Enterprise Risk Management & Information Technology

Presented by Scott Perry - Slalom Consulting

Agenda

▸ **Introductions**

▸ **Session Objectives**

▸ **Overview of Enterprise Risk Management**

▸ **The Role Of IT**

▸ **IT Governance Model**

▸ **IT Risk Assessment**

▸ **How IT Auditors Add Value**

▸ **Key Summary Points**

▸ **Q&A**

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Introductions

Scott Perry, CPA, CISA

National Leader, IT Risk & Control Solutions, Slalom Consulting

Focuses on areas such as
- **IT Governance**
- **IT Security & Regulatory Compliance**
- **ERM**
- **PKI Audit**

Oversees all methodology and delivery in this specialization area.

Session Objectives

- **Provide an overview and historical context for Enterprise Risk Management (ERM)**
- **Discuss the changing risk landscape and how ERM is evolving in companies today**
- **IT and its emerging role in ERM**
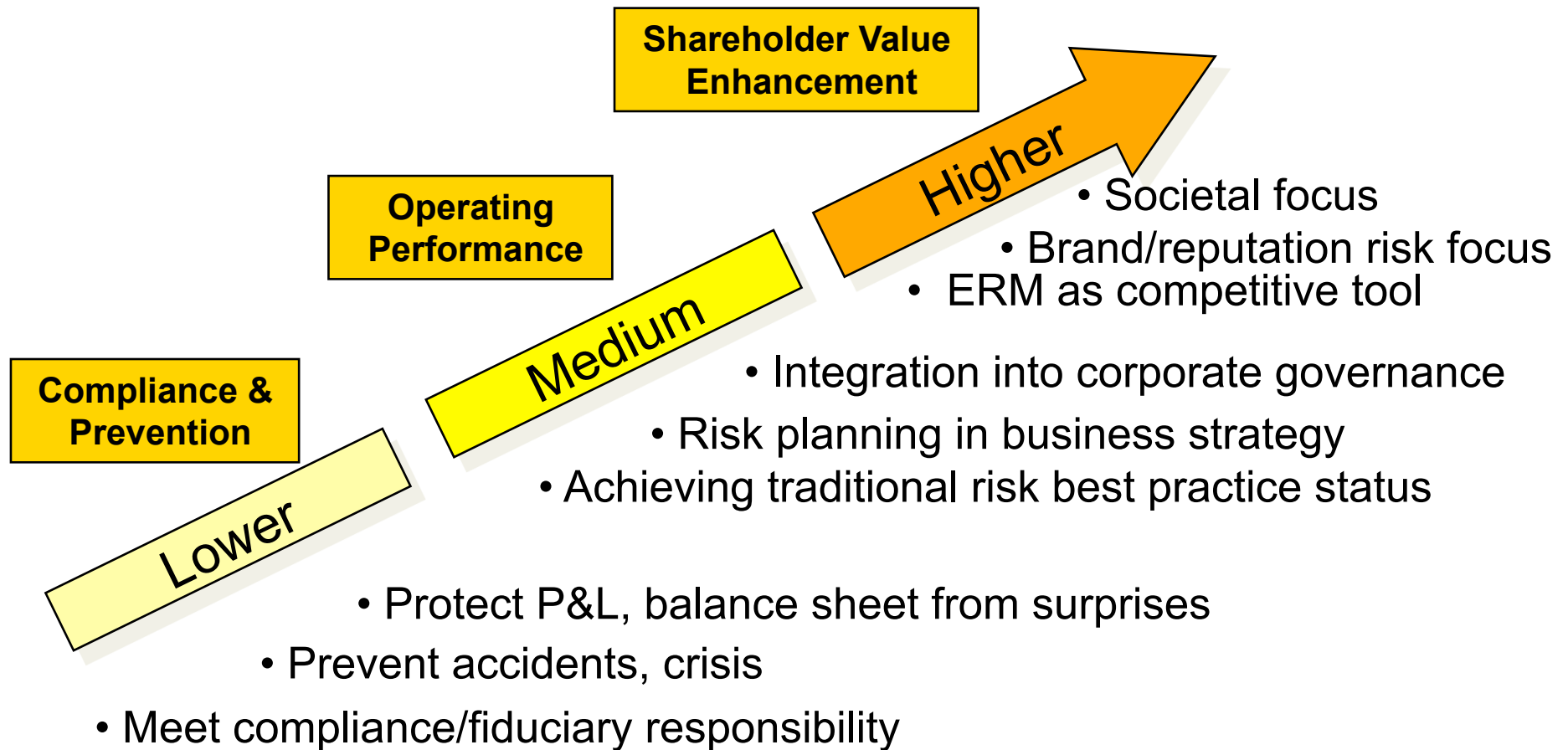- **How IT Auditors can add value in the ERM process**

Types of Business Risk

Compliance Risk
Environmental Risk
Litigation Risk
Reputation Risk
Financial Reporting Risk
Credit Risk
Inherent Risk
Control Risk
Liquidity Risk
Availability Risk
Going Concern Risk

What kinds of
Risks does your
Company Face?

