CFO’s Guide to Managing Technology Risks

June 14, 2011

McGladrey

Assurance ▪ Tax ▪ Consulting

About McGladrey

Ranked fifth-largest assurance, tax, and business consulting provider in the U.S., for RSM McGladrey, Inc. and McGladrey & Pullen, LLP combined

(Source: Accounting Today 2010 Top 100 Firms)

- Nearly 90 offices in the U.S.
- 7,000 employees in the U.S.

Members of RSM International, one of largest global networks of independent accounting, tax, and consulting firms

- Presence in 76 countries
- More than 32,000 people in 736 offices

Provides global resources with a single point of contact

Delivering outstanding client service for over 80 years

McGladrey is the brand under which RSM McGladrey, Inc. and McGladrey & Pullen, LLP serve clients' business needs. The two firms operate as separate legal entities in an alternative practice structure.

Agenda

- Introductions

- Managing Technology Risks
  - Beyond the Fundamentals
  - Real-world Considerations

- Making Compliance Manageable
  - Payment Card Industry (PCI)

- Questions & Answers

CFO is the Top IT Decision Maker

- Most IT organizations report to the CFO, rather than the CEO or any other executive
- CFO plays a vital role in determining IT investment
- CFO reporting can lead to success if the CFO has a deep understanding of IT's value

McGladrey

Achieving Business Value

- Greater return on investments
- Expense reduction
- Legal, statutory and regulatory compliance
- Process, risk, and control efficiencies
- Elimination of redundancies
- Issues and risk prioritization
- Risk mitigation
- More effective resource management

Achieving Business Value

Objectives

- Protecting Information Assets
- Meeting Compliance Requirements (HIPAA, PCI, FISMA, SAS-70, SOX..)
- Optimizing Cash Flow

Challenges

- Lack of skilled and experience resources to support IT risk management
- Integration of IT risks into broader corporate risk management programs
- Fear of unknown security, compliance or disruption of service risks
- Too many compliance requirements

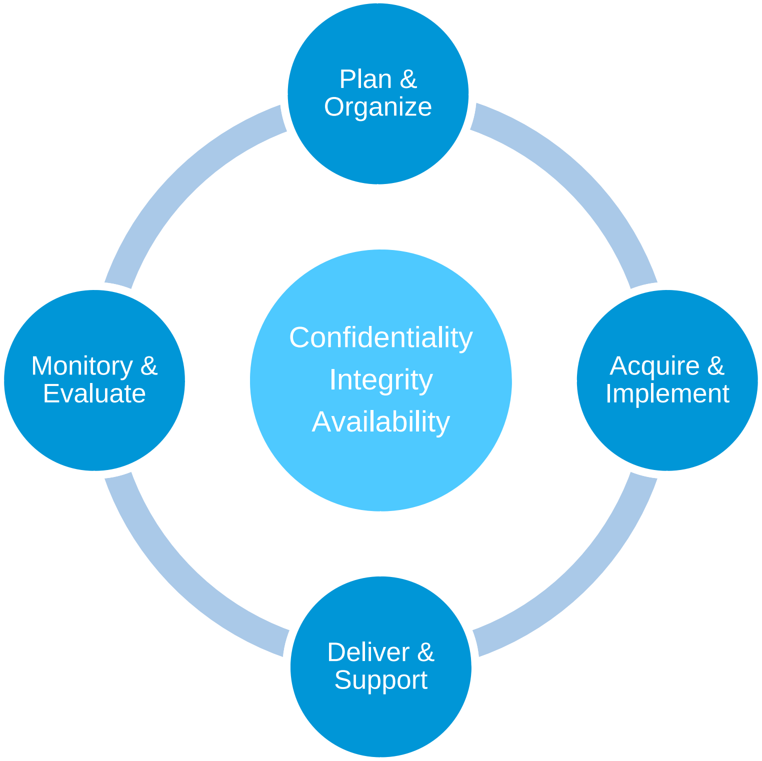
McGladrey

Security is an Investment

- Key Questions To Ask:
  - Have we identified our critical information assets?
  - Do we conduct periodic risk assessments?
  - Do our written security plans & policies address these risks?
  - Have we implemented our security program? Do we monitor it? Do we regularly reassess it?
  - Have we addressed employee training issues regarding security?
  - Have we addressed third-party information security?
  - Are we prepared for a security breach?
  - Do we view security as part of our day-to-day business?
  - In the event of a disaster, how long before our business is operational again? Do we periodically test this?

