Aligning Your Organization's Business Units to Achieve a Cohesive Cybersecurity Strategy

Orus Dearman, Director, Business Advisory Services, Grant Thornton
Johanna Terronez, Senior Manager, Business Advisory Services, Grant Thornton

Professional Strategies – S13

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Learning objectives

- Describe how recent changes in cybersecurity regulation and enforcement can impact your business
- Determine how to leverage the NIST Framework for Improving Critical Infrastructure Cybersecurity across your organization
- Identify best practices for aligning your organization’s business units to achieve a cohesive cybersecurity strategy
- Achieve multiple reporting demands through a test once apply to many approach

Agenda

- **Current cybersecurity threat landscape**
- Standards, regulation and enforcement
- Leveraging the NIST framework
- Best practices
- Test once, apply to many

Current cybersecurity threat landscape

Reasonably current events….

Shellshock

Apple iCloud allegedly suffers privacy breach of celebrity photos

Target Data Breach

Michaels says breach at its stores affected nearly 3M payment cards

Russian cyber gang steals over one billion passwords

Current cybersecurity threat landscape

Cybersecurity breach incidence is on the rise

The cost of responding to each cyber breach event in the U.S. rose to $5.4 million in 2013[2]

Cybercrime and cyber espionage costs the worldwide economy about $400 billion per year[3]

Over 740 million online records were exposed in 2013[1] at an average cost of $145 per compromised record[2]

There were around 500 data breaches in the first half of 2013[1]

[1] Online Trust Organization [2] The Ponemon Institute's "2013 Global Cost of Data Breach" study [3] The Center for Strategic and International Studies' "The Economic Impact of Cybercrime and Cyber Espionage" study

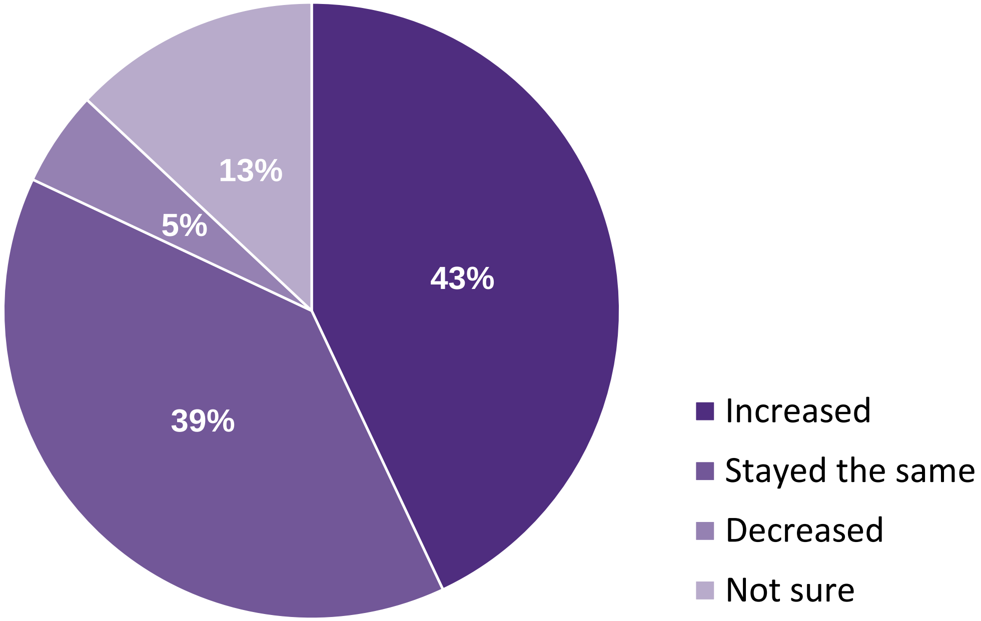
Current cybersecurity threat landscape

How are your peers responding?

General Counsel

More than **40%** of General Counsel claim that the risk of a cybersecurity/data privacy breach has increased in the past year, and that risk was at record-high levels last year.

Change in cybersecurity and data privacy risk



Current cybersecurity threat landscape

How are your peers responding?