Health & Safety Risk
Ethics Risk
Mergers & Acquisition Risk
Capacity Risk
Supplier Risk
Personnel Risk
Systems Performance Risk
Control Risk
Capital Market Risk
Government Risk
Natural Disaster Risk
Economic Risk
Data Integrity Risk

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Various Levels of Risk

Shareholder Value Enhancement

Operating Performance

Compliance & Prevention

Higher

Medium

Lower

- Societal focus
- Brand/reputation risk focus
- ERM as competitive tool
- Integration into corporate governance
- Risk planning in business strategy
- Achieving traditional risk best practice status
- Protect P&L, balance sheet from surprises
- Prevent accidents, crisis
- Meet compliance/fiduciary responsibility

Risk Management Options

There are several options that management may consider to address risks:

▸Acceptance

▸Avoidance

▸Mitigation

▸Reduction

▸Sharing

Risk Management Framework

Governance

- setting and evaluating performance against objectives
- power to authorize a business strategy and model to achieve objectives

Risk Management

- proactively identifying, rigorously assessing and addressing potential obstacles to achieving objectives
- identifying and addressing risks that the organization will step outside of mandated and voluntary boundaries

Culture

- establishing an organizational climate and individual mindsets that promote trust, integrity and accountability

Compliance

- proactively encouraging and requiring compliance with established policies and boundaries
- detecting noncompliance and responding accordingly

GOVERNANCE

RISK MANAGEMENT

CULTURE

COMPLIANCE

Source – Open Compliance and Ethics Group

Risk Management Framework

The guidelines are organized into four areas:

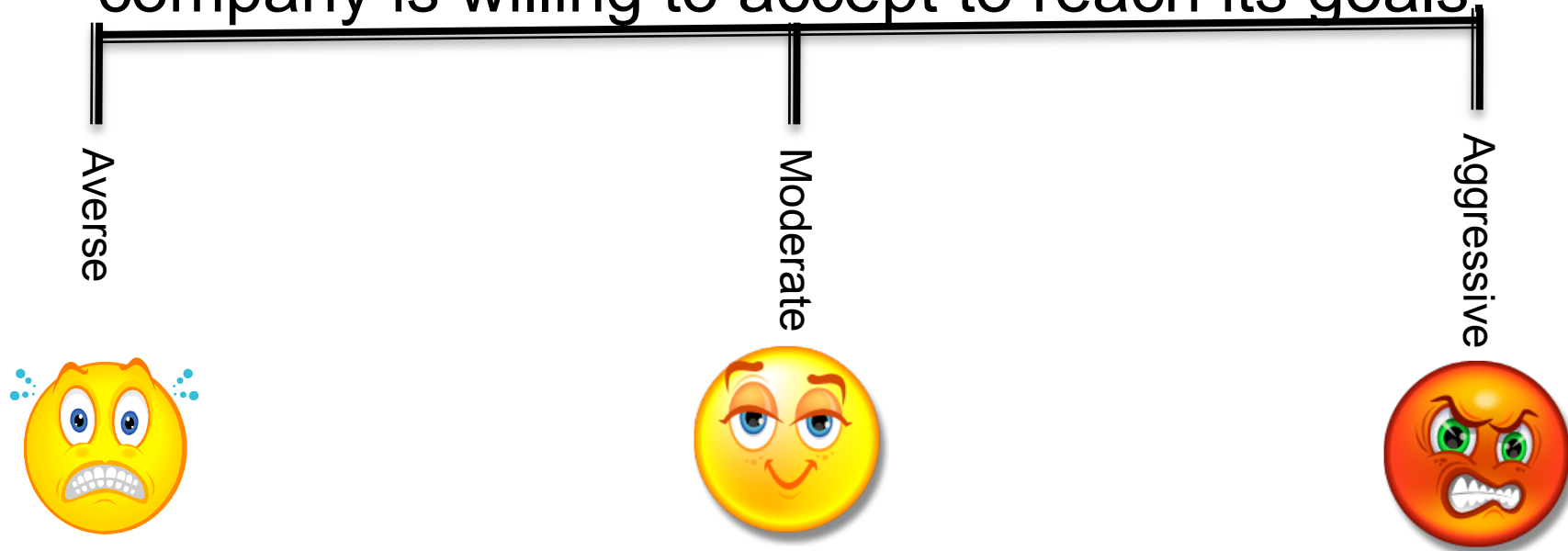| CULTURE	ORGANIZATION / PERSONNEL	PROCESS	TECHNOLOGY
A strong culture helps to guide corporate conduct when formal structures are weak or absent.	Qualified personnel must be responsible for program oversight, strategy and operation.	A program must address several key process areas and topics to ensure they are not only effective, but also efficient and responsive.	An underlying system and technology architecture should enable the process. Organizations should seek to leverage existing investments where possible.