Fundamentals of Technology Risk Management

- Plan & Organize
  - Define a strategic plan
  - Define technological direction
- Acquire & Implement
  - Identify automated solutions
  - Acquire and Maintain Software and Infrastructure
  - Manage Changes
- Deliver & Support
  - Define and manage service levels
  - Educate and train users
  - Manage help desk incidents
- Monitor & Evaluate
  - Evaluate IT performance
  - Ensure compliance



McGladrey

Drivers of Enterprise Security

Operating environment & operational criteria

Requirements for incident response & crisis communications

Culture & management policies

System interconnectivity and dependencies

Risks, threats, & vulnerabilities assessments

Requirements for business continuity & disaster recovery

Business plan & strategic goals

Legal & cybercrime considerations

Risk Management Programs & Enterprise Security Strategy

Standards, best practices & guidance

Digital assets: Information/data, applications, networks

ROI & financial information

Technological considerations & system architecture

Enterprise Security Program

Security Plan

Security Policies & Procedures

System Architecture

McGladrey

Governance

Technology Risk Management

Governance > Logical Security > Physical Security > Change Management > Monitor Compliance

Overview	Common Questions
▪ Controls surrounding the organizational approach to risk management ▪ Ownership, accountability, and oversight ▪ Effective policies and standards ▪ Corporate culture- Tone at the top	▪ Have we identified our critical information assets? ▪ Do we conduct periodic risk assessments? ▪ In the event of a disaster, how long before our business is operational again? Do we periodically test this? ▪ Do we view security as part of our day-to-day business? ▪ Do our written security plans & policies address our risks?

Industry Observations

- Organizations with effective leadership teams are poised to embrace and promulgate change.
- Do not underestimate the time frame required to implement an effective technology risk program; 2 to 3 years is not usual.
- A common fallacy it to associate all technology and security issues to the IT team alone; rather, these are shared responsibilities.
- Unless business continuity controls are tested, do not rely on their effectiveness to resume critical operations.

Logical Security

Technology Risk Management

Governance → **Logical Security** → Physical Security → Change Management → Monitor Compliance

Overview	Common Questions
▪ Controls surrounding user access & authentication to all systems ▪ Document & Approval of Adds/Changes/Deletes to Access ▪ Unique user ID's ▪ Periodic changing of passwords ▪ Password complexity ▪ Super-User Access ▪ Segregation of Duties ▪ Remote Access	▪ Are we following a formal process to grant and remove user access to systems? ▪ Do I need to hire a new person to meet segregation of duties requirements? ▪ If we implement a formal user access review process and complex passwords, I should be secure, right?

Industry Observations

- Organizations lacking a formal system/application access process have 99% probability of inappropriate access.
- By understanding your system logging capabilities, system audit trails could be used to compensate for segregation of duties risks.
- Logical security controls can be easily undermined by cyber-criminals as a result of poor security patch management practices.

McGladrey

Physical Security

Technology Risk Management

Governance → Logical Security → Physical Security → Change Management → Monitor Compliance

Overview	Common Questions

▪ Controls surrounding access to locations where sensitive information reside
    ▪ Security Guard
    ▪ Biometric Access
    ▪ Key Card Access
    ▪ Locked file cabinets
    ▪ Security Cameras
	▪ Are we following a formal process to grant and remove user access to the premise?
	▪ Are my employees trained respond to “social engineering” behavior?

Industry Observations

- “Protect the innocent” by granting building access on an as needed basis.
- Ensure confidential material is securely stowed or discarded. Unauthorized access to unlocked file cabinets and “dumpster diving” are still prevalent today.
- Publicly available tools exist which can be used perform reconnaissance and exploits from a networked workstation with bootable media access.

Change Management

Overview	Common Questions
▪ Controls surrounding changes to existing systems ▪ Document & approval of change requests ▪ Testing of changes ▪ Separation between development and production ▪ Monitoring access to production	▪ How do I know if I have an effective change management process? ▪ With limited personnel, how can I leverage technology to improve this process?

Industry Observations

- Frequent system outages and performance issues is a typical indicator of a weak change management process.
- This remains one of this most difficult controls to implement effectively. If occasionally problematic, a lack of people, system resources, or training may be the root causes. If consistent, the root cause is likely a weakness in governance controls.