General Counsel

Top cybersecurity concerns for General Counsel include:

57%	Customer and client data
49%	Fear of unknown risks
46%	Legal compliance with laws
42%	Potential for undetected breaches
42%	Employee and workplace privacy

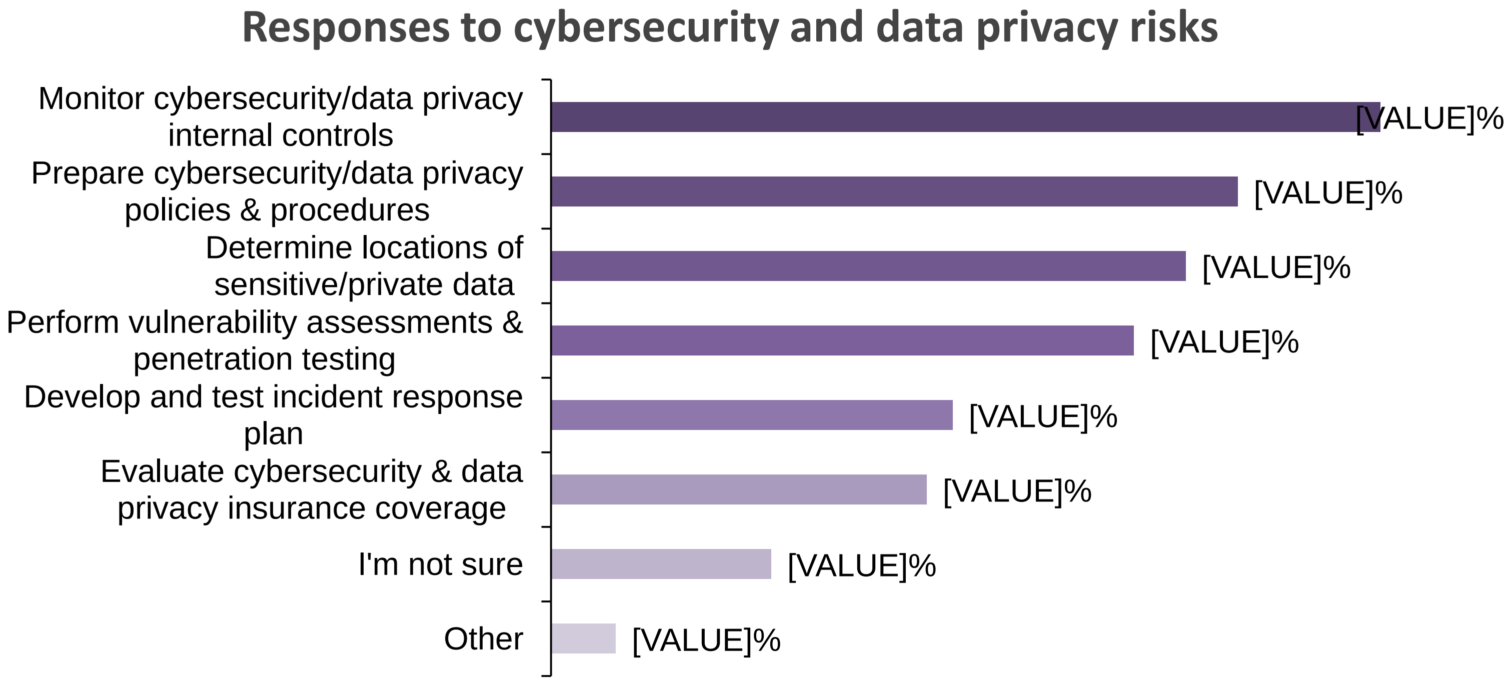
Respondents may select more than one answer.

Current cybersecurity threat landscape

How are your peers responding?

General Counsel

Responses to cybersecurity risk are lacking. **17%** of General Counsel respondents were unsure about what was being done to deal with these risks within their organizations.