Source – Open Compliance and Ethics Group

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Risk Appetite

Risk appetite is the degree of uncertainty a company is willing to accept to reach its goals.

Averse

Moderate

Aggressive

What is your Company's Risk Appetite?

Evolution Of Risk Management Activities

From	To
Limited strategic influence	Effective support of strategic and business planning
Risk aversion	Proactive risk management
Silo effects and barriers	Integrated, holistic approach
Inconsistent risk reporting	Concise and consolidated reporting
Infrequent risk assessment	Continuous risk assessment & reevaluation
Ambiguous ownership for certain types of risk	Risk ownership assigned in management business and evaluation plans
Closed communication	Open communication
Lack of clear definitions of roles and responsibilities	Risk management roles and responsibilities clearly defined and communicated

Benefits OF ERM

▸ **Better Understanding of Risk Posture**

▸ **More Effective Risk Mitigation**

▸ **Less Business Fear**

▸ **Greater Corporate Support for Critical Business Ventures**

▸ **Improved Corporate Governance**

Benefits of ERM

▸ **Investors are willing to pay a premium for effective risk management**

▸ **Ratings agencies are increasing their focus on risk management.**

Source – Compliance Week

Model Risk Management Process

1. Define scope and objectives
2. Identify boundaries and types of risks
3. Perform an Enterprise Risk Assessment
4. Bucket and prioritize risks
5. Establish Risk Mitigation projects and reduction programs
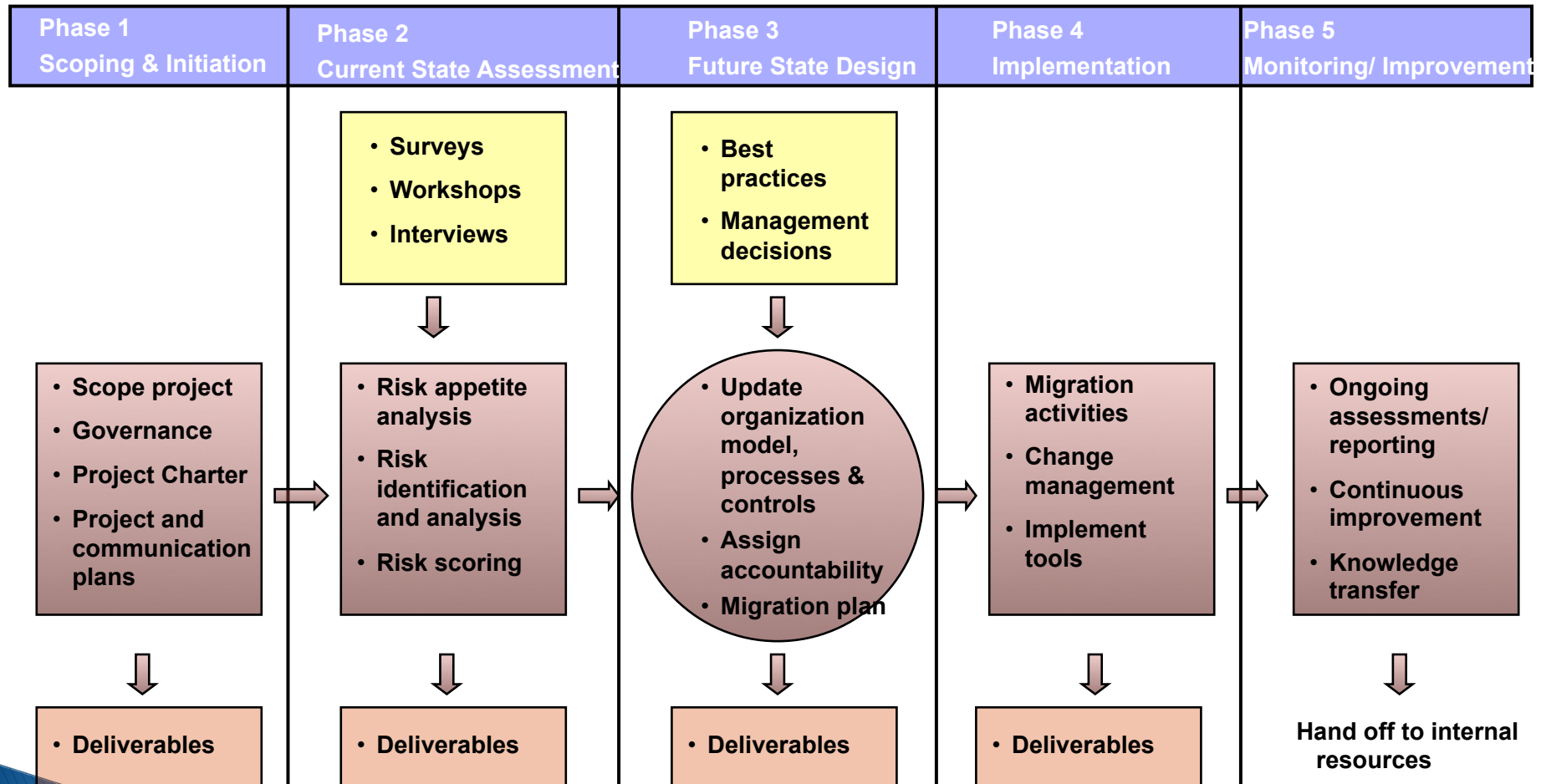6. Institute feedback mechanisms
7. Optimize and refine

