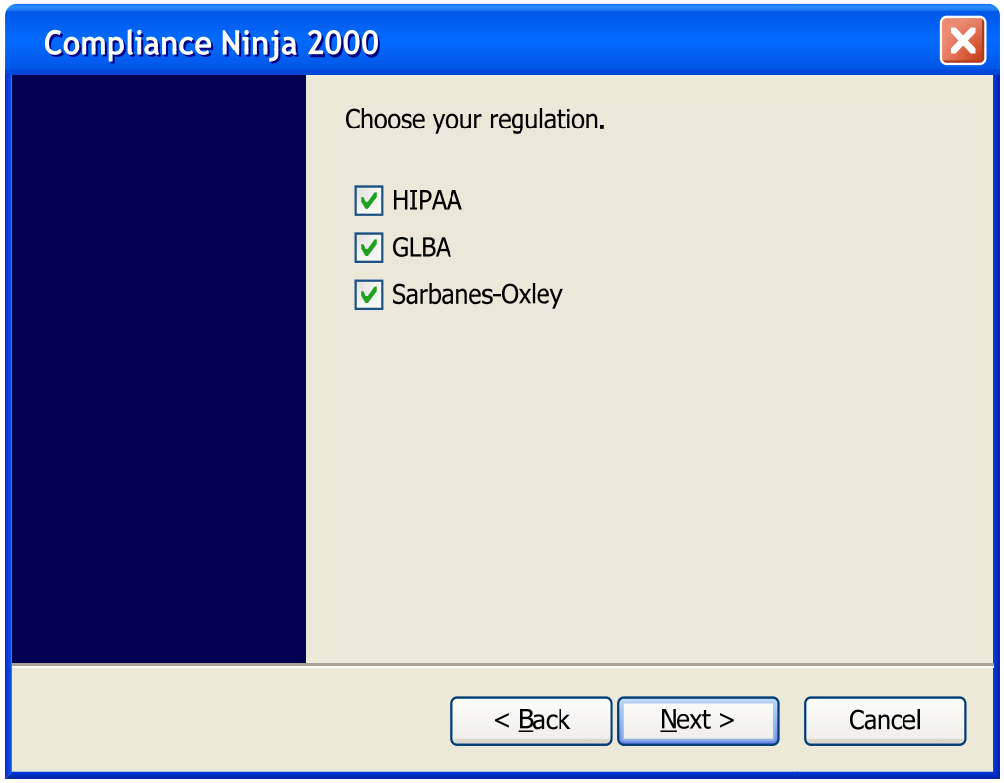
Why All This Attention?

- 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

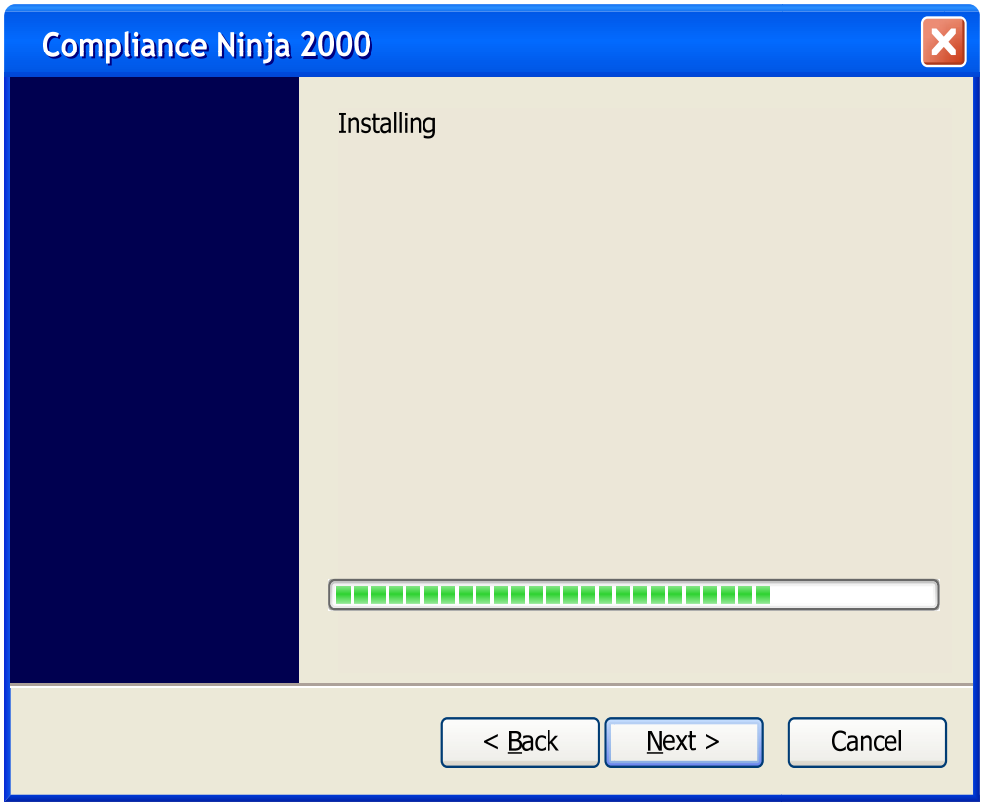
It's Simple, Right?



