Automated IT Compliance

Compliance …
the evolving roles of IT*
June 2008

Phattrapha Hongkumdee, CISSP, CISA
Manager, Advisory

*connectedthinking

PRICEWATERHOUSECOOPERS

Agenda

Compliance Challenges

Leveraging Technology

Case study

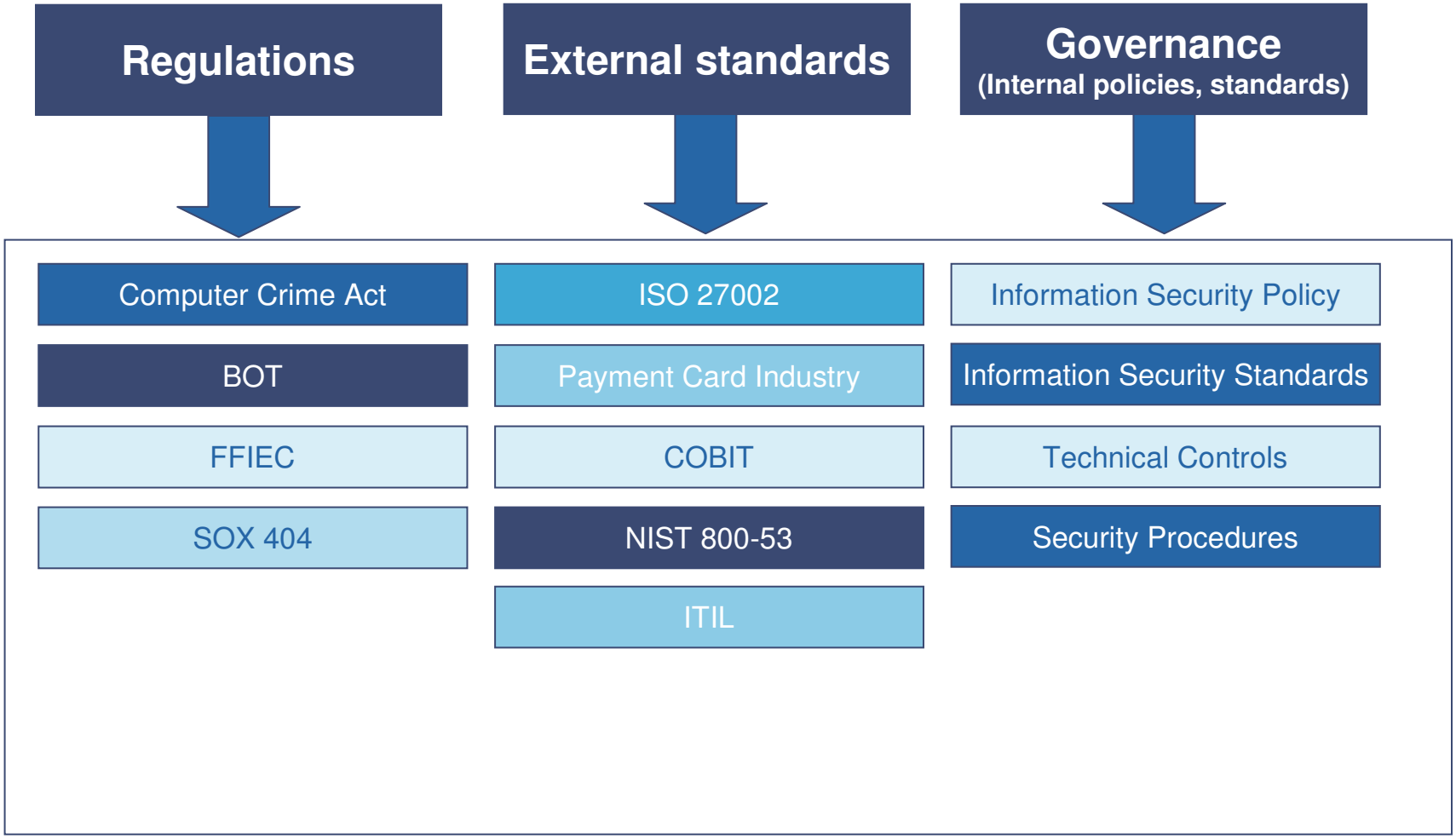
Agenda

Compliance Challenges

Leveraging Technology

Case study

Types of IT compliance



Compliance challenges – pain points

- Difficulty in managing multiple regulations
- Unclear compliance responsibilities
- Poor integration with other functions
- Increasing compliance cost
- Lack of direct communication between compliance and senior management and/or the board
- Insufficient pool of talent in this area of business
- Fragmented view of compliance status