Key Success Factors

▸ **Get Executive management Buy-in**

▸ **Establish the end state**

▸ **Create a common taxonomy**

▸ **Evangelize the concept throughout the enterprise**

▸ **Take on only what you can achieve**

▸ **Get both top-down and bottom-up perspectives**
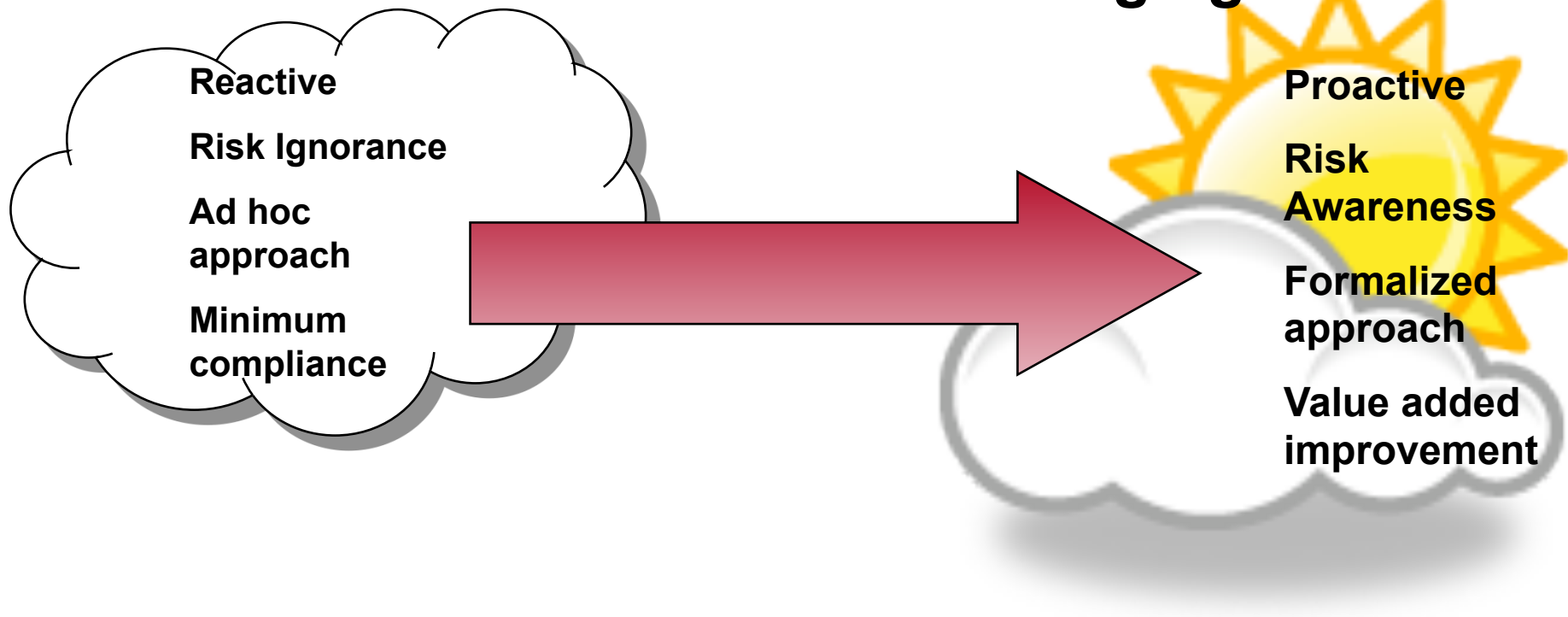
▸ **Get Objective Advice**

