

# Right-sizing Risk and Compliance for Small to Mid-size Companies

Susanne Elizer

Practice Director – Accretive Solutions

Professional Strategies – S32



CRISC  
CGEIT  
CISM  
CISA

2014 Fall Conference - "Think Big"

# Compliance Jeopardy

Sectors	Famous Cases	Intl	Enforcers	Key Rqmts	Gotchas
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500

# Agenda

---

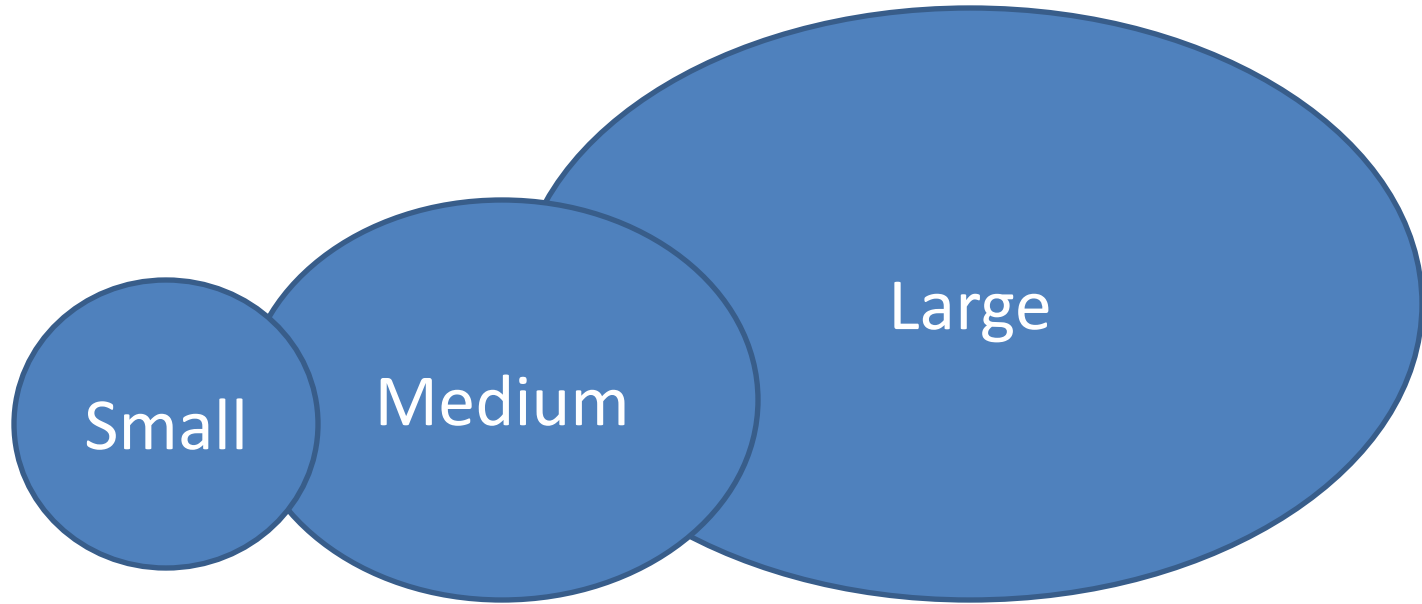
- **Risk and Compliance Programs**
- **Risk and Compliance in Small to Mid-Size Companies**
- **Figuring Out Where To Start**
- **Practical Implementation Pointers**

# Risk and Compliance Programs



# Key Definitions: Company Size

---



- US\*, Small < \$25.5M revenue; Medium < \$1B
- European Union\*, Small < 50 employees; Medium < 250 employees

\*Source: US – Small Business Administration and Ohio State University's National Center for the Middle Market; Europe: Organization for Economic Cooperation and Development