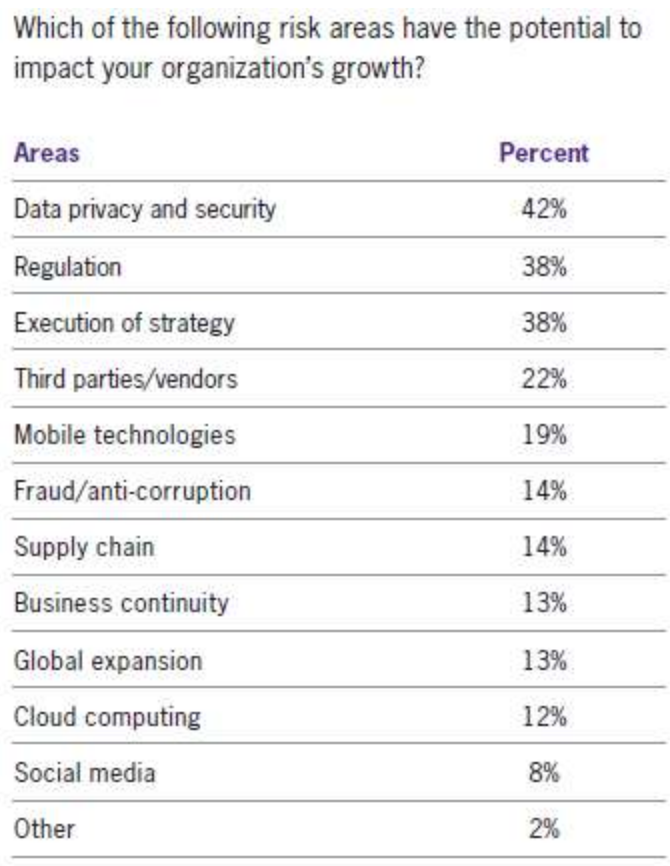


Respondents may select more than one answer.

Current cybersecurity threat landscape

How are your peers responding?

Chief Audit Executives



Which of the following risk areas have the potential to impact your organization's growth?

Areas	Percent
Data privacy and security	42%
Regulation	38%
Execution of strategy	38%
Third parties/vendors	22%
Mobile technologies	19%
Fraud/anti-corruption	14%
Supply chain	14%
Business continuity	13%
Global expansion	13%
Cloud computing	12%
Social media	8%
Other	2%

42% of Chief Audit Executive respondents cite data privacy and security as a risk area that has the potential to impact their organizations' growth.

Current cybersecurity threat landscape

How are your peers responding?

CFOs

Top cybersecurity concerns for CFOs include:

59%	Potential for undetected breaches
54%	Customer/client data privacy
50%	Unknown and identified risks
42%	Employee and workplace privacy
32%	Compliance with data security laws