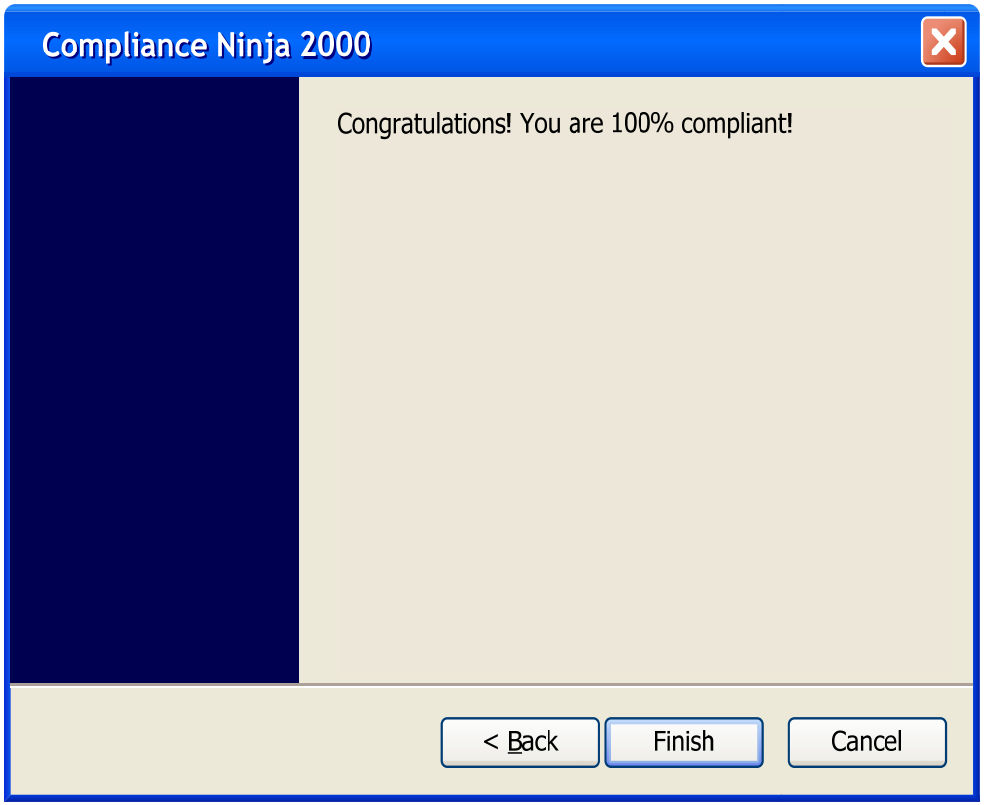
It's Simple, Right?



It's Simple, Right?