# Key Definitions: Governance, Risk and Compliance (GRC)

---

**GOVERNANCE** – Management Approach to Decision Making and Control

**RISK MANAGEMENT** – Processes to Anticipate, Identify, Evaluate, and Respond to Risks

**COMPLIANCE** – Meet Stated Requirements from Internal Governance and/or External Regulatory Bodies

# GRC Benefits – Assurance and Protection

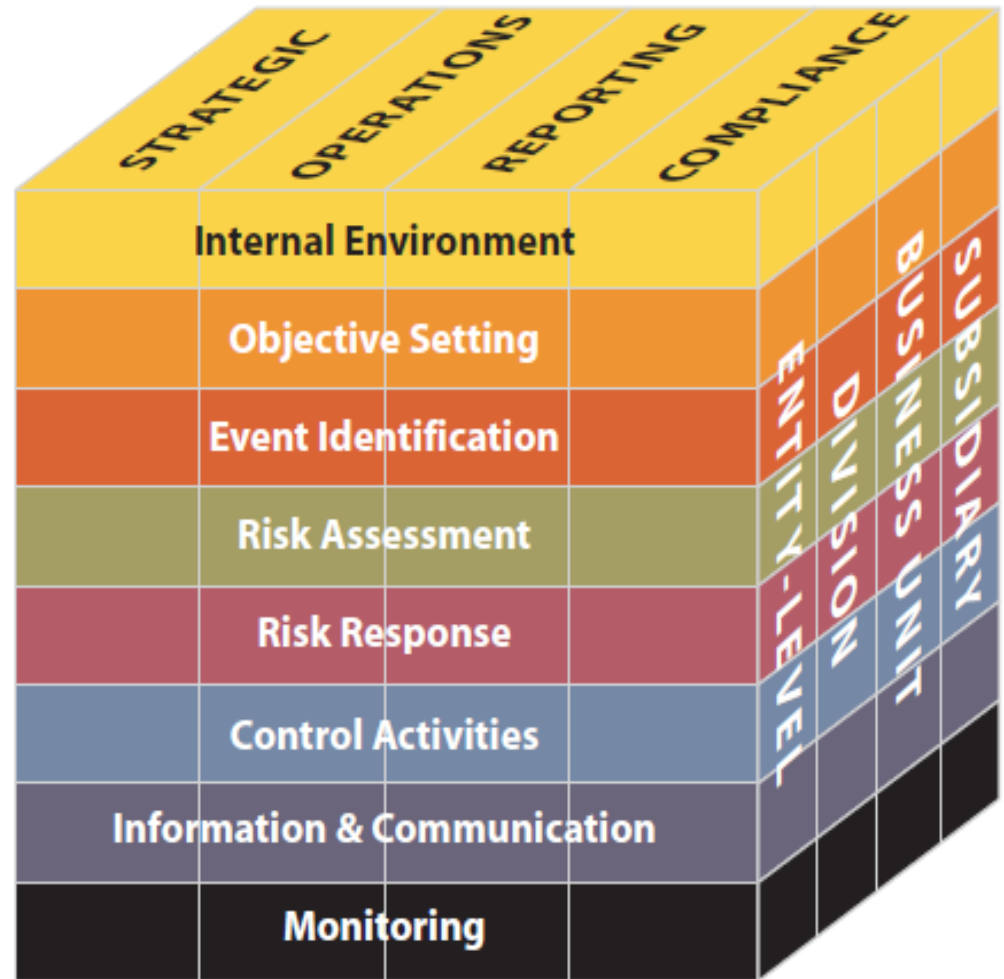
---

- Aligning risk appetite and strategy
- Enhancing risk response decisions
- Reducing operational surprises and losses
- Identifying and managing multiple and cross-enterprise risks
- Seizing opportunities
- Improving deployment of capital

# Enterprise Governance, Risk and Compliance Framework

## Governance Structure:

- Board of Directors
- Risk Committee
- Risk Council
- Office of Risk Management
- Unit Heads
- Control Owners
- Control Performers