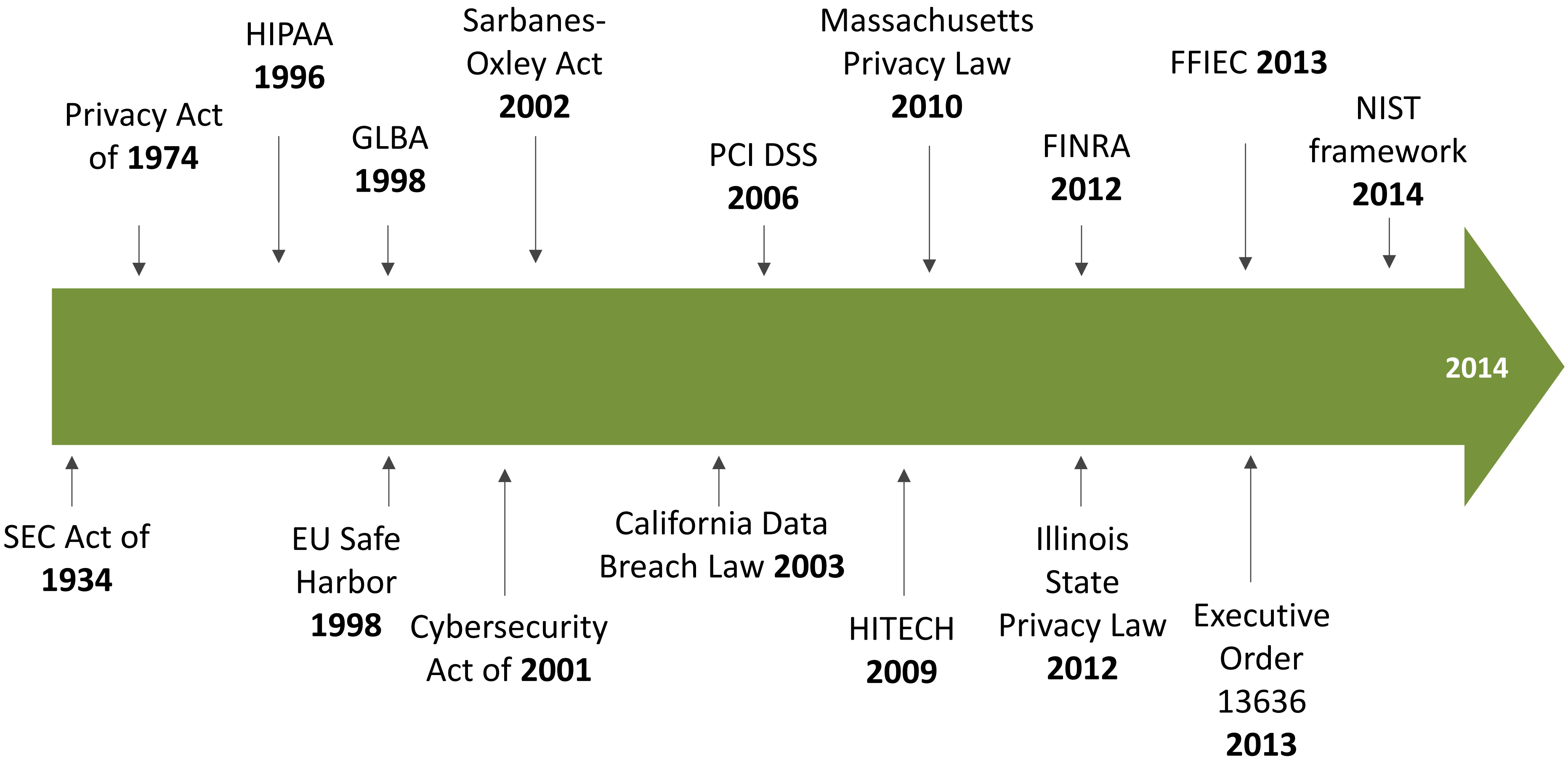
Respondents may select more than one answer.

Agenda

- Current cybersecurity threat landscape
- **Standards, regulation and enforcement**
- Leveraging the NIST framework
- Best practices
- Test once, apply to many

Standards, regulation and enforcement

Cybersecurity: Compliance timeline



Privacy Act of **1974**

HIPAA **1996**

GLBA **1998**

Sarbanes-Oxley Act **2002**

PCI DSS **2006**

Massachusetts Privacy Law **2010**

FINRA **2012**

FFIEC **2013**

NIST framework **2014**

2014

SEC Act of **1934**

EU Safe Harbor **1998**

Cybersecurity Act of **2001**

California Data Breach Law **2003**

HITECH **2009**

Illinois State Privacy Law **2012**

Executive Order 13636 **2013**

Standards, regulation and enforcement

Drivers of Framework Adoption

Adoption of a Cybersecurity Framework

- A framework is a data structure that organizes and categorizes an organization’s internal controls, and which are practices and procedures established to create business value and minimize risk.
- Focus on using business drivers to guide Cybersecurity activities and considering Cybersecurity risks as part of the organization’s risk management processes.

Drivers of Adoption

- Increased litigation surrounding Cybersecurity events.
- The cost of responding to each cyber breach event in the U.S. rose to $5.4 million in 2013. (2)
- Over 740 million online records were exposed in 2013 at an average cost of $145 per compromised record. (1)
- There were approximately 500 data breaches in the first half of 2013. (1)

Standards, regulation and enforcement

Common Frameworks (…not all inclusive)

Established frameworks include:

- NIST Cybersecurity Framework - Consists of standards, guidelines, and practices that enable a prioritized, flexible, repeatable, and cost-effective approach to managing cybersecurity related risk.
- NIST SP 800-37, Risk Management – Establishes a common framework to improve information security and strengthen risk management processes
- SANS Critical Security Controls - Focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" (Subset of the NIST SP 800-53 controls)
- ISO 27001 – Establishes an Information Security Management System
- COBIT 5 – Provides guidance to help IT and security professionals understand, utilize, implement and direct important information security-related activities, and make more informed decisions.