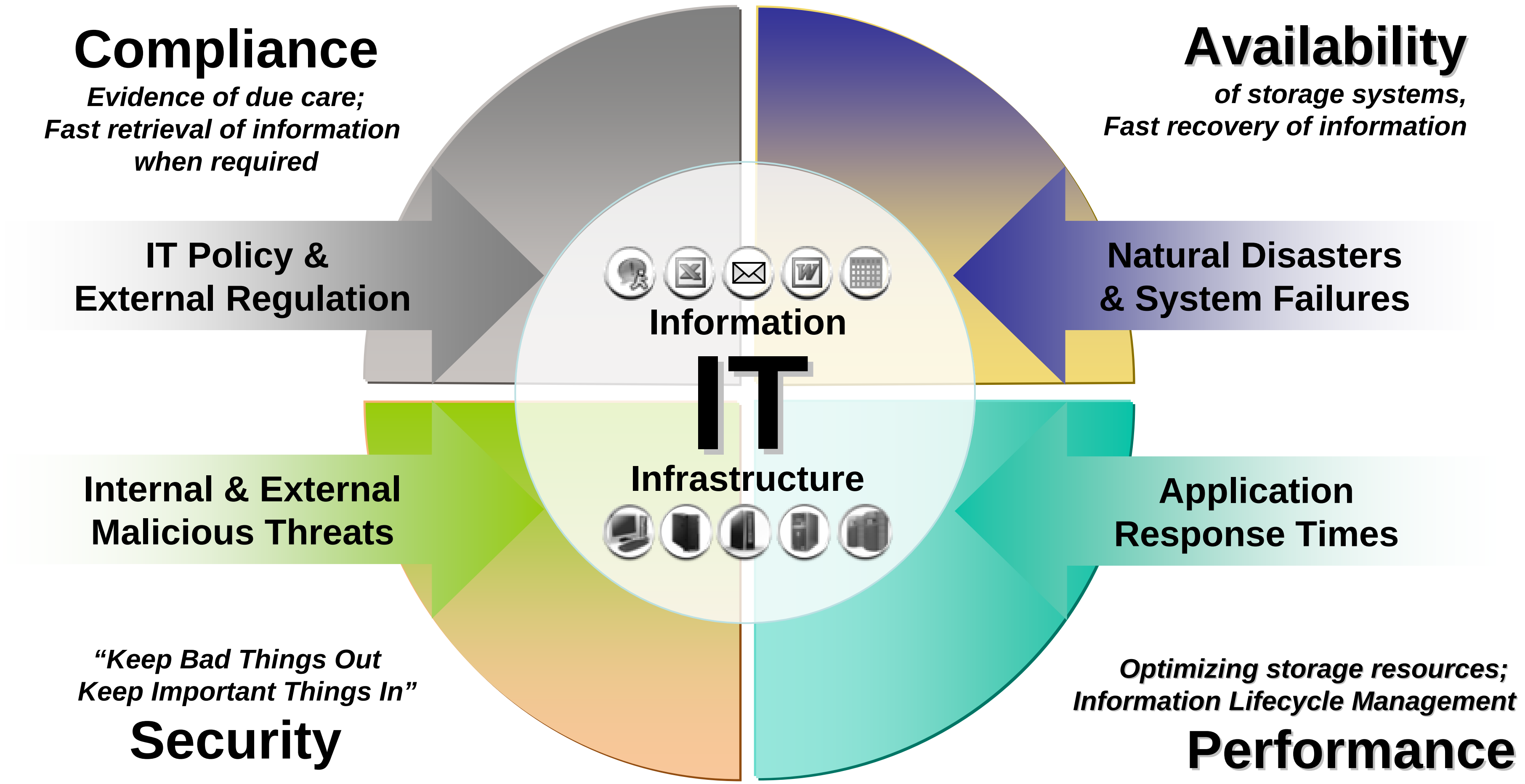
Too Good to be True



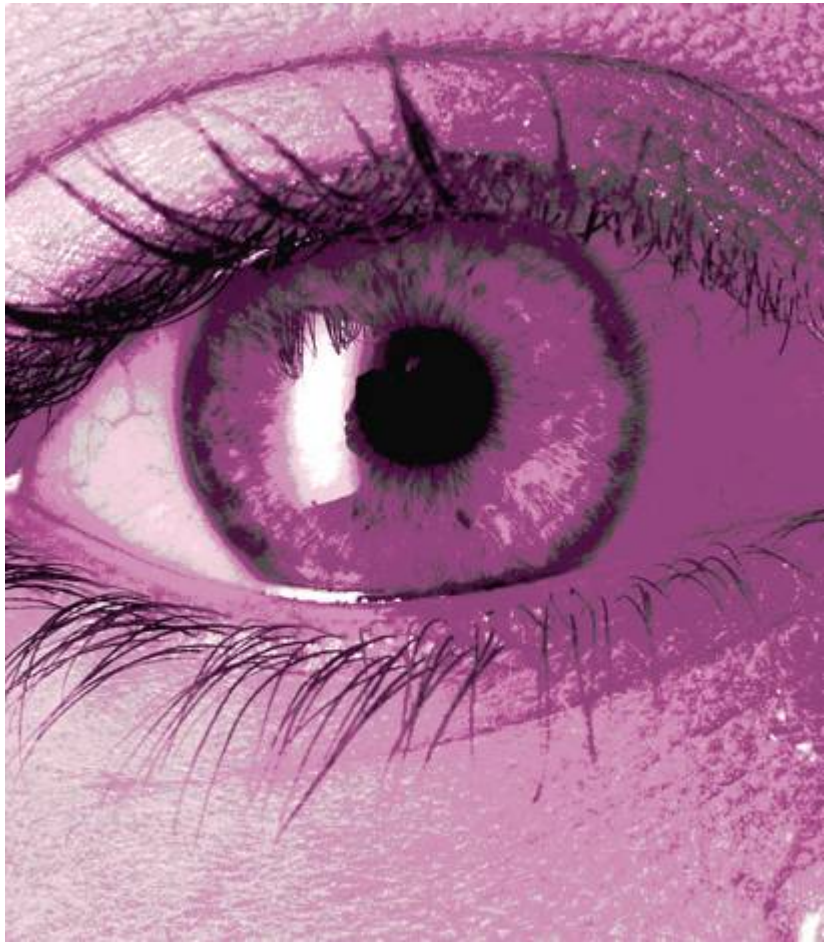
Not That Simple!

- 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



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.

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

Agenda

- Introduction
- SNIA-developed Best Current Practices (BCPs)
  - Introduction
  - Storage Security BCP structure
  - Relevant BCPs
    - Address Data Security Compliance
    - Understand the exposures
    - Utilize Event Logging
- IT Compliance from the top down
- Summary

Introduction

- Storage Security BCPs available from
  - http://www.snia.org/forums/ssif/programs/best_practices/
- BCPs created from review of existing standards definitions
  - ISO/IEC 27001 & 17799 (Now 27002)
  - ISACA Audit Guidelines
  - 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 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
  - Archive 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.)
- Detect, Monitor, and Evaluate
  - Monitor the audit logging events and issue appropriate alerts