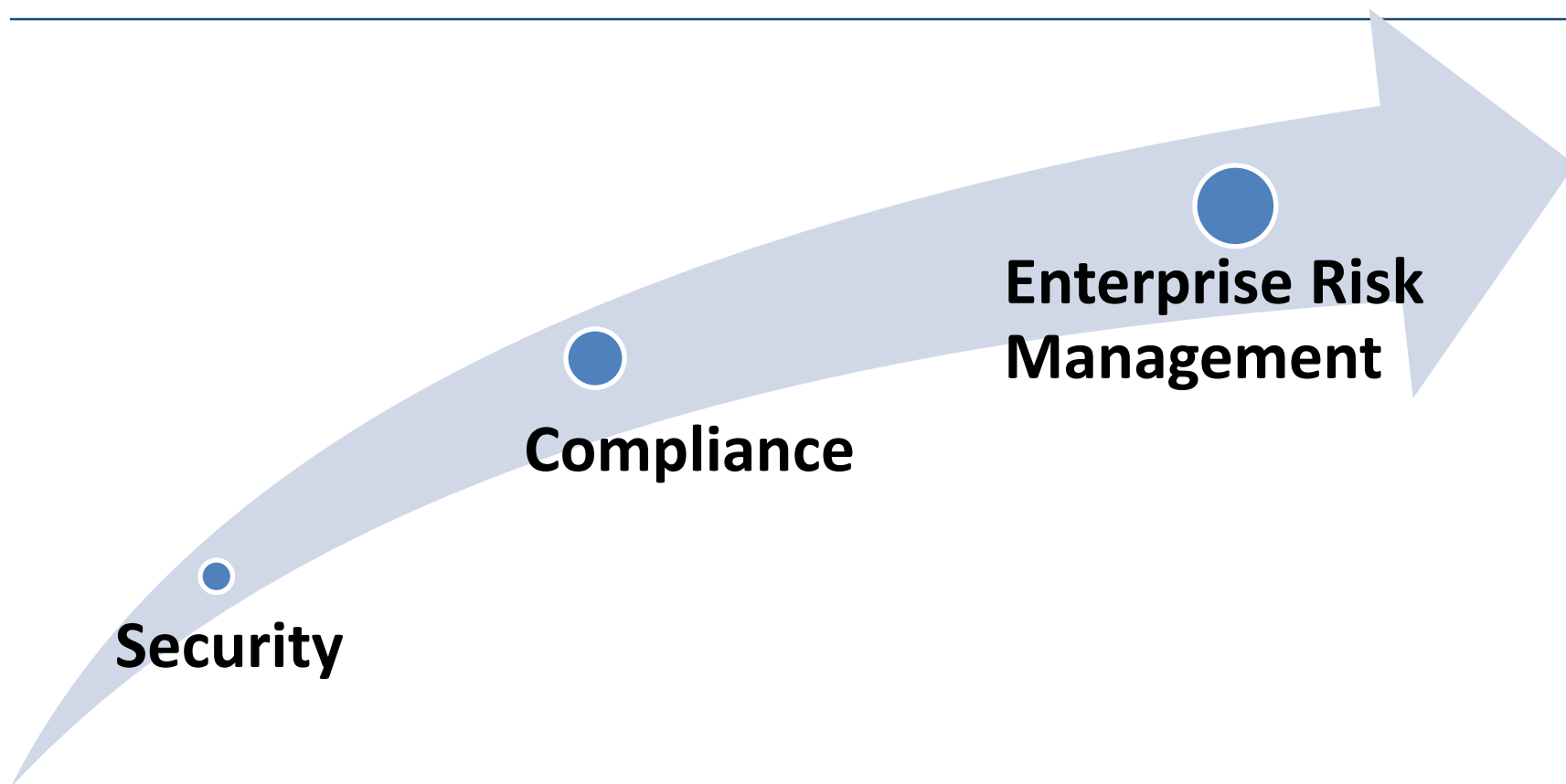


Source: COSO ERM



# The Road to Enterprise Risk Management

---










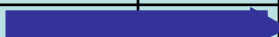




Business Continuity and Disaster Recovery

# Company Awesome – Case Study

---

- SaaS provider of collaboration and business analytics tools
- 200 people
- Recently acquired enterprise customers
- Strong security mindset
- Moving into new customer segments

# Company Awesome – Risk and Compliance Roadmap

		Aug / Sep-14	Q4'14	Q1'15	Q2'15	Q3'15	Q4'15	H1-2016	H2-2016	H1-2016
Risk	Risk Assessment									
	BCP/DR									
Compliance	ISO									
	Readiness									
	Certification									
	HIPAA*									
	Readiness									
	Certification									
	SOC 2									
	Readiness									
	Certification									
Security	Core Policy Development									
	Pen Testing									
	Threat Modeling									

Critical Path



Recommended



\* - Evaluate ROI before Implementing

# Compliance Jeopardy



# Sample Major Compliance Initiatives

## Broadly Applicable

SOX  
PCI  
Privacy Laws  
SSAE 16  
ISO

## International

Safe Harbor  
European Union  
Data Directive

## Healthcare

HIPAA  
HITECH  
PSQIA

## Financial Transactions and Trade

EFTA  
C-TPAT  
FAST

## Financial

GLBA  
Bank Protection  
BITS  
FFIEC

## Media

MRC

## Government

FISMA  
FedRAMP  
CJIS

# Compliance Jeopardy

Sectors	Famous Cases	Intl	Enforcers	Key Rqmts	Gotchas
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500

# Risk & Compliance in Small to Mid-Size Companies



# What Spurs Differences From Large Companies

---

- Key Principles
- Drivers
- Risk Appetite
- Organizational Factors



# Key Principles

---

- Adaptable – keep it flexible. Your business is changing
- Efficient – do it once where possible
- Pragmatic – keep it simple
- Alignment – tie to business strategy must be clear and transparent

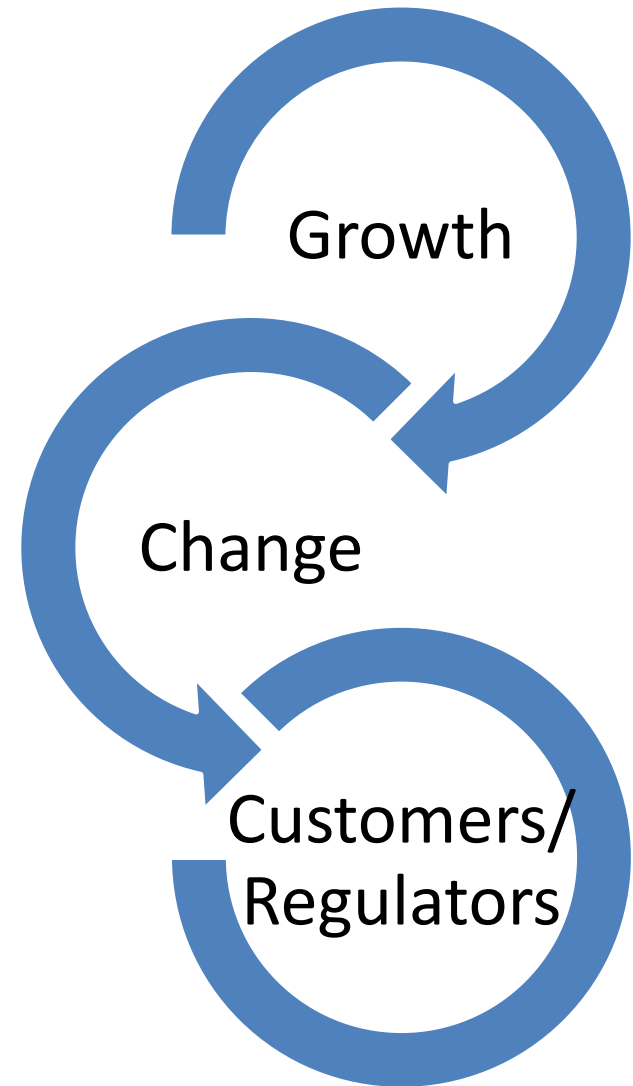
# Drivers

---

Has your growth outpaced your span of control?