Compliance challenges – pain points

- Inadequate technological infrastructure for monitoring compliance
- No sustainable process to manage compliance
- Difficulty in translating requirements to technical parameters
- Disparate accountability for compliance across the organization
- Lack of measures to evaluate effectiveness of compliance functions

Gartner: Top Five Issues and Research Agenda, 2008: The IT Compliance Manager (20 March 2008)

1 How should common controls for multiple compliance mandates be developed and implemented?

Challenge: An overwhelming and constantly growing of compliance mandate

Solution: To develop and implement both manual and automated common control sets

Benefits: Improved auditing, simplified testing and enterprise wide reporting

2 How can the cost and complexity of compliance be reduced?

Challenge: The cost and complexity of compliance

Solution: 1) common control sets 2) a risk-oriented approach, 3) controls automation

Benefits: 2) Focusing on high risks find that costs drop 70%
3) Reducing internal labor and audit costs

Gartner: Top Five Issues and Research Agenda, 2008: The IT Compliance Manager (20 March 2008)

3 How can positive performance benefits be derived and demonstrated from compliance investments?

Challenge: How to show compliance spending can be offset by performance improvement

Solution: A risk-oriented compliance

Benefits: Risk management enabled better performance reporting, with risk information enabling a forward-looking aspect to balanced scorecard reports

4 How can compliance efforts align with the enterprise's legal, financial and other business needs?

Challenge: How to ensure controls are effective in mitigating IT and business risks

Solution: To collaborate with legal, finance, business, risk, other stakeholders

To establish where the highest risk lie and what IT Controls must be established

To provide advice on IT solutions to improve compliance for the entire enterprise

Gartner: Top Five Issues and Research Agenda, 2008: The IT Compliance Manager (20 March 2008)

5 How can enterprises select the right compliance technologies?

Challenge: More point solutions or GRC platform solutions in automated compliance processes and controls