Address Data Security Compliance

- 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

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

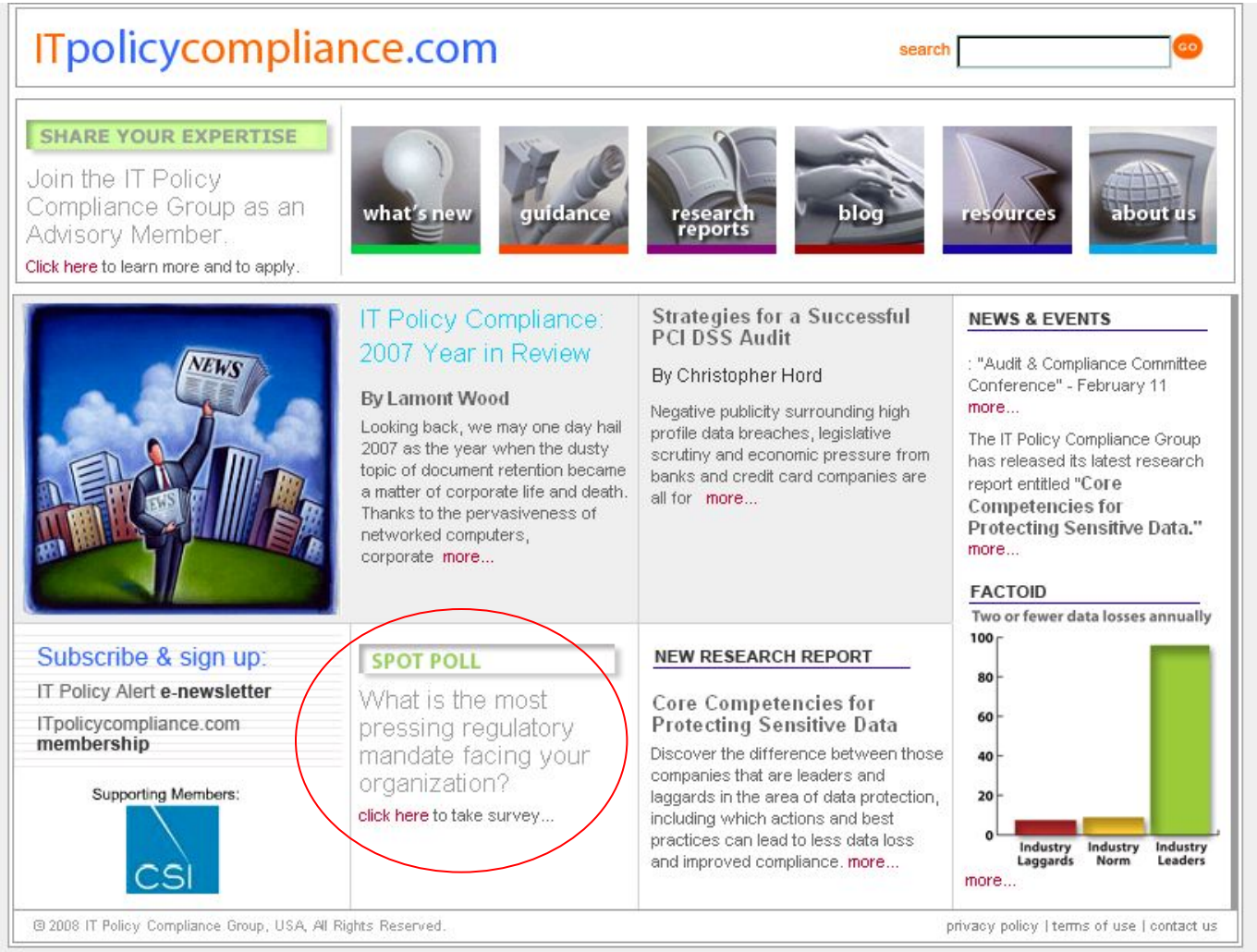
- Ensure Complete Event Logging
  - Log both in-band and out-of-band activity
  - Log many kinds of events
    - Good list of suggestions in the BCPs
  - Each entry should include:
    - Timestamp (date and time)
    - Severity level (
    - Source of the log entry (distinguishing name, IP address, etc.)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

Why automation??

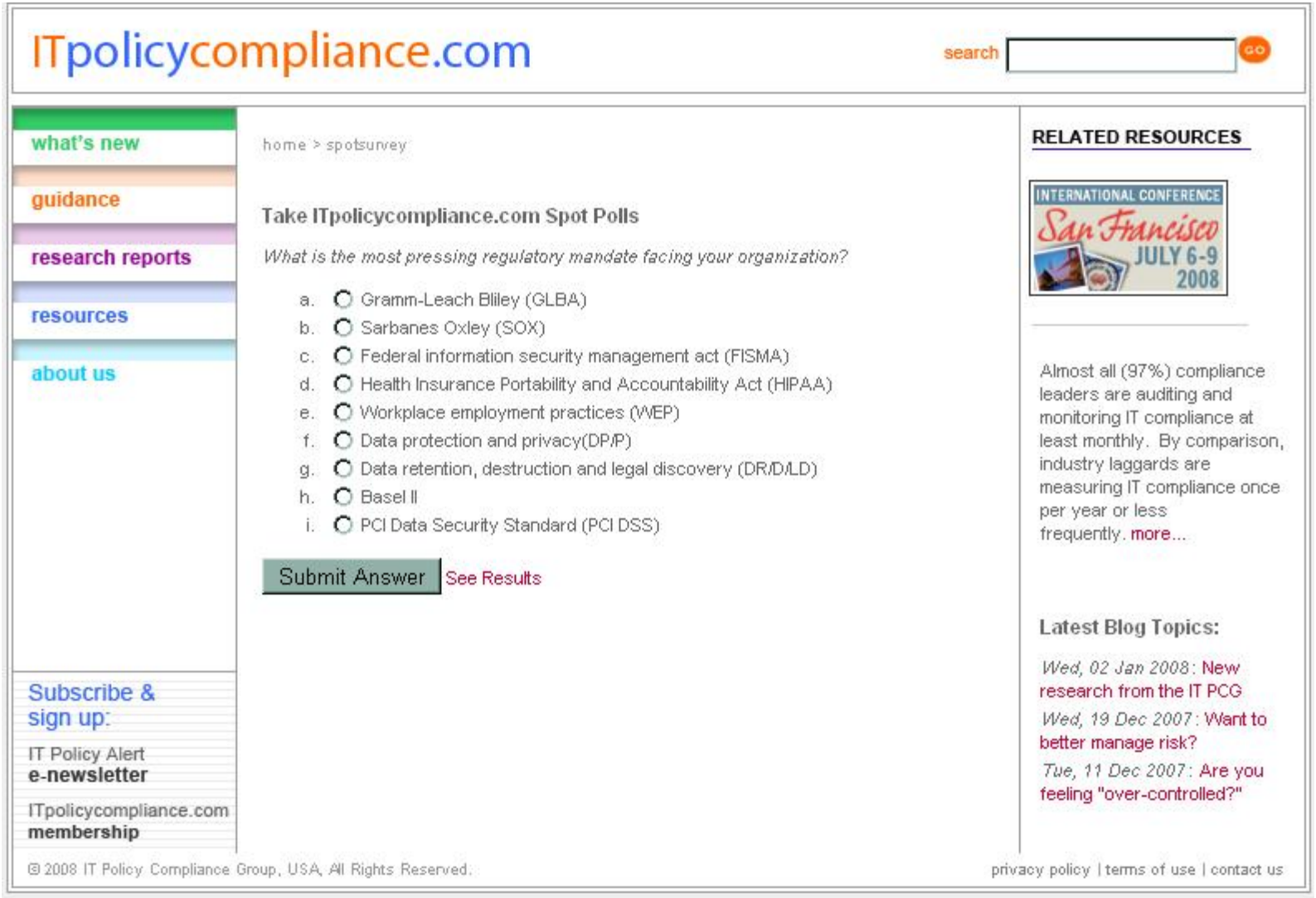
Agenda

- Introduction
- An Information Security Architecture
- SNIA-developed Best Current Practices
- IT Compliance from the Top Down
  - The Top Challenges
  - From Regulations … to Policies .. to Controls
  - The To-Do list
- Summary