Can you drive change in your organization to address risks?

Are your customers or regulators demanding proof that they can trust your service?

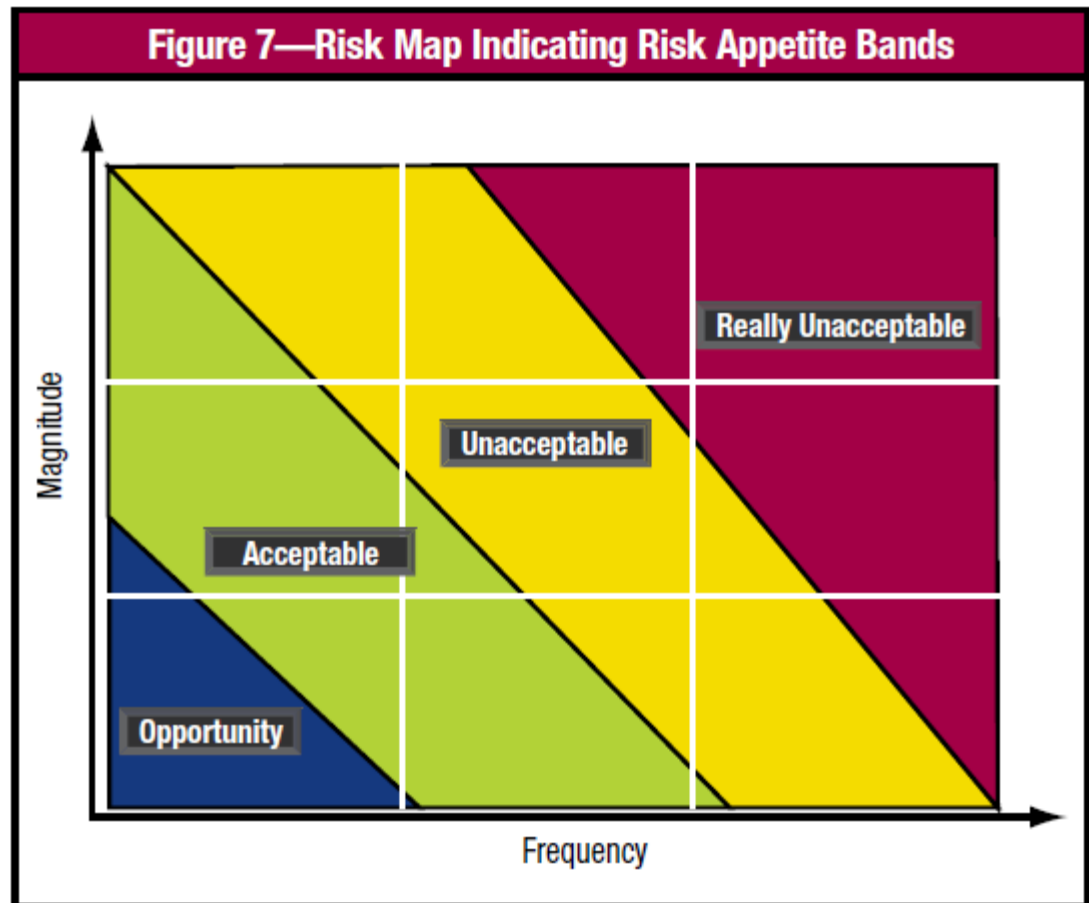


# Risk Appetite

Risk Appetite = amount of risk an organization is willing to take to achieve its objectives

Based on:

- Capacity to absorb loss
- Risk culture
- Cost/Benefit



Source: ISACA IT Risk Framework

# Organizational Factors

---

- Current Maturity
- Time Horizon
- Organizational Complexity (Geography, Size, IT Environment, etc.)
- Pain Points (e.g. breach, inefficiency, etc.)

# Compliance Jeopardy



# Compliance Jeopardy

Sectors	Famous Cases	Intl	Enforcers	Key Rqmts	Gotchas
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500