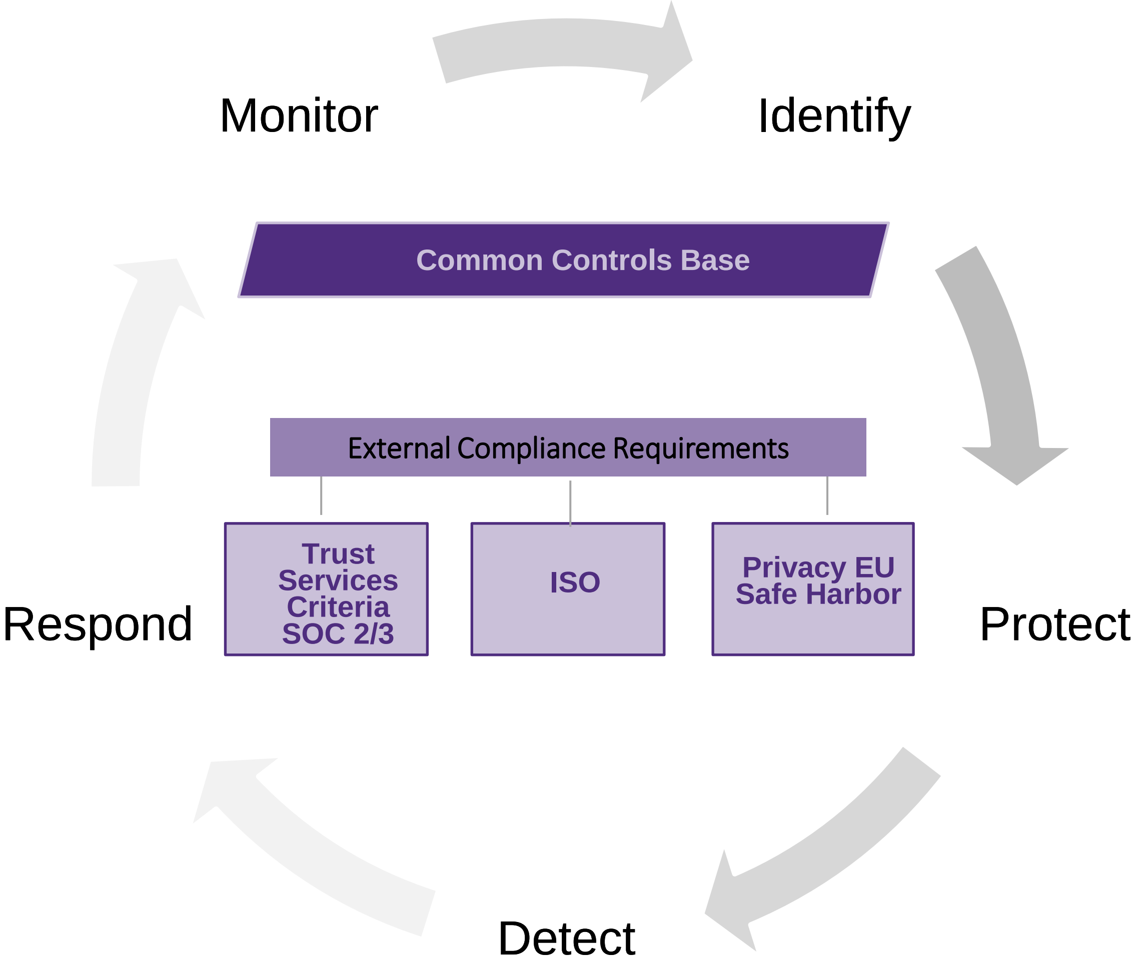
Standards, regulation and enforcement

A Framework can help

Driver	Benefit
Process Maturity	• Develops process maturity enabling formal, repeatable procedures • Enables proactive responses to changes in business conditions and direction
Reporting & Measurement	• Drives the definition and operationalization of controls • Once baseline is established, enables insightful reporting on Cybersecurity preparedness • Enables measurement of success and ongoing monitoring
Risk Management	• Enables the organization to clearly demonstrate how they monitor and manage Cybersecurity risk throughout the security lifecycle • In the event of a breach event, better position an organization to demonstrate that it made a good faith effort to implement a framework that encompasses best practice Cybersecurity practices and guidelines
Alignment to Business Objectives & Strategy	• Clear view of how ongoing projects align with defined business objectives enabling strategic adjustments while understanding objective dependencies

Standards, regulation and enforcement

How a framework works



Monitor

Identify

Common Controls Base

External Compliance Requirements

Trust Services Criteria SOC 2/3

ISO

Privacy EU Safe Harbor

Respond

Protect

Detect

Standards, regulation and enforcement

NIST Framework for Improving Critical Infrastructure Cybersecurity

- Created through collaboration between industry and government
- Consists of standards, guidelines, and practices to promote the protection of critical infrastructure
- Based on existing standards, guidelines, and practices - for reducing cyber risks

Identify	•Asset Management •Business Environment •Governance •Risk Assessment •Risk Management Strategy
Protect	•Access Control •Awareness and Training •Data Security •Information Protection and Procedures •Maintenance •Protective Technology
Detect	•Anomalies and Events •Security Continuous Monitoring •Detection Process
Respond	•Response Planning •Communications •Analysis •Mitigation •Improvements
Recover	•Recovery Planning •Improvements •Communications

Standards, regulation and enforcement

NIST Framework for Improving Critical Infrastructure Cybersecurity

- Experts warn that recommendations included in the Framework may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the institution
- Since the Framework was created with industry best practices in mind, its recommendations may be recognized as industry standards in litigation