Monitor Compliance

Technology Risk Management

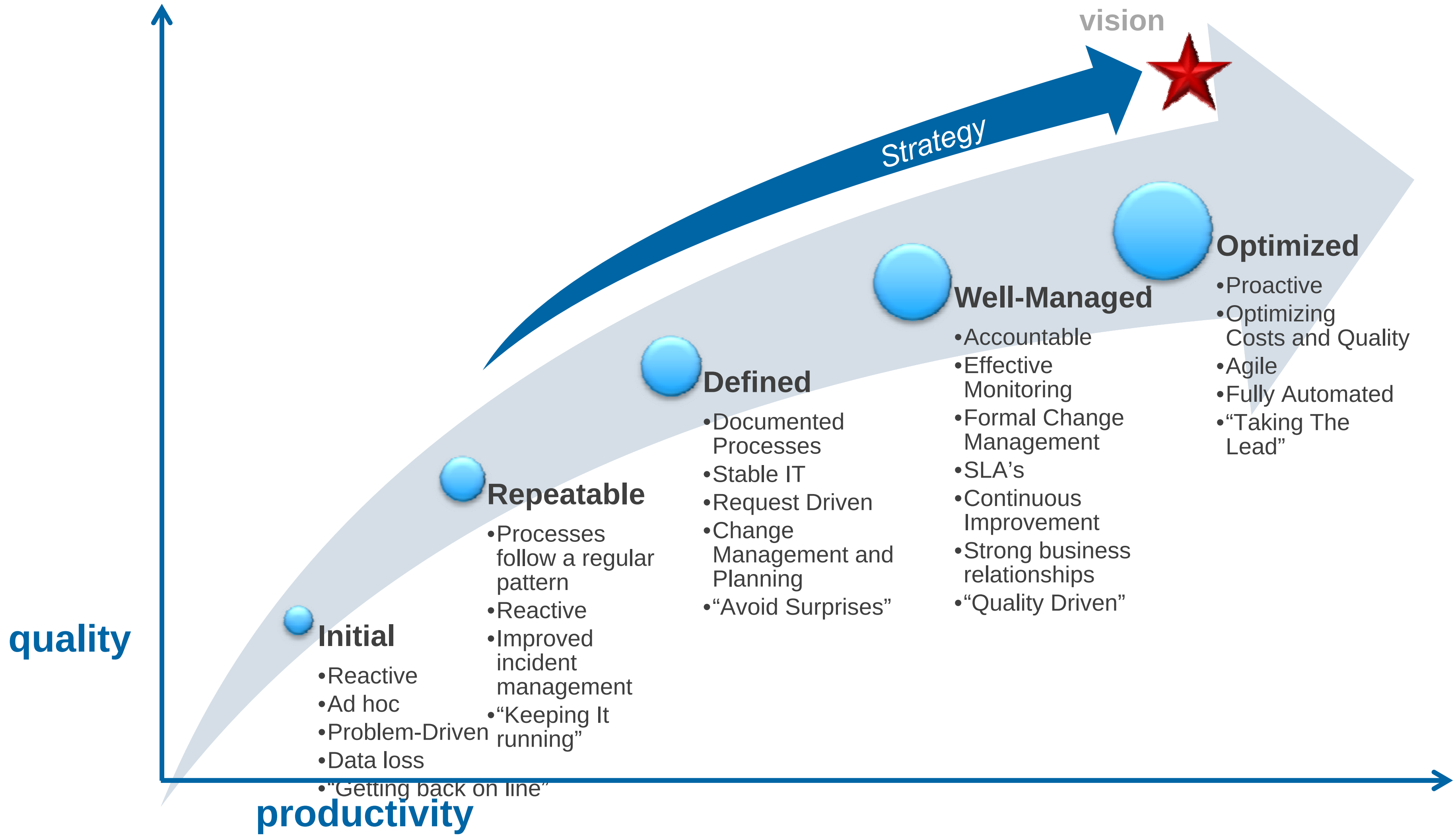
Governance → Logical Security → Physical Security → Change Management → **Monitor Compliance**

Overview	Common Questions
▪ Controls to provide management with organizational views and trend analysis for risks, controls issues, and vulnerabilities ▪ Assess risks with policies, standards, procedures, legal, statuary and regulatory requirements.	▪ Have we implemented our security program? Do we monitor it? Do we regularly reassess it? ▪ Have we addressed employee training issues regarding security? ▪ Have we addressed third-party information security? ▪ Are we prepared for a security breach?