# Figuring Out Where To Start



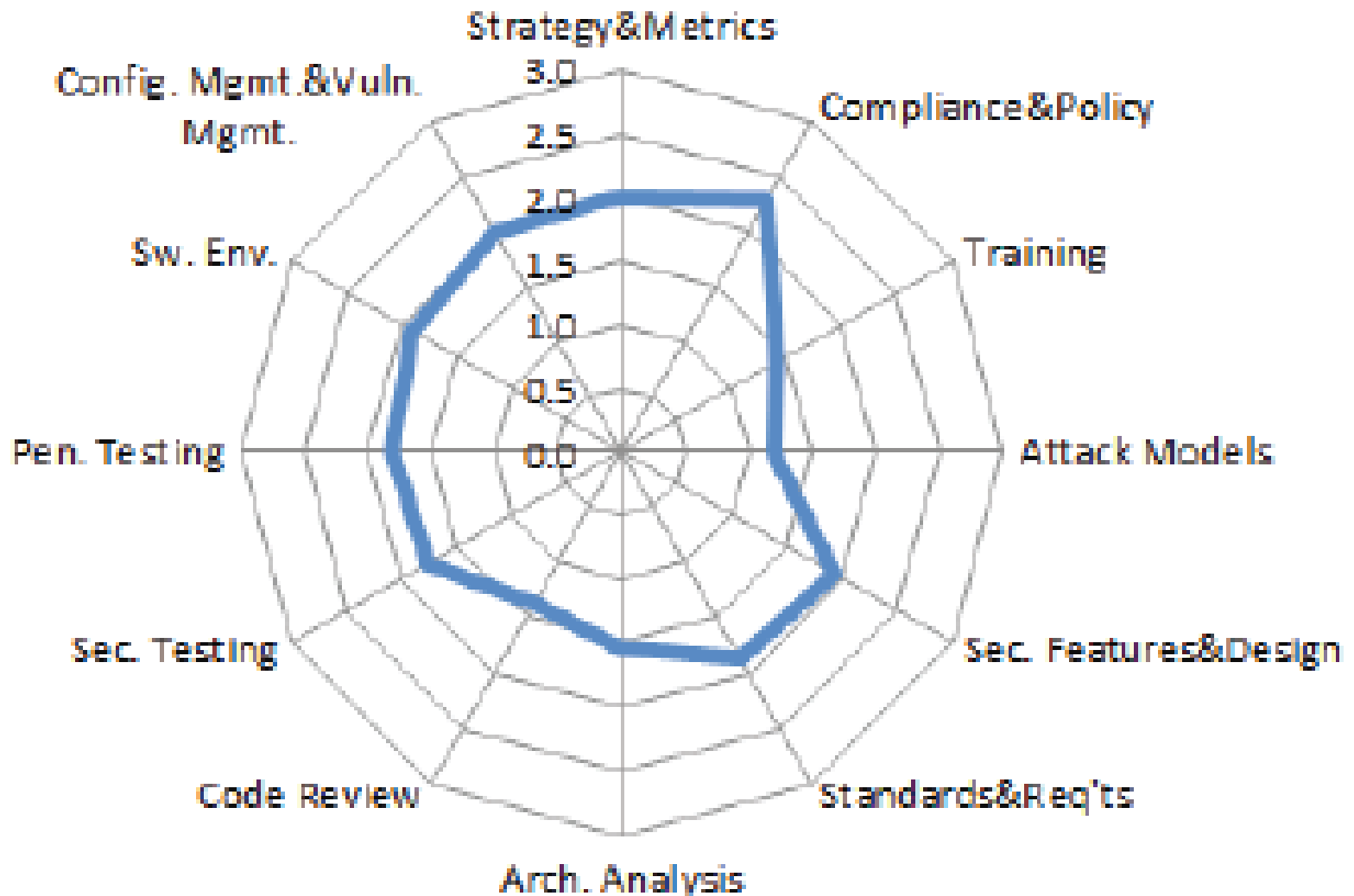
# Getting To Priorities

---

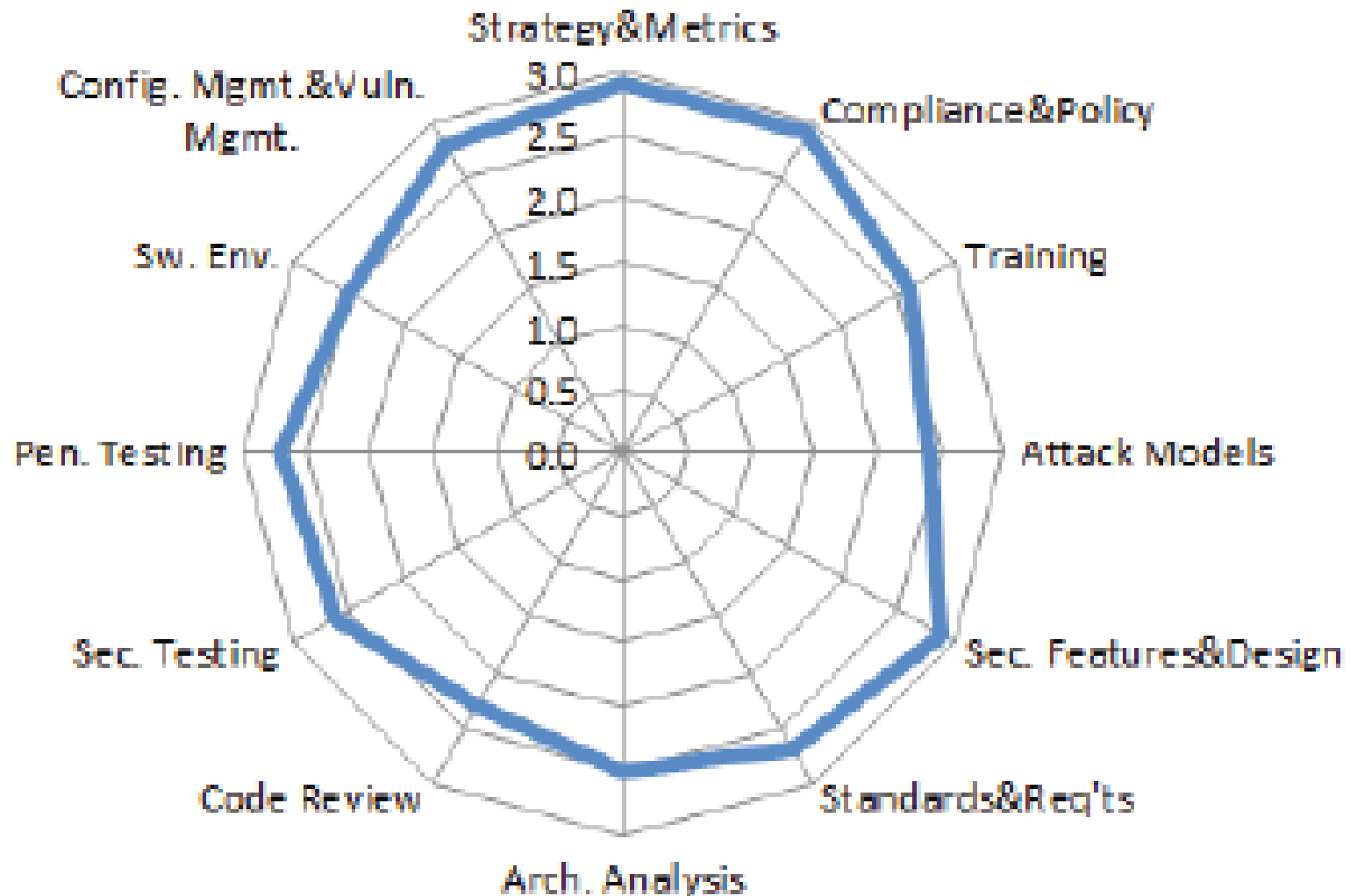
- Security
- Risk Assessment
- Compliance Strategy