Solution: Identifying solutions that close gap in GRC architecture

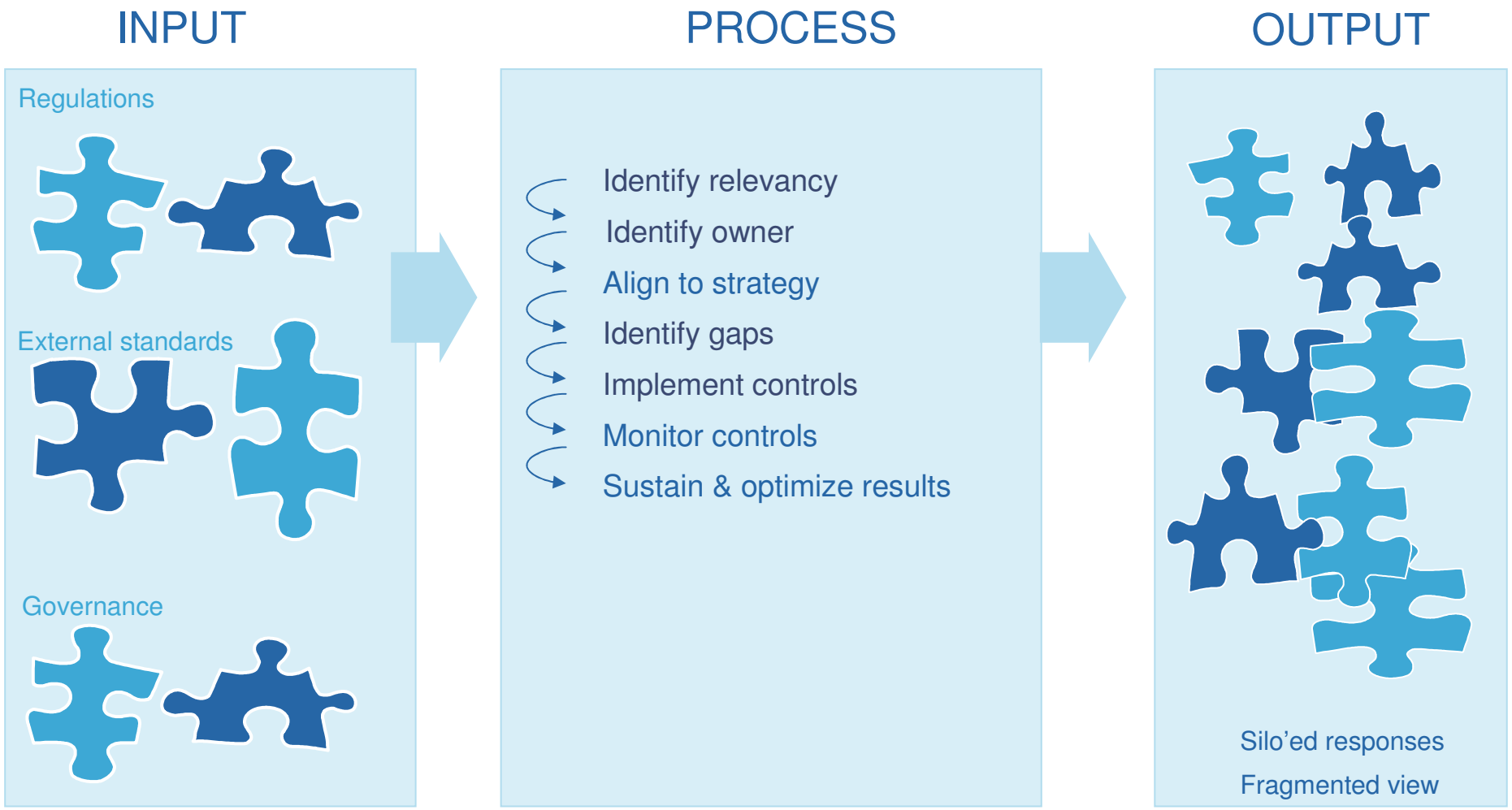
Benefits: Aligning compliance and risk management activities to business risks

Gartner: Top Five Issues and Research Agenda, 2008: The IT Compliance Manager (20 March 2008)

Recommendation

- **Conduct a gap assessment of the enterprise's governance, risk and compliance (GRC) architecture**, and focus technology investments on closing the highest-risk gaps.
- Focus on **developing common control sets** for different compliance mandates. Some mandates will require special controls, but these unique controls should be the exception.
- **Eliminate or reduce "siloed" compliance activities, particularly through the use of automated controls and tools**, and through organizational alignment of the IT compliance and risk management functions with the enterprise compliance and risk management functions.

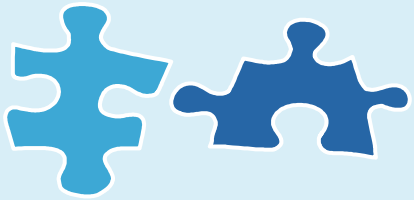
IT compliance process



IT compliance process

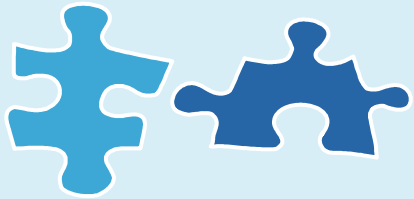
INPUT

Regulations



External standards

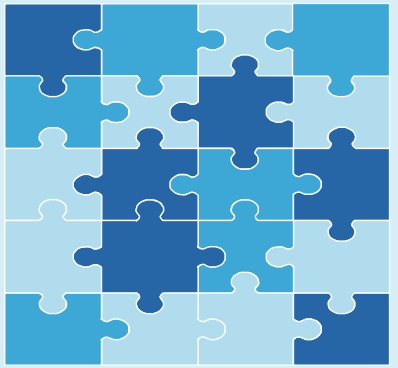
Governance



PROCESS

- Identify relevancy
- Identify owner
- Align to strategy
- Identify gaps
- Implement controls
- Monitor controls
- Sustain & optimize results