Key Success Factors

▸ **Management Acceptance and Ownership**

▸ **Treat ERM like a Mission Critical Project**

▸ **Coordinate ERM for other Compliance and Risk Mitigation Efforts**

▸ **Create a Central Repository for Risks**

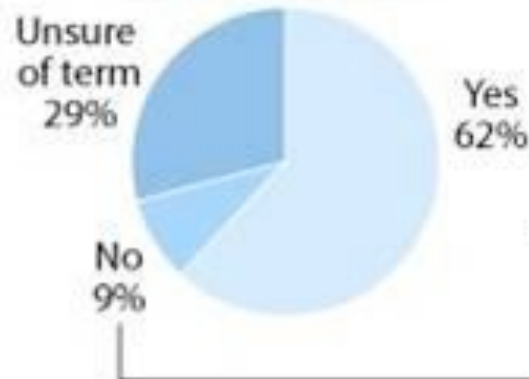▸ **Link To Performance Measures**

ERM Implementation Project Phases

Phase 1 Scoping & Initiation	Phase 2 Current State Assessment	Phase 3 Future State Design	Phase 4 Implementation	Phase 5 Monitoring/ Improvement
	• Surveys • Workshops • Interviews	• Best practices • Management decisions		
• Scope project • Governance • Project Charter • Project and communication plans	• Risk appetite analysis • Risk identification and analysis • Risk scoring	• Update organization model, processes & controls • Assign accountability • Migration plan	• Migration activities • Change management • Implement tools	• Ongoing assessments/ reporting • Continuous improvement • Knowledge transfer
• Deliverables	• Deliverables	• Deliverables	• Deliverables	Hand off to internal resources

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

How Does IT Look At Risk ?

The IT risk focus is changing

Reactive

Risk Ignorance

Ad hoc approach

Minimum compliance

Proactive

Risk Awareness

Formalized approach

Value added improvement

IT is Getting Onboard

"Does your company have an initiative underway in the area of risk management and compliance?"

Unsure of term 29%

Yes 62%

No 9%

Percentage of CIOs who have implemented or are actively implementing IT's own processes for risk management and compliance

59%

25%

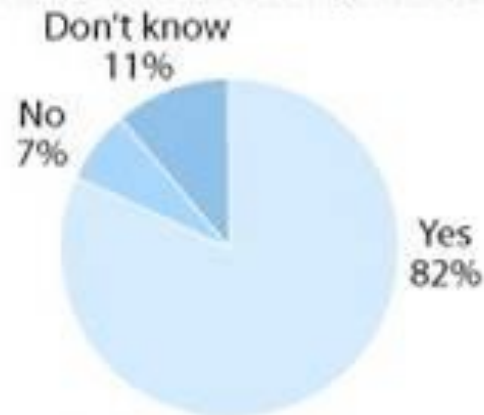Base: 231 CIOs at North American companies

Source Forrester Research

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT is Getting Onboard

"Are your IT risk management and compliance efforts integrated with your company's overall risk management and compliance efforts?"