# Security Early Stages



# In Later Stages...



# Risk Assessment

---



- **What are your Company Killers?**

# Sample Risks for Small to Mid-sized Companies

---

## What are your Company Killers?

### **Strategic**

- Competition
- Market Concentration
- Economic Conditions
- Reputation
- Customer creditworthiness

### **Financial**

- Cash flow
- Fraud

### **Operational**

- Founder/Management
- Key Employees
- Supply Chain
- Capacity Planning
- Security of data and intellectual property
- Acts of God and Governments
- Litigation
- Compliance

# Risk-Assessment Exercise

---

**What are your Company Killers?**

# Compliance Challenges

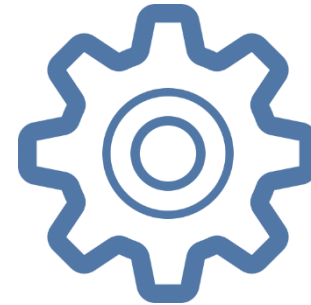
---



## Compliance Readiness and Audits

Costly and time consuming

*(and they can consume you, if you let them!)*



## Security Questionnaires

Cumbersome

# Compliance Pain Points

---

## Pain Points:

- Cost of multiple compliance assessments
  - Direct monetary cost
  - Opportunity cost of internal resource time
- Managing multiple service providers
- Hiring internal resources with skillsets to manage multiple efforts
- Maintaining multiple control lists
  - Responding to multiple PBC lists

# Compliance Consistency

Area	COBIT	HIPAA	ISO	NIST	FedRA	PCI	BITS
					MP		
Compliance	x	X	x	x	x	x	x
Data Gov	x	X	x	x	x	x	x
Facility Security	x	X	x	x	x	x	x
HR	x	X	x	x	x	x	x
Info Sec	x	X	x	x	x	x	x
Ops Mgmt	x	X	x	x	x	x	x
Release Mgmt	x	x	x	x	x	x	x
Resiliency	x	x	x	x	x	x	x
Risk Mgmt	x	x	x	x	x	x	x
Sec Arch	x	x	x	x	x	x	x



# Alleviating the Compliance Burden

---

## **“Test once - comply with many” approach:**

- Enable one test to cover multiple compliance initiatives
- Leverage common requirements across standards
- Aligns controls to cover multiple compliance initiatives
- Consolidate service providers
- Achieve reduction in overall assessment resources for the environment

# Exercise: Building Out Your Roadmap

---

1. What won't scale? Where is your company most vulnerable?
2. What are your current products and what's in the pipeline?
3. Which customer segments are served now? Which ones are planned?
4. What are the compliance requirements for those segments?
5. What's the cost/benefit to implement?

# Compliance Jeopardy



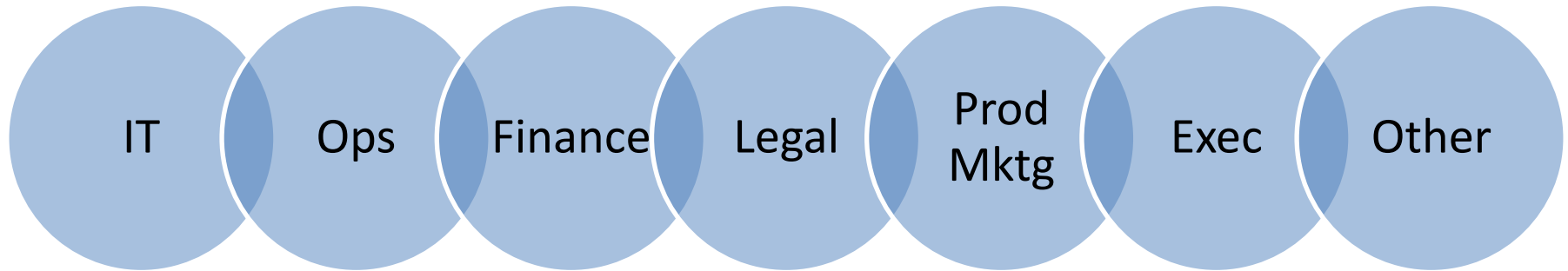
# Compliance Jeopardy

Sectors	Famous Cases	Intl	Enforcers	Key Rqmts	Gotchas
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500

# Practical Implementation Considerations

# Who Owns Governance, Risk and Compliance?

---



Key factors:

- Maturity
- Organizational Factors (Access to Board, Independence, Guardianship, Skills and Expertise, Strategic Thinking)
- Can Be Person Dependent

# Implementation Resourcing

---

## **Decision 1: In-Source or Outsource?**

- What skills exist within your organization?
- How regulated is your industry? How regulated are your customers?
- What volume of work do you expect?