OUTPUT



Holistic view of
IT compliance

Regulatory compliance

Industry	Regulation									
	HIPAA	SOX	GLBA	FERC	NERC	CISP	FDICIA	CFR	Basel II	FISMA
Hospitals	X	X				X		X		
Pharmacies	X	X				X		X		
Retail		X				X		X		
Banking		X	X			X	X	X	X	
Energy Producers		X		X	X			X		
Insurance	X	X				X		X		
On-line Retail	X	X				X		X		
Credit Card Service Providers		X				X		X		
Governmental Agencies	X			X				X		X

Frameworks and standards

Framework or Standard	Regulation									
	HIPAA	SOX	GLBA	FERC	NERC	CISP	FDICIA	CFR	Basel II	FISMA
COSO		X	X	X	X	X	X	X	X	X
CoBiT		X	X							
ITIL		X					X			
ISO 27001/27002	X						X			
NIST				X						X
FFEIC Handbooks							X			
Payment Card Industry						X				
CIP					X					
FIPS				X						X

Computer Crime Act

มาตรา 26 และ 27 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

มาตรา 5 และ 6 มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์

มาตรา 7 มาตรการป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์

มาตรา 5 และ 6 การป้องกันการเข้าถึงระบบคอมพิวเตอร์

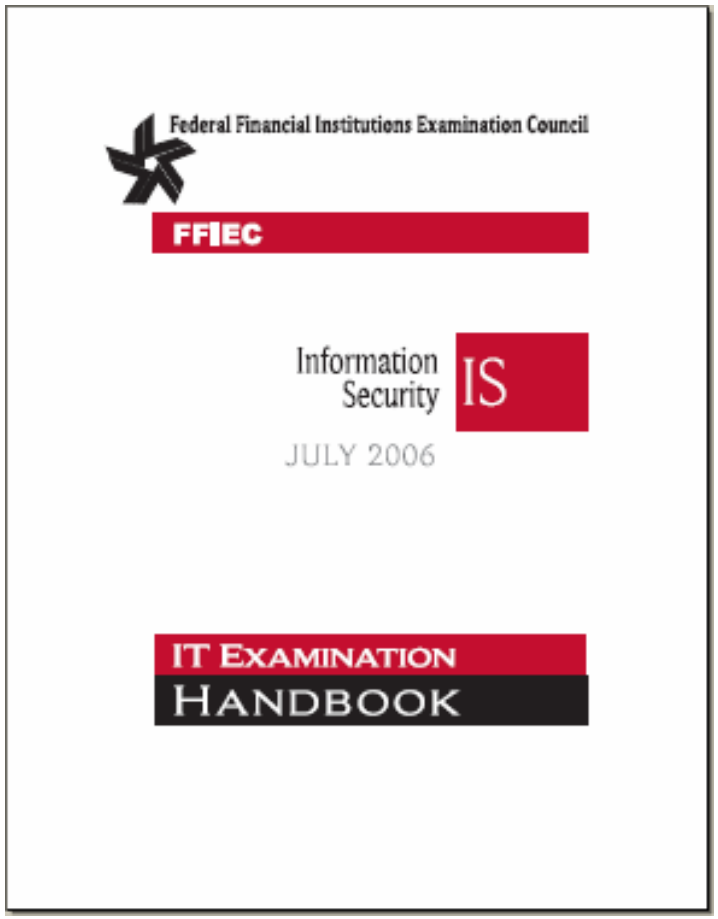
มาตรา 8 การป้องกันการดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์

มาตรา 10 การป้องกันการระงับชะลอ ขัดขวาง การทำงานของระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

มาตรา 11 ป้องกันการปกปิดแหล่งที่มาการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น

มาตรา 15 ไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

Federal Financial Institutions Examination Council (FFIEC)



- Information Security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- Security Monitoring
  - Architecture
  - NIDS, HIDS
  - Honeypots
  - Log
- Security Process Monitoring and Updating

ISO27002

11 domains, 133 controls

Payment Card Industry (PCI)