Standards, regulation and enforcement
Enforcement

- The Federal Trade Commission (FTC) has begun bringing lawsuits against entities in relation to their cybersecurity policies.
- The SEC's Office of Compliance Inspections and Examinations (OCIE) is issuing a Risk Alert concerning cybersecurity preparedness in the securities industry. The NIST Framework is listed as information it may request when conducting an examination.

Standards, regulation and enforcement

The NIST Framework for Improving Critical Infrastructure Cybersecurity was designed to?

Agenda

- Current cybersecurity threat landscape
- Standards, regulation and enforcement
- **Leveraging the NIST framework**
- Best practices
- Test once, apply to many

Leveraging the NIST framework

IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery planning
- Improvements
- Communications

Leveraging the NIST framework

Where do we start?

External	Internal
• Extended data supply chain	• Financial and IT systems
• Third parties	• PCI, PII, NPI, HIPAA
• Cloud/SaaS	• Regulatory
• Breach detection	• Legal/compliance
• Prevention and response	• Governance/audit

NIST, CCS, COBIT, ISA, ISO

Leveraging the NIST framework

What is the most effective method of managing cybersecurity risk across your organization?

Who is really responsible for cybersecurity risk management, response planning and strategy?

Agenda

- Current cybersecurity threat landscape
- Standards, regulation and enforcement
- Leveraging the NIST framework
- **Best practices**
- Test once, apply to many

Best practices

Common misconceptions

- It will never happen to me
- Our network is secure
- We are in compliance with industry standards
- We are not a big company
- We don't have any personal information so we aren't a target
- We have never been attacked

Best practices
Planning ahead

- Align your organization's cybersecurity risk strategy to the overall business strategy
- Determine your business unit's role in assessing organizations capabilities
- Form a cross-functional cybersecurity task force and incident response team (IRT)
- Determine who manages communication between management and board
- Develop relationships with outside companies
- Perform a vendor management assessment

Best practices
Planning ahead

- Constant vigilance
- Vendor management program responsibility
- Have warm standby systems
- Effective DR or BCP plan can allow for an investigation to proceed while recovery is effected
- Have IRT trained and ready