The Top Challenges



The Top Challenges



ITpolicycompliance.com

search GO

what's new
guidance
research reports
resources
about us

home > spotsurvey

Take ITpolicycompliance.com Spot Polls

What is the most pressing regulatory mandate facing your organization?

a. Gramm-Leach Bliley (GLBA)
b. Sarbanes Oxley (SOX)
c. Federal information security management act (FISMA)
d. Health Insurance Portability and Accountability Act (HIPAA)
e. Workplace employment practices (WEP)
f. Data protection and privacy(DP/P)
g. Data retention, destruction and legal discovery (DR/D/LD)
h. Basel II
i. PCI Data Security Standard (PCI DSS)

Submit Answer See Results

Subscribe & sign up:
IT Policy Alert **e-newsletter**
ITpolicycompliance.com **membership**

RELATED RESOURCES

INTERNATIONAL CONFERENCE San Francisco JULY 6-9 2008

Almost all (97%) compliance leaders are auditing and monitoring IT compliance at least monthly. By comparison, industry laggards are measuring IT compliance once per year or less frequently. more...

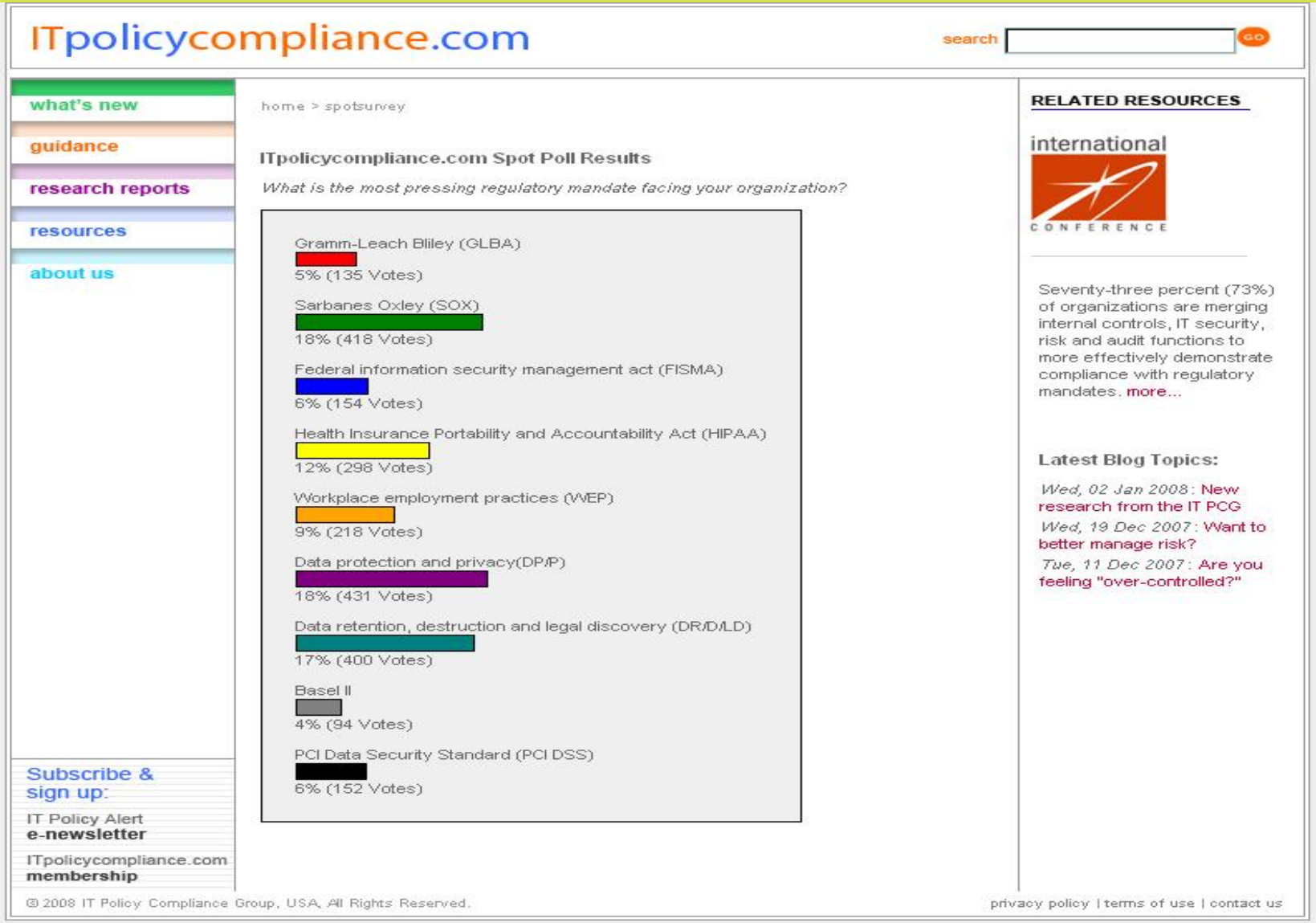
Latest Blog Topics:

Wed, 02 Jan 2008: New research from the IT PCG
Wed, 19 Dec 2007: Want to better manage risk?
Tue, 11 Dec 2007: Are you feeling "over-controlled?"