6 categories, 12 requirements

Build and Maintain a Secure Network	Implement Strong Access Control Measures
1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor supplied defaults for system passwords and other security parameters	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Protect Cardholder Data	**Regularly Monitor and Test Networks**
3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain Vulnerability Management Program	**Maintain an Information Security Policy**
5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications	12. Maintain a policy that addresses information security

Internal security policies

5. Security Policy

6. Organization of Information Security

7. Asset Management

8. Human Resources Security

9. Physical and Enviromental Security

10. Comunications and Operations Management

11. Access Control

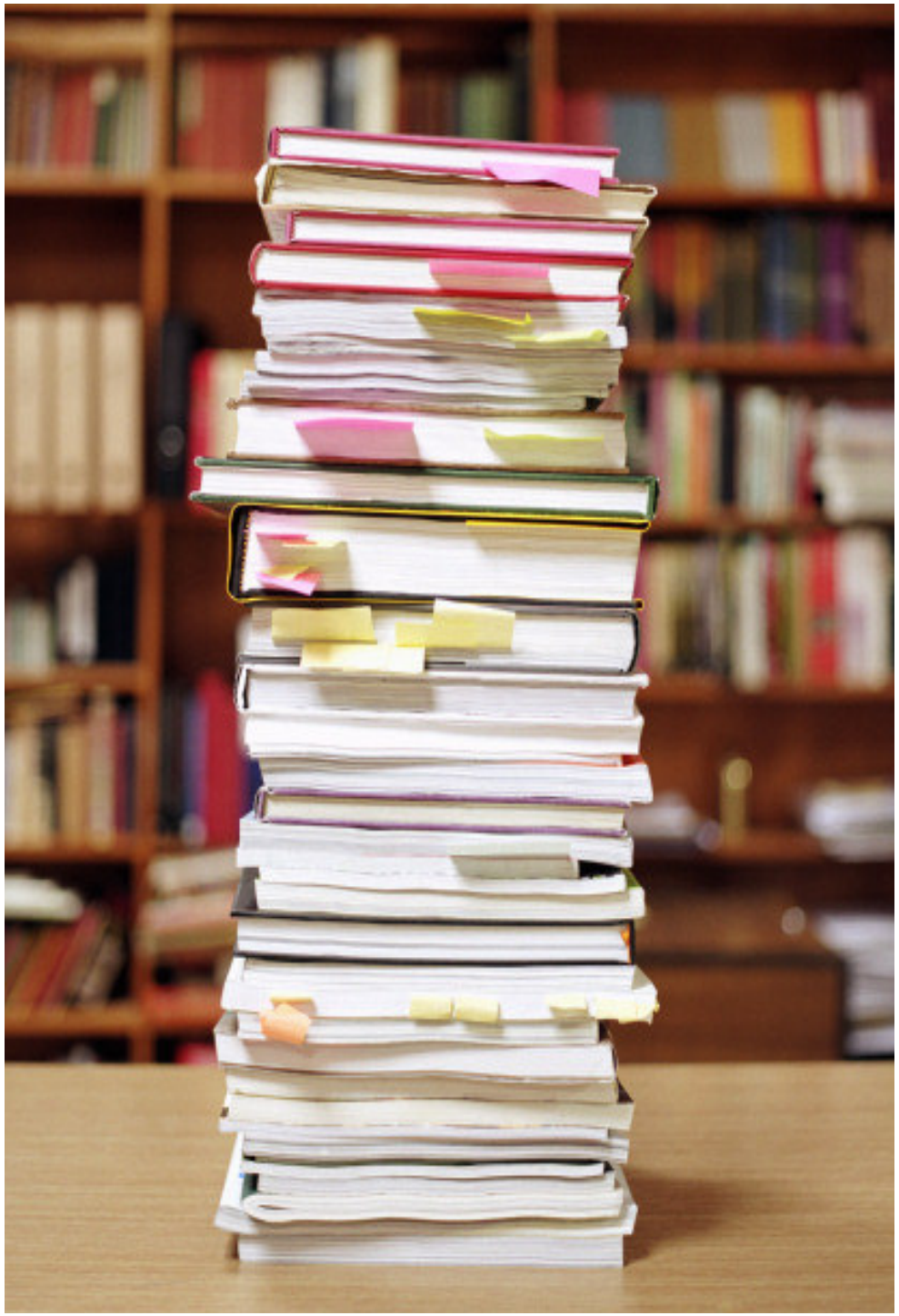
12. Information Systems Acquisition, Development and Maintenance

13. Information Security Incident Management

14. Business Continuity Management

15. Compliance

PricewaterhouseCoopers




Requirements are overlapped!
Opportunities for integration exist!