Agenda

- Current cybersecurity threat landscape
- Standards, regulation and enforcement
- Leveraging the NIST framework
- Best practices
- **Test once, apply to many**

Test Once, Apply to Many: Company Challenge

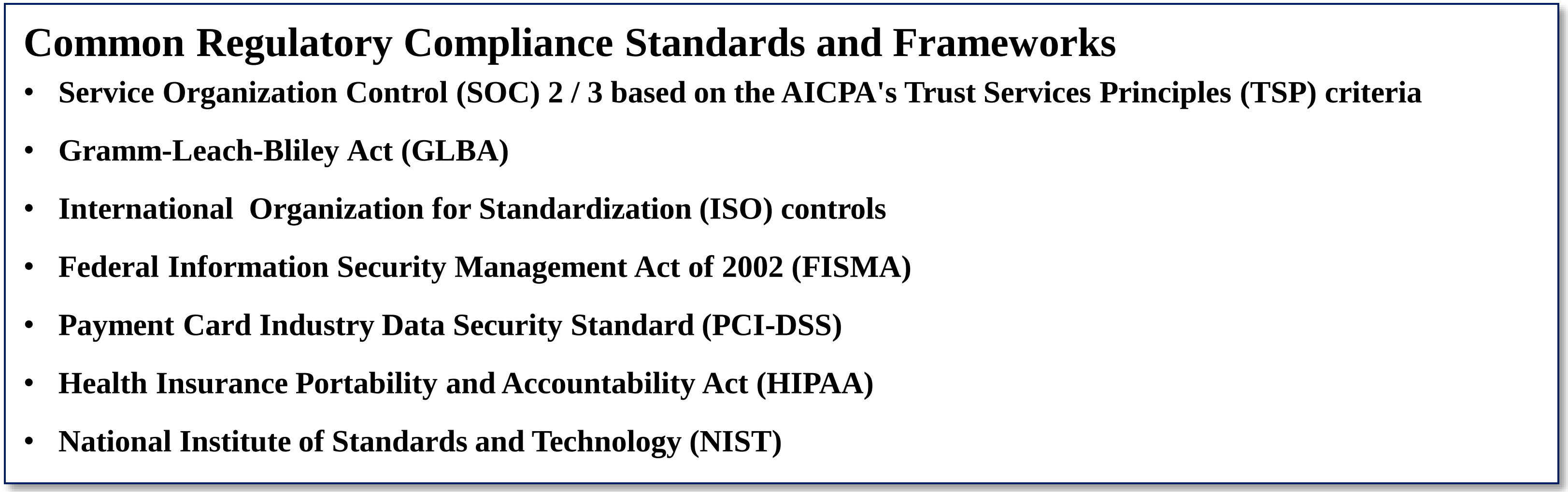
- Service providers in every industry find themselves having to comply with multiple regulations (e.g. federal-, state- or industry-related)
- Additionally, enforcement actions for noncompliance are increasing in highly regulated industries, such as, healthcare and financial services
- Service providers are struggling with developing and maintaining adequate controls that address **multiple regulations and frameworks** and reporting its compliance on multiple standards to customers for an **affordable spend**
- Historical viewpoint: the differences across the compliance mandates are greater than the similarities, resulting in companies using different vendors and having different owners across the organization. **Inefficient**!!

Test Once, Apply to Many: Company Challenge – cont'd -

- Survey of US CFOs and Senior Controllers revealed:
  - Nearly 50% believe that regulatory compliance is a barrier to growth
  - 60% are concerned that new and pending regulations will further constrict business expansion

  AND

  - 60% view regulatory compliance as a strategic imperative to the org.