© 2008 IT Policy Compliance Group, USA, All Rights Reserved.

privacy policy | terms of use | contact us

The Top Challenges



ITpolicycompliance.com

search GO

what's new
guidance
research reports
resources
about us

home > spotsurvey

ITpolicycompliance.com Spot Poll Results

What is the most pressing regulatory mandate facing your organization?

Gramm-Leach Bliley (GLBA)
5% (135 Votes)

Sarbanes Oxley (SOX)
18% (418 Votes)

Federal information security management act (FISMA)
6% (154 Votes)

Health Insurance Portability and Accountability Act (HIPAA)
12% (298 Votes)

Workplace employment practices (WEP)
9% (218 Votes)

Data protection and privacy(DP/P)
18% (431 Votes)

Data retention, destruction and legal discovery (DR/D/LD)
17% (400 Votes)

Basel II
4% (94 Votes)

PCI Data Security Standard (PCI DSS)
6% (152 Votes)

RELATED RESOURCES

international CONFERENCE

Seventy-three percent (73%) of organizations are merging internal controls, IT security, risk and audit functions to more effectively demonstrate compliance with regulatory mandates. more...

Latest Blog Topics:

Wed, 02 Jan 2008: New research from the IT PCG
Wed, 19 Dec 2007: Want to better manage risk?
Tue, 11 Dec 2007: Are you feeling "over-controlled?"

Subscribe & sign up:
IT Policy Alert **e-newsletter**
ITpolicycompliance.com **membership**

© 2008 IT Policy Compliance Group, USA, All Rights Reserved.

privacy policy | terms of use | contact us

From Regulations to …

Regulation

Framework

Policy

Evidence

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

SOX 404(a)(2)