Don't know
11%

No
7%

Yes
82%

Base: 141 CIOs at North American companies

Source Forrester Research

The Role Of IT in Managing Risk

Yesterday – Reacting and Firefighting

Today – Some are proactively managing IT risk and compliance

Tomorrow - Risk central nervous system

Drivers For Change

There are many interdependent IT risks

Increased liability and regulatory oversight

Companies are formalizing IT risk and compliance

IT is a core components of operational risk

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Has Responded

Huge adoption of IT governance, security and operational frameworks

IT is leveraging:
- ▸ Better integration
- ▸ Tools & Templates
- ▸ Incentives
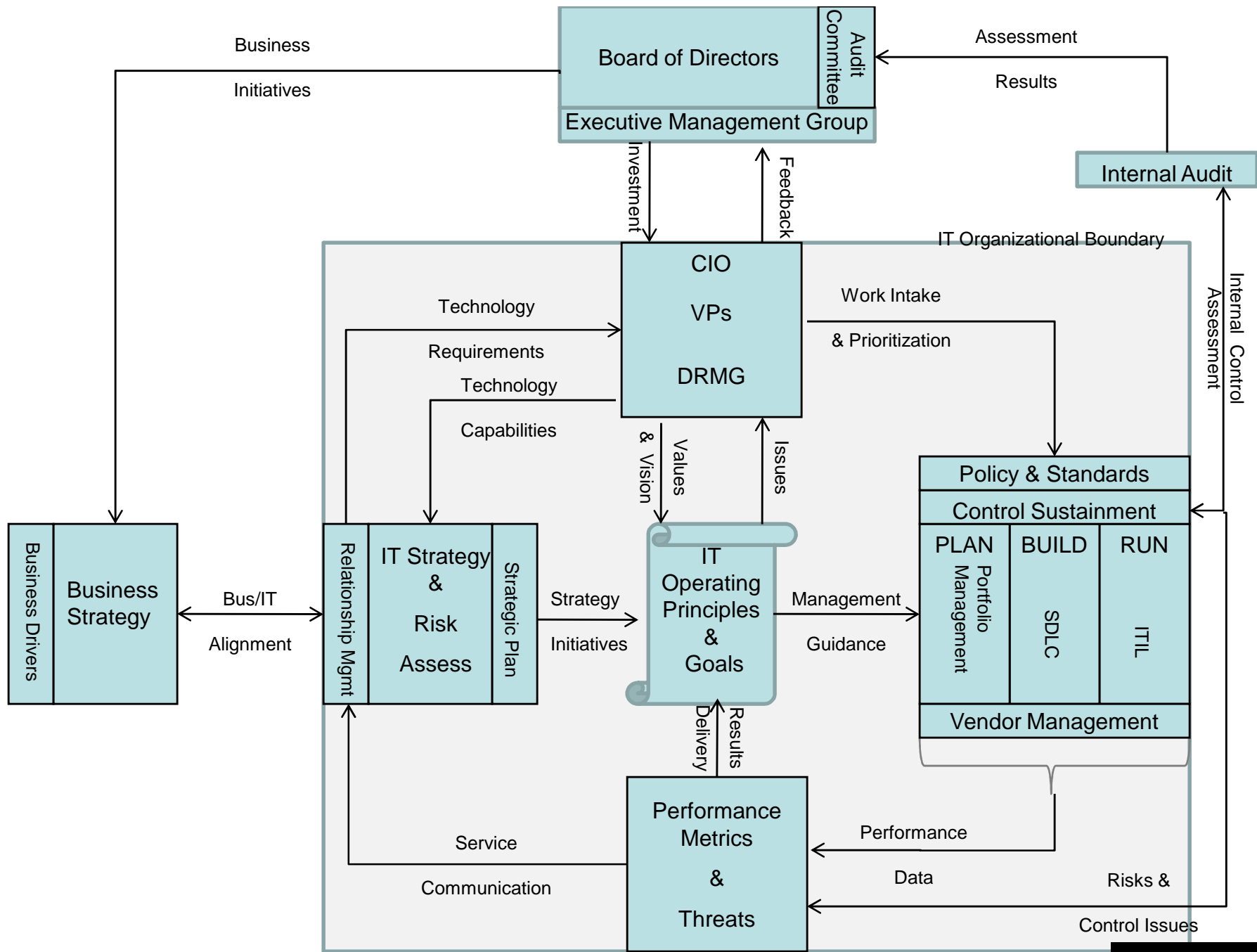
Executive Management Reporting

Dashboards, scorecards and metrics allow for better IT performance and risk management

Developing A Governance Model

- ▸ **Give IT a prominent seat at the risk table**
- ▸ **Appoint IT risk and compliance focal points**
- ▸ **Develop an IT risk and compliance strategy**
- ▸ **Develop IT measurements and feedback mechanisms**

IT Governance Framework

Advantages Of Control Frameworks

▸ **Consistent and Defensible**

▸ **Tailored for progressive implementation**

▸ **Aligns IT process with business goals/objectives and regulatory requirements**

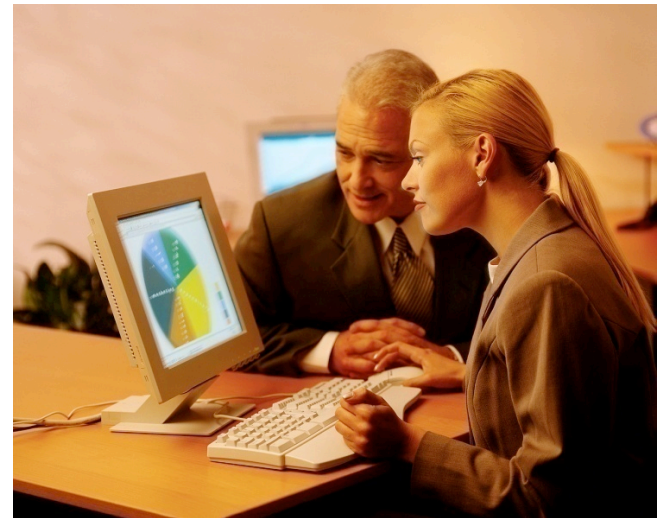▸ **Educates Management and executives to better manage risks associated with IT**