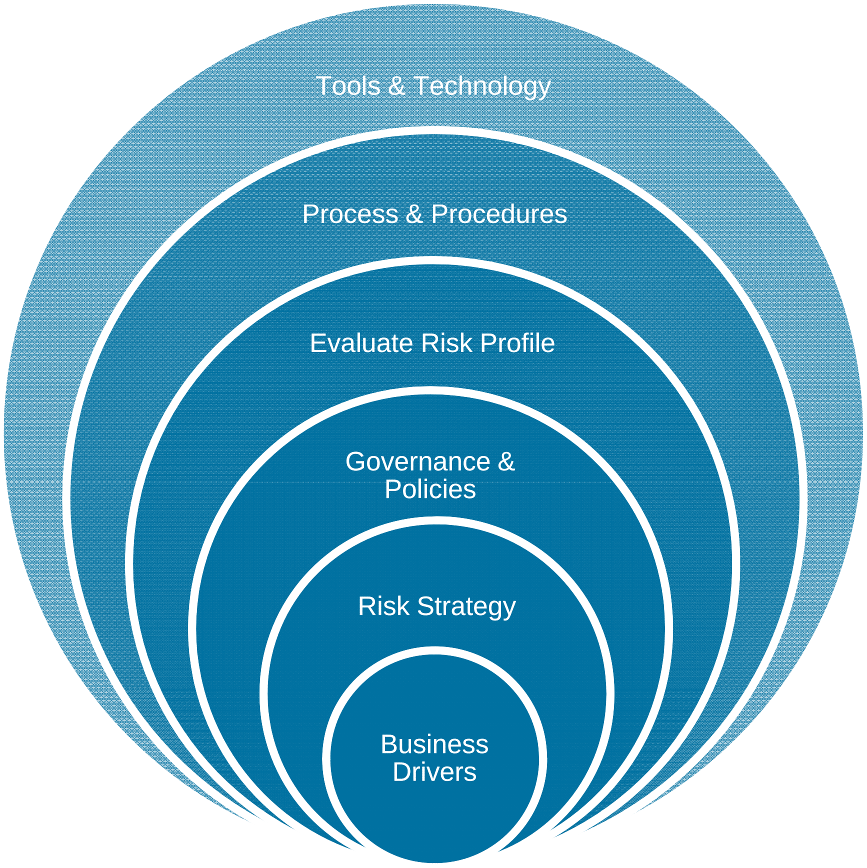
Industry Observations

- Implementing compliance controls after an event is far most costly than implementing them in the first place.
- Risks when activities are outsourced to a third-party does not eliminate them; rather, it changes them. Ensure proper due diligence and also leverage independent audits.
- ABC – **Always Be Connected**. While a positive trend, technology solutions are not a panacea for monitoring governance, risk, security and compliance.

Manage Risks While Maturing



Manage Risks While Maturing



McGladrey

PCI Compliance Case Study

Payment Card Industry (PCI) Overview

- PCI Council is comprised of:
  - Membership Association/Corporation
    - Visa International
    - MasterCard Worldwide
  - Independent Credit Card Networks
    - Discover Financial Services
    - American Express
    - JCB

McGladrey

Reasons for Attaining PCI Compliance

The PCI Council has stated:

> *"All organizations that store, process, or transmit card holder data must be in compliance with the PCI standard"*

- Typically part of the contract for card services
- Penalties and fines
- New data breaches are reported daily
- Safe Harbor status

McGladrey

PCI Levels and Transaction Volume

	American Express	Discover	JCB	MasterCard	Visa (US)
Level 1	2.5+ million transactions annually	6+ million transactions annually	1+ million transactions annually	6+ million transactions annually	6+ million transactions annually
Level 2	50,000 to 2.5 million	1 million to 6 million	Less than 1 million	1 million to 6 million	1 million to 6 million (all channels)
Level 3	Less than 50,000	20,000 to 1 million	N/A	20,000 to 1 million	20,000 to 1 million e-commerce
Level 4	N/A	All other Discover Network merchants	N/A	All other Mastercard merchants	Less than 20,000 e-commerce, and all other merchants processing up to 1 million

McGladrey

Typical PCI Engagement

Advise	Deliver	Assess
Gap Analysis	Remediation	Attestation of Compliance

Achieving PCI Compliance

McGladrey

PCI Data Security Standard

- PCI Data Security Standard – High Level Requirements
  - Build and Maintain a secure network
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

For more information on PCI, visit: www.pcisecuritystandards.org

McGladrey

Questions & Answers

Reggie Nepaul
reginald.nepaul@mcgladrey.com
617.241.1130

Ed Connolly
ed.connolly@mcgladrey.com
617.241.1135

McGladrey

RSM McGladrey, Inc.

www.mcgladrey.com

McGladrey

Assurance ▪ Tax ▪ Consulting