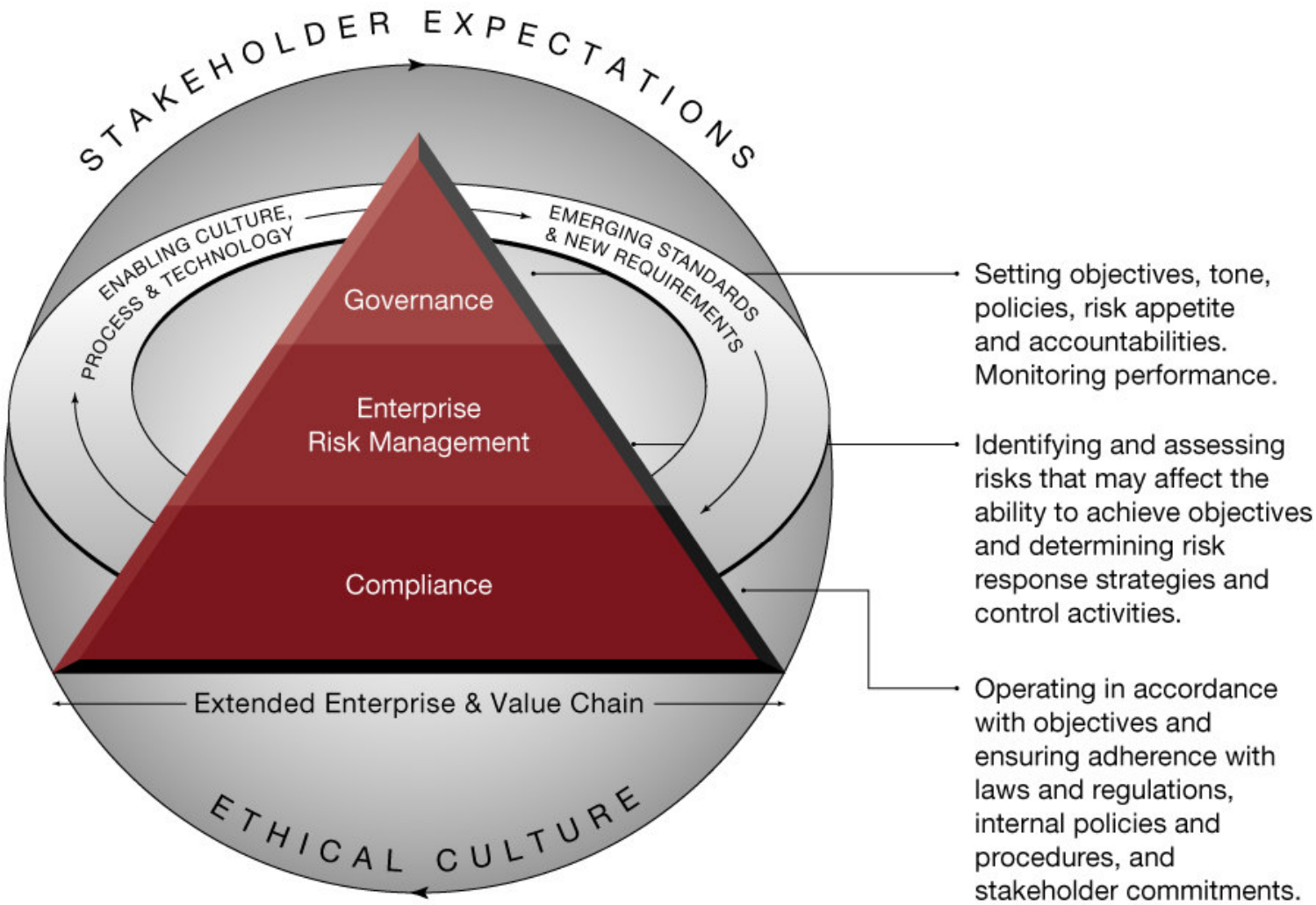
Agenda

Compliance Challenges

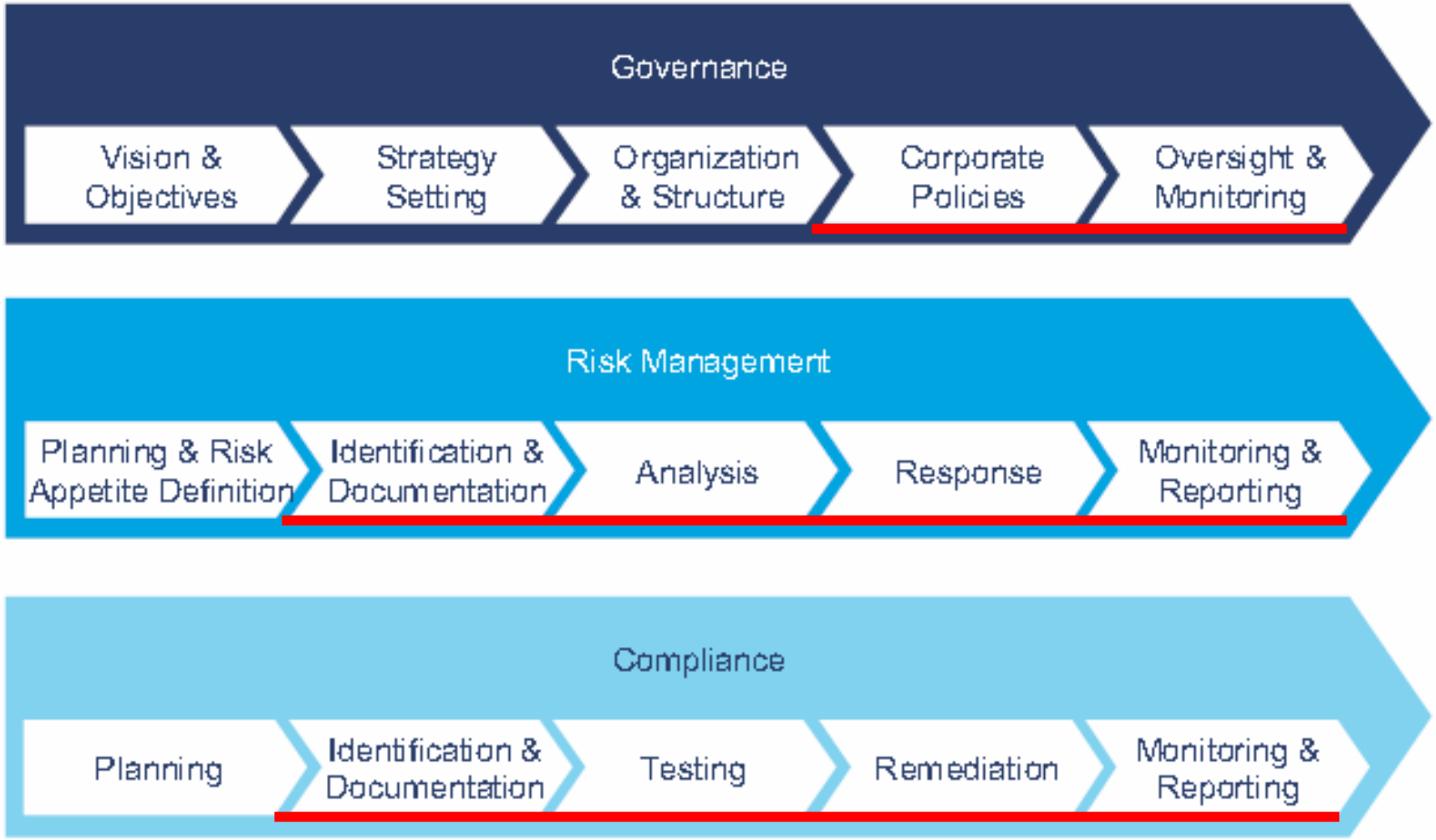
Leveraging Technology

Case study

Governance Risk and Compliance Management



IT Governance Risk and Compliance Management Process



Effective compliance

7. Prevent further offenses: use performance information to prevent further similar offenses once a violation has been detected.