Common Regulatory Compliance Standards and Frameworks

- **Service Organization Control (SOC) 2 / 3 based on the AICPA's Trust Services Principles (TSP) criteria**
- **Gramm-Leach-Bliley Act (GLBA)**
- **International Organization for Standardization (ISO) controls**
- **Federal Information Security Management Act of 2002 (FISMA)**
- **Payment Card Industry Data Security Standard (PCI-DSS)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **National Institute of Standards and Technology (NIST)**

Test Once, Apply to Many: In Practice

- Reality is that we are using a lot of the same information for the different regulating bodies and are asking similar or the same questions of the same people
- We recommend a "**Test Once, Apply Many**" approach to manage the complexity of complying with and reporting on multiple regulations
- Rather than performing separate compliance testing and reporting on each requirement, efforts can be streamlined to test once and comply with multiple mandates.

SOC	HIPAA	GLBA	PCI	ISO 27001/2	FISMA	NIST

Test Once, Apply to Many: In Practice – cont'd -

EX: A Bank that also provides commercial and personal banking services, and lockbox services for healthcare organizations (e.g. patient payments)

They collect, use and retain PII and PHI. The organization’s compliance requirements include some type of data security program that ensures compliance with privacy regulations, as well as with non-disclosure and confidentiality clauses within customer agreements. The obligations may require generating a report on controls relevant to PCI DSS; or to Security, Confidentiality or Privacy, three of the TSP criteria; and even a report regarding compliance with HIPAA requirements

SOC	**HIPAA**	**GLBA**	**PCI**	**ISO 27001/2**	**FISMA**	**NIST**

Test Once, Apply to Many: In Practice – cont'd -

- We would begin the compliance for SOC/PCI/HIPAA integration by first selecting one highly applicable standard for its company and industry.
  - EX: The TSP criteria, which underlie SOC 2/3 reports, can be used to develop a listing of all controls or criteria applicable to the Bank.
- We would then align the Bank's existing controls to address the TSP criteria AND map those control requirements to meet PCI and HIPAA.
- Where a particular compliance standard may demand additional controls or processes, those additional elements can be noted, and the control can be elevated to satisfy the highest standard.
- Leverage existing testing information, approaches and scripts; minimize unnecessary duplication of walk-throughs and testing; and maximize the use of test results across reports or other mandates.

Test Once, Apply to Many: In Practice – cont'd -

EX: The NIST framework may be mapped to Company controls and other standards, such as ISO and COBIT, allowing the incorporation of multiple standards and establishing of overall compliance monitoring.

Function	Category	Sub Category	Common Controls	References
Identify	**Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.**	ID.AM-1: Physical devices and systems within the organization are inventoried	Defined and mapped to establish adherence to the framework	· CCS CSC 1
				· COBIT 5 BAI09.01, BAI09.02
				· ISA 62443-2-1:2009 4.2.3.4
				· ISA 62443-3-3:2013 SR 7.8
				· ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
				· NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried		· CCS CSC 2
				· COBIT 5 BAI09.01, BAI09.02, BAI09.05
				· ISA 62443-2-1:2009 4.2.3.4
				· ISA 62443-3-3:2013 SR 7.8
				· ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
				· NIST SP 800-53 Rev. 4 CM-8

Test Once, Apply to Many: Benefits

- Reduce risk of noncompliance and associated penalties and/or fees
- Decrease the complexity and disruption inherent in working with multiple auditors and consultants by consolidating compliance and audit activities with one service provider
- Refocus resources and spending on activities that drive business growth
- Reduce the burden on functional areas that must respond to multiple data requests for compliance information
- Cost savings to the business in terms of spending and resources.
- Create a competitive advantage by meeting certain quality standards associated with compliance and valued in the marketplace

Questions?

Contact Information

Orus Dearman

Director, Business Advisory Services

San Francisco, CA

T: 415-318-2240

E: orus.dearman@us.gt.com

Johanna Terronez

Senior Manager, Business Advisory Services

San Francisco, CA

T: 415-318-2228

E: johanna.terronez@us.gt.com

Disclaimer

This Grant Thornton LLP presentation is not a comprehensive analysis of the subject matters covered and may include proposed guidance that is subject to change before it is issued in final form. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this presentation. The views and interpretations expressed in the presentation are those of the presenters and the presentation is not intended to provide accounting or other advice or guidance with respect to the matters covered.

For additional information on matters covered in this presentation, contact your Grant Thornton, LLP adviser.