Role Clarification is Key

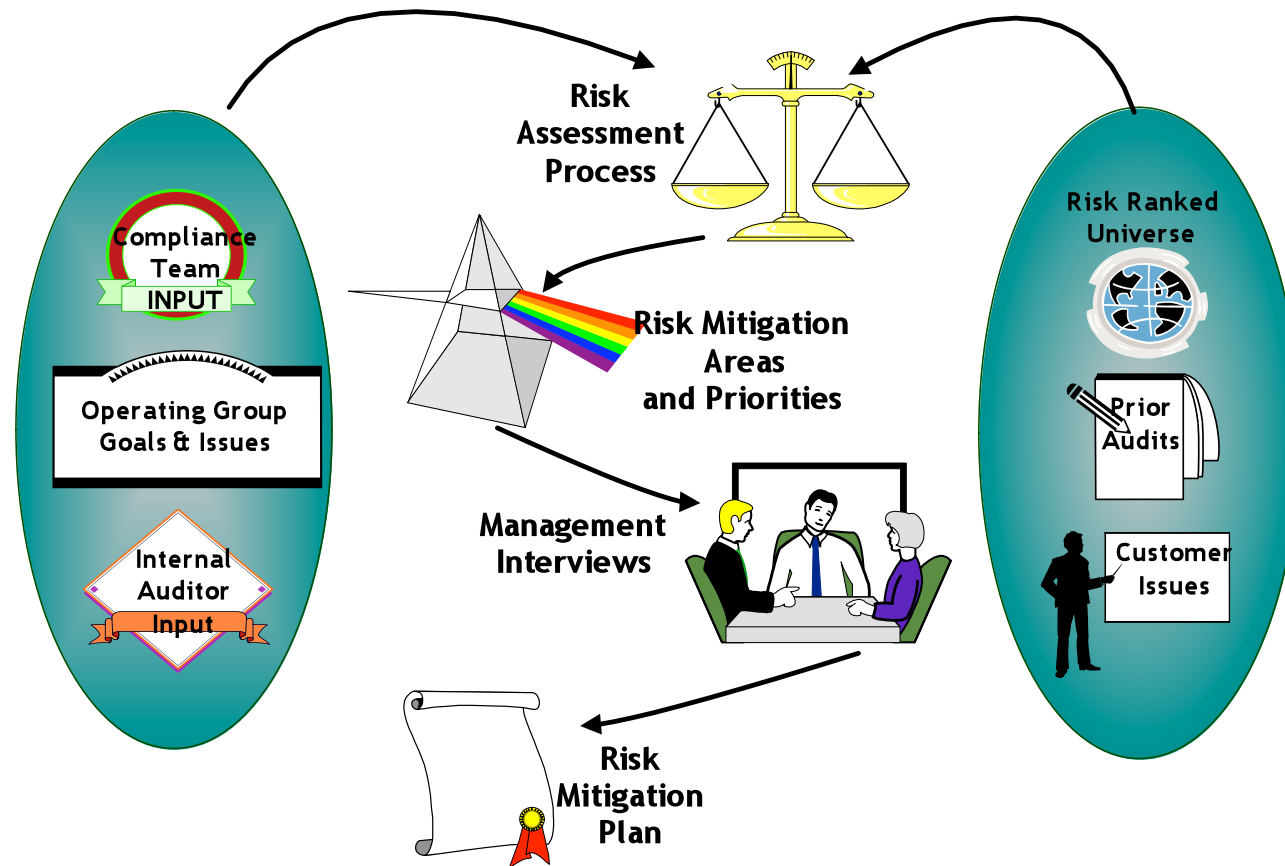| Stakeholder	Role
Director of Audit	Designs audit plans based on risks
General Counsel	Translates regulatory reqs
CFO	Validates control strength
Chief Risk Officer	Creates control structures
Director of Procurement	Protects against vendor access
CIO	Manages IT risk program

How Do You Approach IT Risk Assessments ?