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

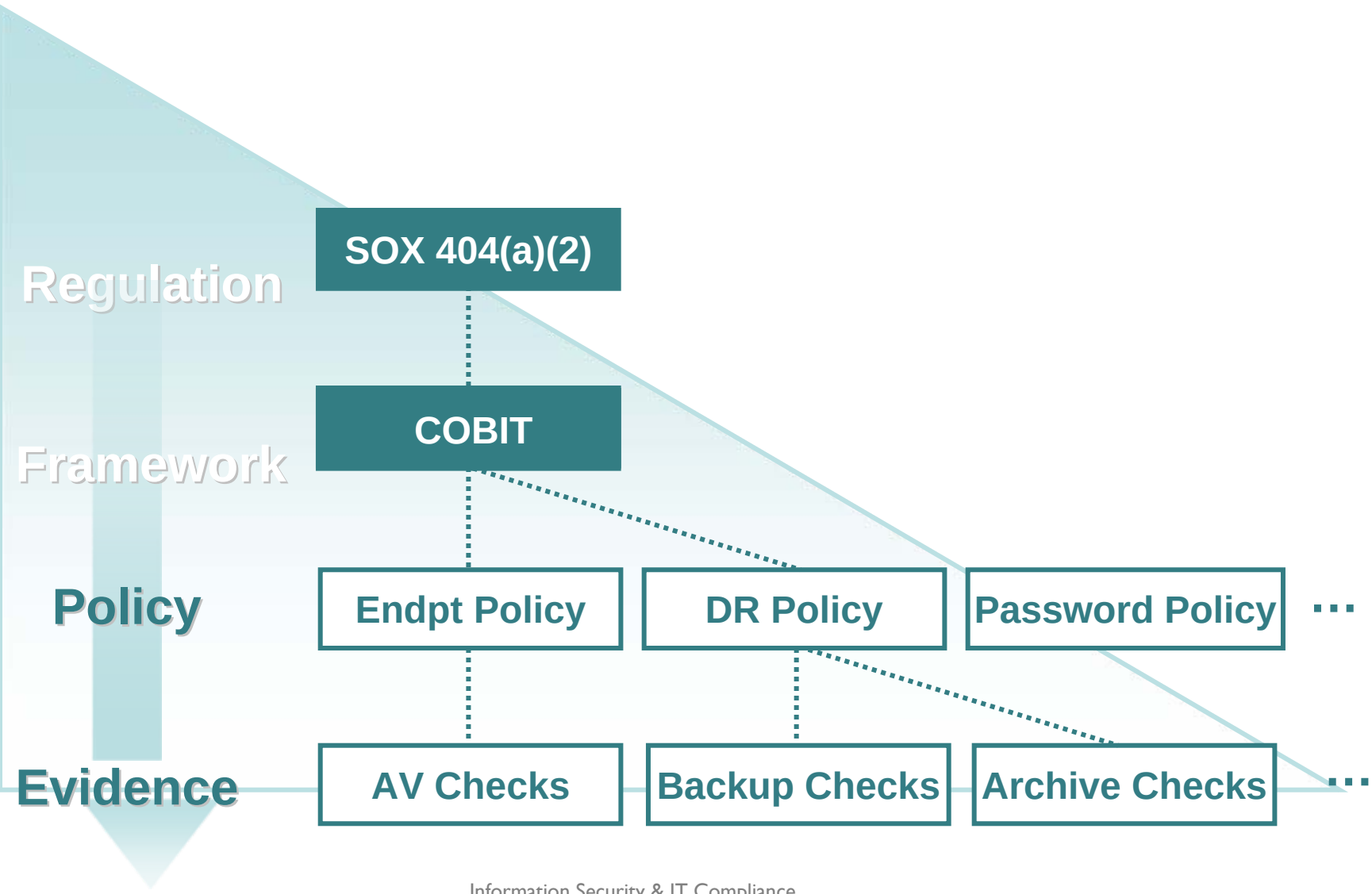
COBIT DS5.19

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

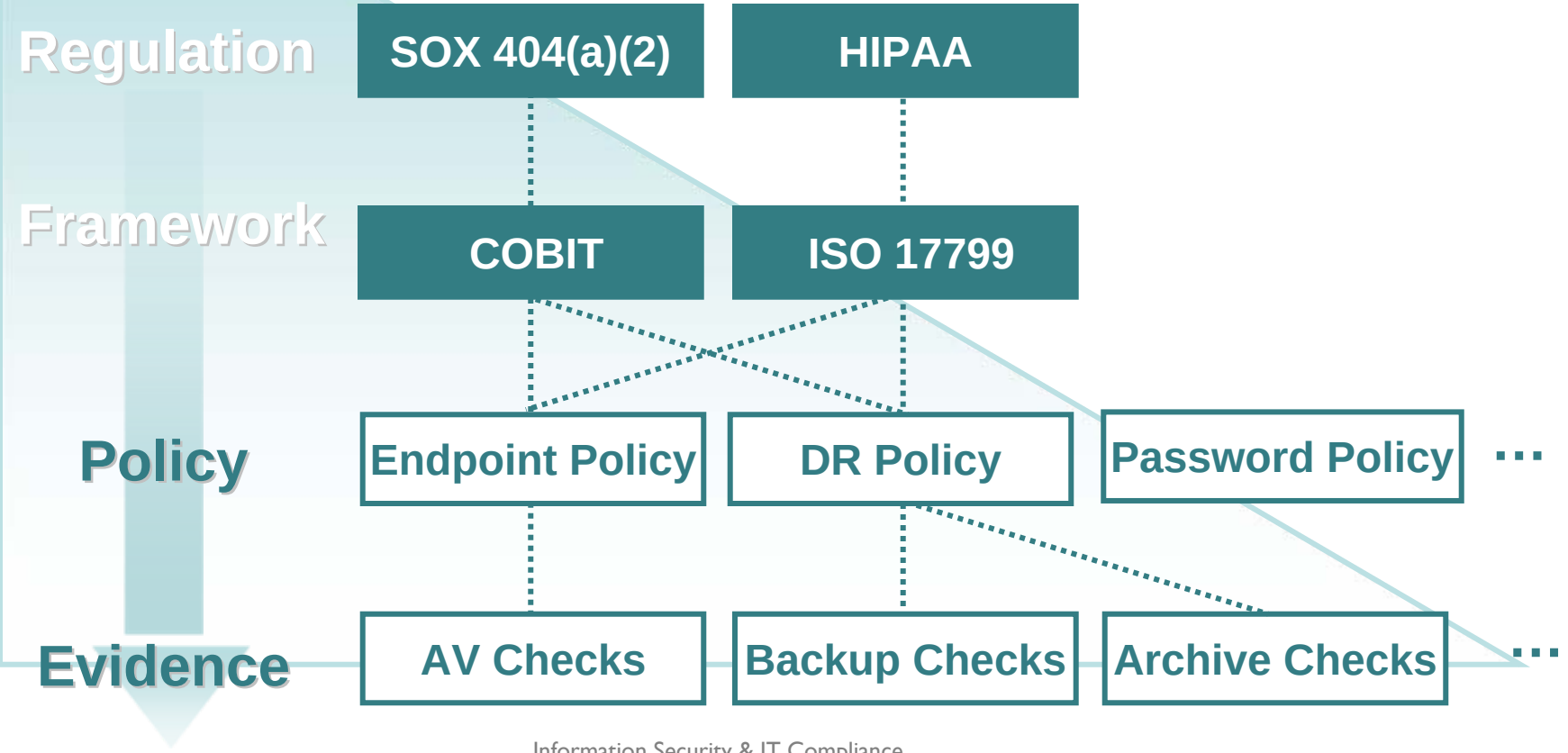
Endpoint Policy

AV Checks

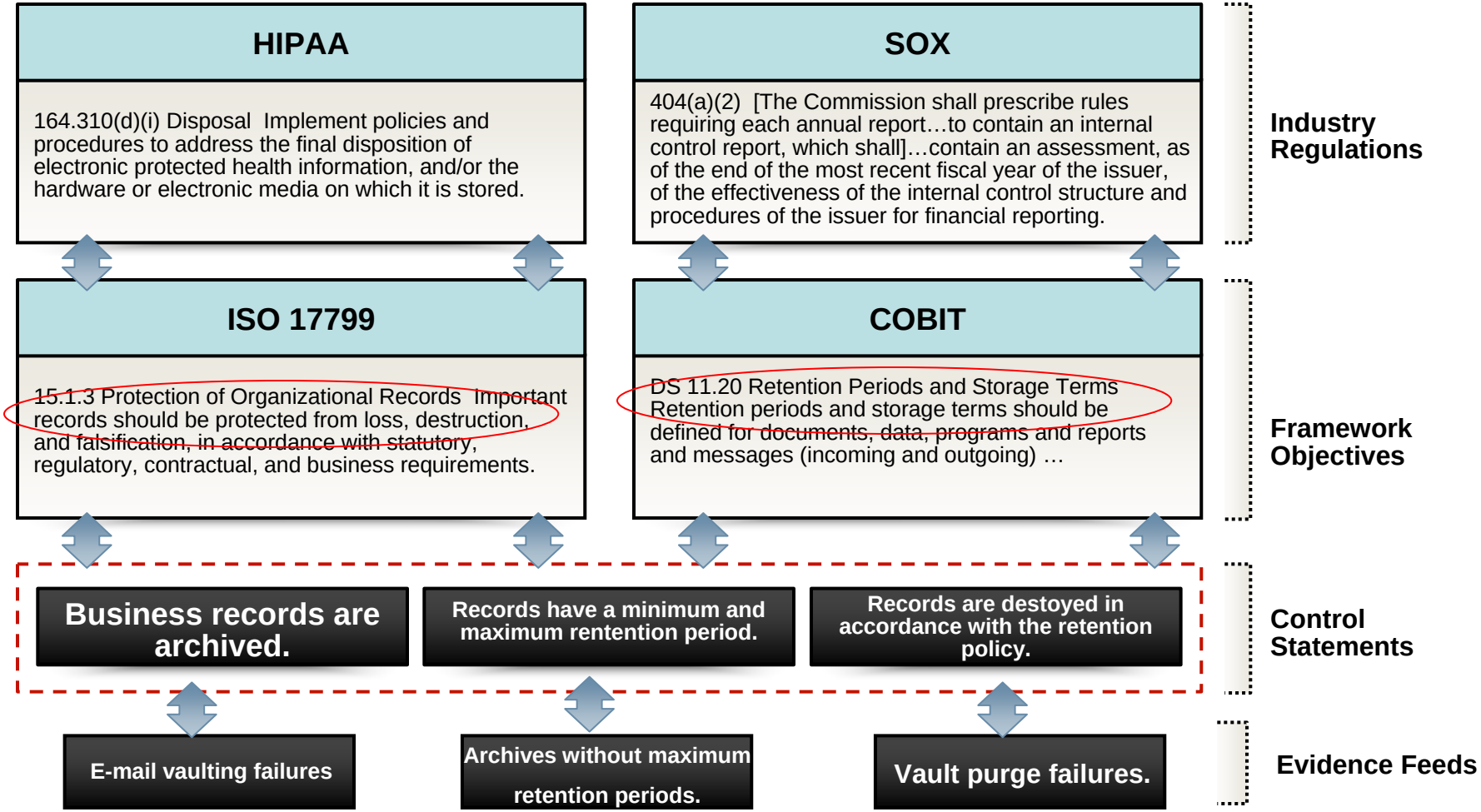
… Multiple Policies that …



Show Coverage across Regulations



Map Policies to IT controls - Archiving



Management of IT Compliance

Education SNIA

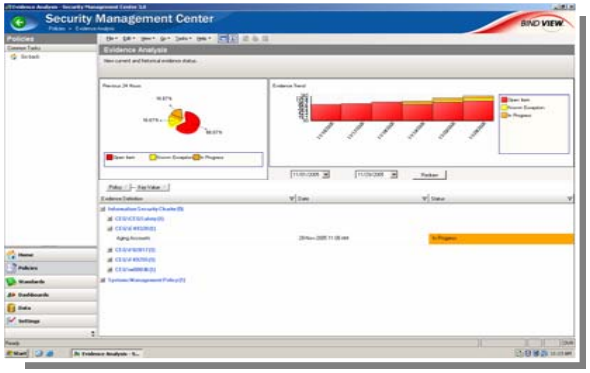
Regulation

SOX View

HIPAA View

COBIT View

ISO 17799 View



Framework

Policy & Evidence Integration Engine

Policy

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

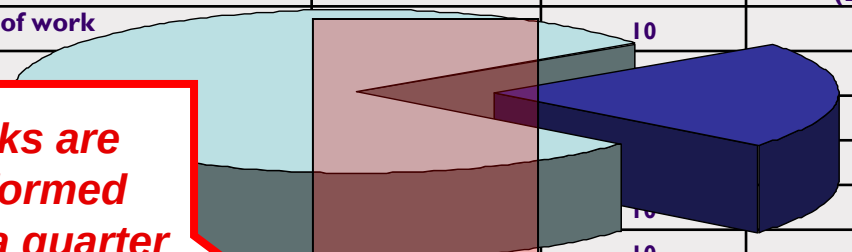
Evidence

Focus On IT Controls

Education SNIA

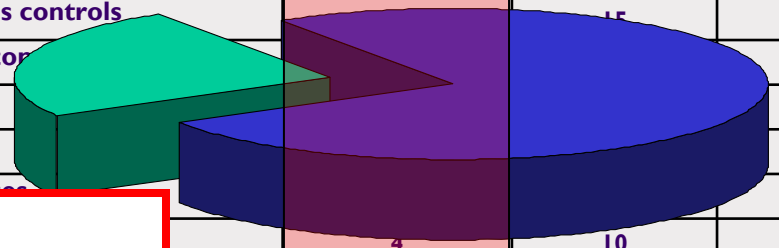
TYPE	TASKS	FREQUENCY / YEAR	COST (Days)	TOTAL COST / YEAR (Days)
NON IT Related	Create compliance scope of work	1	10	10
	Establish/review policy	1	10	10
	Project Mana	1	20	20
	Design/Reviev	1	10	10
	Design/Reviev	1	10	10
	Design/Reviev	1	10	10
	Design/Reviev	1	10	10
	Design/Reviev	1	10	10
	Design/Review purchasing inventory controls	1	5	5
	Design/Review other systems controls	1	15	15
	Design/Review HR processes	1	5	5
	Implement/update controls	1	60	60
	Test controls	1	40	40
	Evaluate Material Weaknesses	1	40	40
	Submit Exem	4	10	40
			NON IT RELATED TOTAL MAN DAYS	*295*
IT Related	Design/Revie	4	10	40
	Run It Contr	52	10	520
	Disseminate	52	2	104
	Remediation	52	5	260
			IT RELATED TOTAL MAN DAYS	*924*

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 externals ones
- Report results and demonstrate compliance internally or to external auditors

Summary

- IT Risk Management is a 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

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

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

- SNIA Education Committee

Frank Bunn
Roger Cummings
Eric Hibbard CISSP, CISA
Larry Hofer CISSP
Chris Parker
Blair Semple, CISSP-ISSEP
Chris Lionetti