6. Uniform enforcement and appropriate incentives: policies and procedures must enforced and when exceptions are discovered, consistent corrective action must be applied. Compliance should be part of performance evaluation.

5. Audit, monitor, self-evaluation, and reporting: compliance efforts must be monitored and audited, and risks periodically assessed, to ensure the programs are effective.

Enabling Technology

1. Policies and procedures: develop policies and procedures to institutionalize and encourage appropriate behavior.

2. High-level oversight: create role specifically responsible for compliance management and performance, with oversight by board and executives.

3. Decentralized administration and proper delegation: designate appropriate accountabilities and exhibit due care in delegating discretionary administrative authority.

4. Establish communication and training channels: provide effective communication between all levels of employees and training appropriate to role.

Source: Federal Sentencing Guidelines for Organizations (FSGO)

The 3 Steps to Compliance

1 **Fist Step** Understand the risks and identify key areas not covered

2 **Second Step** Develop a plan

3 **Third Step** Begin a real-time GRC pilot

1 First Step

Understand the risks and identify key areas not covered

- Establish an IT compliance function
- Establish clear communication channels and protocols
- Manage compliance as a program, not a project
- Understand the requirements of relevant compliance obligations
- Review risk and compliance issues that facing the enterprise and each business unit
- Determine pacts on processes, technology and resources
- Determine how technologies can address risks and compliance issues
- Envision a real-time compliance architecture that handle both the technology required at the enterprise-level to manage compliances and technologies that can integrate compliance into business process

2 Second Step

Develop a plan

- Map real-time compliance architecture and overlay it with existing systems to identify gaps
- Determine areas that can be addressed by leveraging existing technologies
- Formulate a plan to move to a real-time environment
- Prioritize implementation based on cost and risk factors
- Factor in potential enhancements to existing systems

3 Third Step

Begin a real-time GRC pilot

- Start with a project that offers tangible improvements at a modest cost
- Initiate a pilot program and specify expected results in measurable terms
- Practice change management

Agenda

Compliance Challenges

Leveraging Technology

Case study

Case Study

A Major Financial Services in US

Challenges

- Understaffed in IT organization
- Wished to automate and sustain server security assessments

BENEFIT

Based on previous client implementations it is estimated that the new compliance assurance processes will **provide an average of 90% time savings** on compliance tracking, **significantly reduce operational failures** due to inconsistencies and result in radical annual cost savings. Collectively, these results will **help the CIO improve IT effectiveness and provide improved quality services.**

PwC Service offered

Helped the client translate their security standards into tangible policy compliance rules within compliance tool to automate compliance monitoring

Helped the client define tailored management reports to identify overall policy compliance, high impact gaps and technical detail reports.

Helped the client adopt new business processes and enabling technology through knowledge transfer sessions with business and technical stakeholders.

A Major Aerospace Defense Contractor in US

Challenges

- Administrators were focusing more than 80% of time on compliance management.
- Stakeholders experience critical operational issues and failures.
- CIO recognized a need for compliance management to take burden away from the administrators and provide some structure around roles and responsibilities.

BENEFIT – Based on previous client implementations, the new compliance processes will provide an average of **90% time savings** on compliance tracking, significantly **reduce operational failures** due to inconsistencies and result in **radical annual cost savings**. Collectively, these results will help the CIO **improve IT effectiveness** and provide **improved quality services** to their clients.

PwC Service offered

Helped the client interpret compliance requirements and translate them into objective components within compliance tool to automate initial compliance tracking

Helped the client create an inventory resources for compliance tracking

Helped the client define a sophisticated roles and responsibilities framework to segregate duties

Provided an objective view of over 100 compliance requirements for the stakeholders.

3 Key Ideas to Take Away

1. Establishing risk-oriented compliance management framework
2. Establishing common control sets
3. Selecting a tool associated to your risk profiles

Q & A

Phattrapha Hongkumdee
Manager, Advisory
phattrapha.hongkumdee@th.pwc.com

PRICEWATERHOUSECOOPERS