The same way as enterprise risk

IT should influence the strategic opportunities and benefits identified by the enterprise
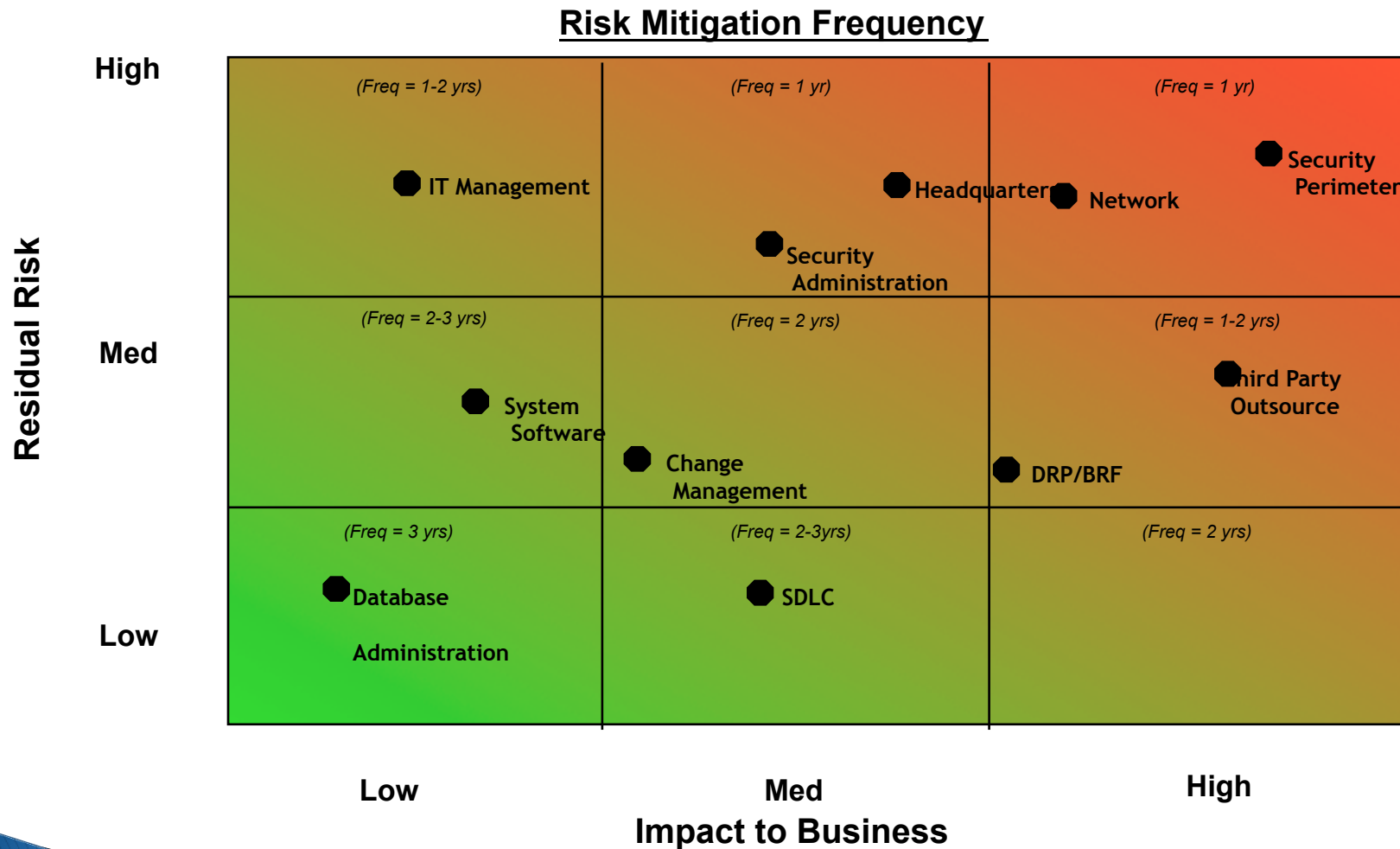
ERM Planning Methodology

IT Risk Assessment Dashboard

The IT Risk Assessment Dashboard graphically depicts how well inherent risks in IT Resources are controlled by the organization

Risk Attributes

IT Resources	Availability	Security	Integrity	Maintainability	Compliance
Data					
Applications					
Infrastructure					
Facilities					
Personnel					

Heat Map

Risk Mitigation Frequency

Residual Risk / Impact to Business heat map:

- **High Residual Risk:**
  - (Freq = 1-2 yrs) — IT Management
  - (Freq = 1 yr) — Headquarters, Security Administration
  - (Freq = 1 yr) — Network, Security Perimeter
- **Med Residual Risk:**
  - (Freq = 2-3 yrs) — System Software
  - (Freq = 2 yrs) — Change Management
  - (Freq = 1-2 yrs) — Third Party Outsource, DRP/BRF
- **Low Residual Risk:**
  - (Freq = 3 yrs) — Database Administration
  - (Freq = 2-3yrs) — SDLC
  - (Freq = 2 yrs)

Impact to Business: Low — Med — High

How Auditors Add Value

Be the In-house Expert on Risk

▸ **Education on IT risk frameworks**

▸ **Determine levels of process maturity**

▸ **Leverage prioritization and continuous process improvement**

Be a Facilitator

▸ **Taxonomy to bridge the business-technology gap**
▸ **Control "rogue" IT activities**

Key Summary Points

- **Critical success factors in any ERM effort:**
  - **Clear ownership and accountability of risk**
  - **Realistic expectations of success of risk control plans**
  - **Ongoing communications, "governance" processes to continually re rank risks, and identify new ones**

- **ERM is ultimately about changing culture and behavior, driving decision making and measurable results**

Key Summary Points

Covey Quadrant

Quadrant I: Urgent and Important	Quadrant II: Important and Not Urgent
To Do: • • • • • • •	To Do: • • • **ERM** • • •
Quadrant III: Urgent and Not Important	**Quadrant IV: Not Urgent and Not Important**
To Do: • • • • • • •	To Do: • • • • • •

Q&A – Contact Information

Scott Perry
Scott.perry@slalom.com