## **Decision 2: Who to Hire?**

- What type of organization are you? (e.g. engineering, financial, etc.)
- What are your highest priority GRC needs?
- How much money and time do you have?
- What have peer organizations done?

# Implementation Pointers

---

- Don't release security info without a mutual NDA
- IT controls are conceptually and fundamentally the same across different compliance initiatives
- Line up the strictest standards and controls that you have to comply, and set your program from those
- Have one provider do as much of your risk and compliance work for you as you can. Check references.
- Save the answers to security questionnaires
- Prepare a Trust Center. Keep it Updated.
- **Risk & compliance doesn't have to be hard**



# Compliance Jeopardy



# Compliance Jeopardy

Sectors	Famous Cases	Intl	Enforcers	Key Rqmts	Gotchas
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500

# Appendix



# Business Size Definition: Wikipedia

## Business Size definitions

	AUS	US	EU
Minute/Micro	1-2	1-6	<10
Small	<15	<250	<50
Medium	<200	<500	<250
Large	<500	<1000	<1000
Enterprise	>500	>1000	>1000

# Practical Example – Compliance Consolidation

## Password Control

PCI	SSAE16 / SOC2&3	ISO 27001	SOX
<p>8.2.4 - Change passwords at least every 90 days</p> <p>8.2.3 - Passwords must be at least seven characters long</p> <p>8.1.6/8.1.7 - Lockout threshold and duration</p> <p>8.2.3 - Passwords must contain both alphabetic and numeric characters</p> <p>8.2.5 - History of at least four passwords remembered</p>	<p>Security Principal 3.2.5</p> <p>The internal network domain is configured to enforce the following password requirements:</p> <ul style="list-style-type: none"><li>•Maximum Password Age</li><li>•Minimum Password Length</li><li>•Invalid Password Lockout</li><li>•Complexity</li><li>•Password History</li></ul>	<p>9.4.1 – Access to information and application system functions shall be restricted in accordance with the access control policy.</p> <p>9.4.2 – Where required by the access control policy, access to systems and applications shall be controlled by a secure log-in procedure.</p> <p>9.4.3 – Password management systems shall be interactive and shall ensure quality passwords.</p>	<p>Applications and systems are configured to comply with password parameters as defined in the Safe Computing Policy.</p>

# Practical Example – Compliance Consolidation

## Physical Access to Datacenter

PCI	SSAE16 / SOC2&3	ISO 27001	SOX
<p>9.1 - Controls to limit and monitor physical access - video cameras and/or access-control mechanisms in place, protected from tampering, monitored/reviewed and correlated with other entries, and data stored for at least three months.</p> <p>9.3 - Visitors authorized, distinguishable, badge expiration controls.</p> <p>9.4 - Visitor log</p>	<p>Security Principal 3.3.2 Physical access to the onsite data center is restricted to authorized personnel.</p>	<p>11.1.1 – Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.</p> <p>11.1.2 – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.</p>	<p>Physical access to the data center is restricted to authorized IT Operations staff only.</p>

# Practical Example – Anti-virus Protection

PCI	SSAE16 / SOC2&3	ISO 27001	SOX
<p>5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</p> <p>5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.</p> <p>5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.</p> <p>5.2 Ensure that all anti-virus mechanisms are maintained as follows:</p> <ul style="list-style-type: none"> <li>• Are kept current</li> <li>• Perform periodic scans</li> <li>• Generate audit logs which are retained per PCI DSS Requirement 10.7</li> </ul> <p>5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.</p>	<p>3.5.1 - Anti-virus software with up to date virus signatures are used to protect all Company network devices. Scans are performed on a daily basis.</p> <p>3.5.2 -Anti-virus software security updates are applied based on automatic update timelines.</p>	<p>12.2.1 Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.</p>	<p>Virus protection software at the Network/Gateway level is configured to scan and filter the incoming and outgoing network traffic (Email, HTTP, FTP and other messaging) for real-time detection and quarantine of malicious code.</p>



# IT GOVERNANCE, RISK AND COMPLIANCE (GRC) – Wikipedia

## Definition

GRC is a discipline that synchronizes information and activity across governance, risk management and compliance in order to create efficiency, enable more effective information sharing and reporting and avoid wasteful overlaps. Often interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance.

Governance describes the overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control structures.

RISK Management is the set of processes through which management identifies, analyzes, and, where necessary, responds appropriately to risks that might adversely affect realization of the organization's business objectives.

Compliance means conforming with stated requirements. At an organizational level, it is achieved through management processes which identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), assess the state of compliance, assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and hence prioritize, fund and initiate any corrective actions deemed necessary.

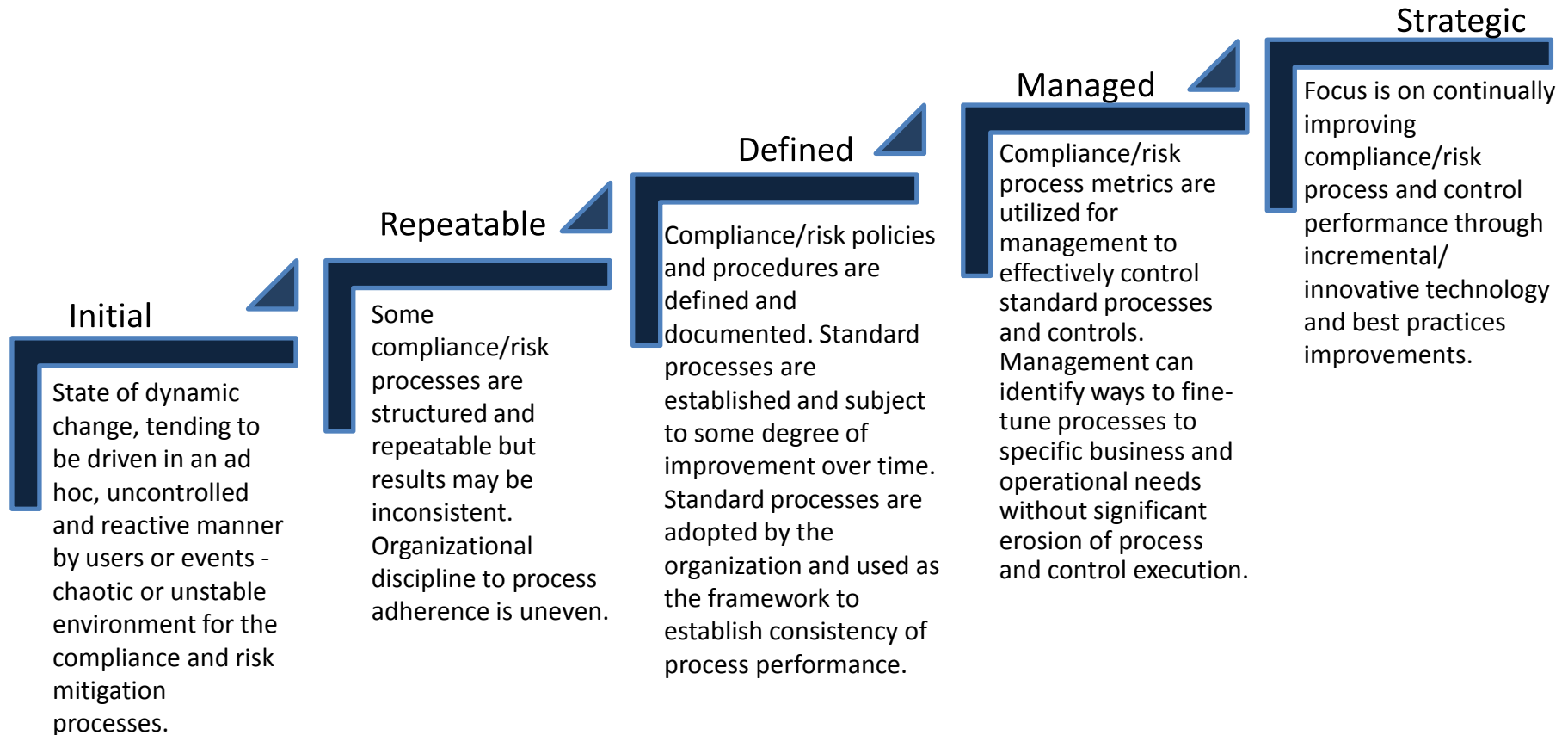


# Framework vs. a Standard

---

	Definition
Framework	Generally accepted, business-process oriented structure that establishes a common language and enables repeatable business processes
Standard	Mandatory requirement, Code of Practice or Specification approved by a recognized external standards organization.

# Compliance/Risk Maturity Model



# GRC in Practice

Strategy and Governance

Risk Categories

Strategic

Tools

Financial

Operational

Process

Information and Communications



# Strategy and Governance

---

- Risk Culture
- Objective Setting
- Decision-making Structure
- Ownership and Accountability
- Strategy and roadmaps:
  - Business
  - Product
  - Compliance

# Process

---

- Risk Identification
- Risk Assessment
- Risk Response
- Risk Monitoring
- Compliance Program Management

# Tools – Policies, SOPs, and Systems

---

- BCP/DR
- Back-up and Restoration
- Security Awareness and Communications
- Risk Assessment
- Access & Authentication
- Vendor Mgmt
- Incident Mgmt
- Privacy
- Asset & Info Classification/Mgmt
- Systems Dev & Mtnce
- Personnel Security
- Configuration Mgmt
- Change Mgmt
- Monitoring Compliance
- Confidentiality
- Security Monitoring

# Information and Communications

---

- Training
- Employee Communications
- Board Reporting and Communications

# Risk Categories

---

- Risk categories will vary by industry
- They represent what is most important to an organization and what is most critical to its growth



# Regulatory Landscape

---

