
# Enterprise Risk Management & Information Technology

Presented by Scott Perry and Gary Ross
Slalom Consulting, San Francisco

ISACA® Serving IT Governance Professionals
San Francisco Chapter

SLALOM CONSULTING race to win

# Agenda

- Introductions
- Session Objectives
- Overview of Enterprise Risk Management
- The Role Of IT
- How IT Auditors Add Value
- Key Summary Points
- Q&A

# Introductions

**Gary Ross, CA, CISA**

Regional Lead, Quality & Compliance Solutions, Slalom Consulting

Gary leads our Quality & Compliance Solutions team in San Francisco. He is a former KPMG Risk and Advisory Services Director and Williams Sonoma VP of Internal Audit. Gary has over 17 years of professional experience as a senior financial, operational and IT auditor.

**Scott Perry, CPA, CISA**

National Director, Quality & Compliance Solutions, Slalom Consulting

National Service Leader in Corporate Compliance, Internal Audit, IT Risk & Control, Security & Privacy, and Quality Improvement & Optimization. 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

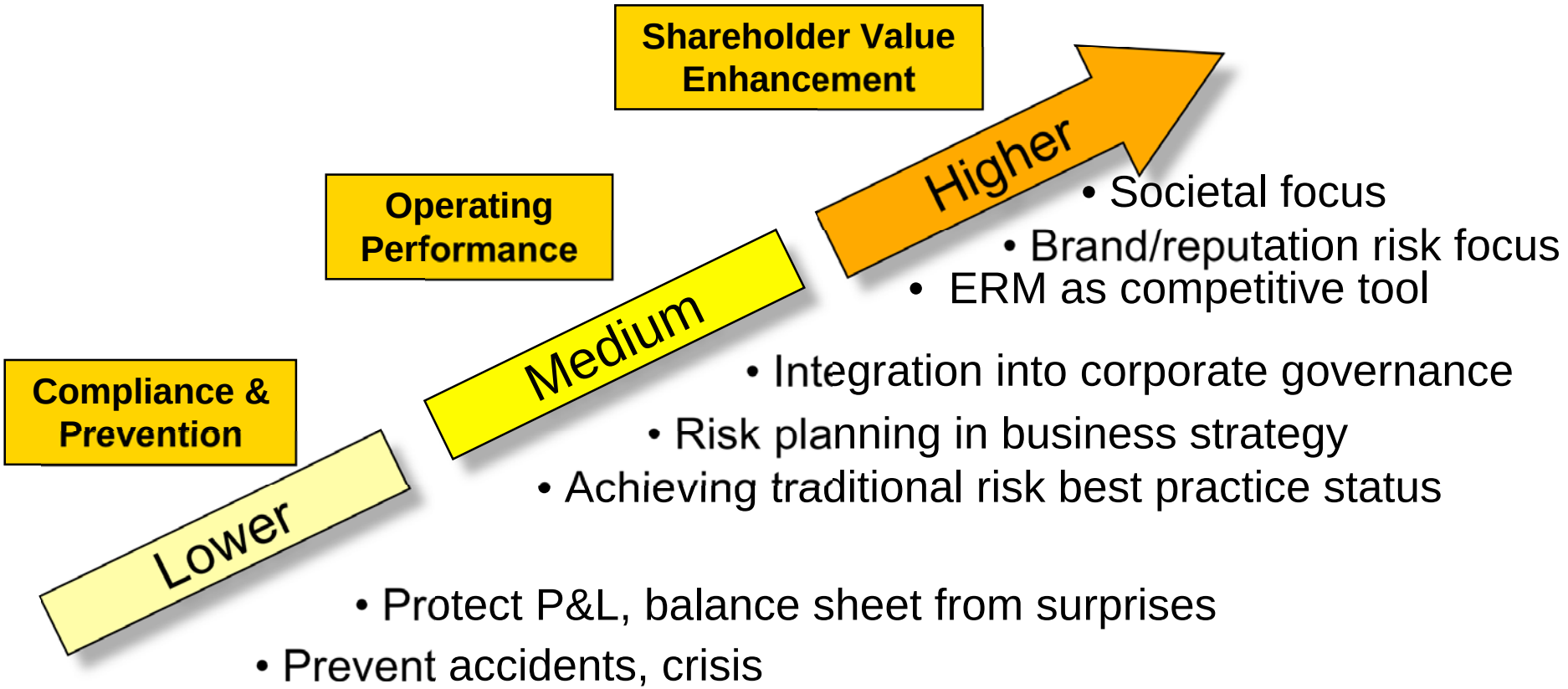
SLALOM CONSULTING
race to win

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

# Overview Of ERM
# Various Levels of Risk



SLALOM CONSULTING
race to win

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

- Acceptance
- Avoidance
- Mitigation
- Reduction
- Sharing

# Overview OF ERM
# 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

# Overview OF ERM
# Risk Management Framework

SLALOM CONSULTING
race to win

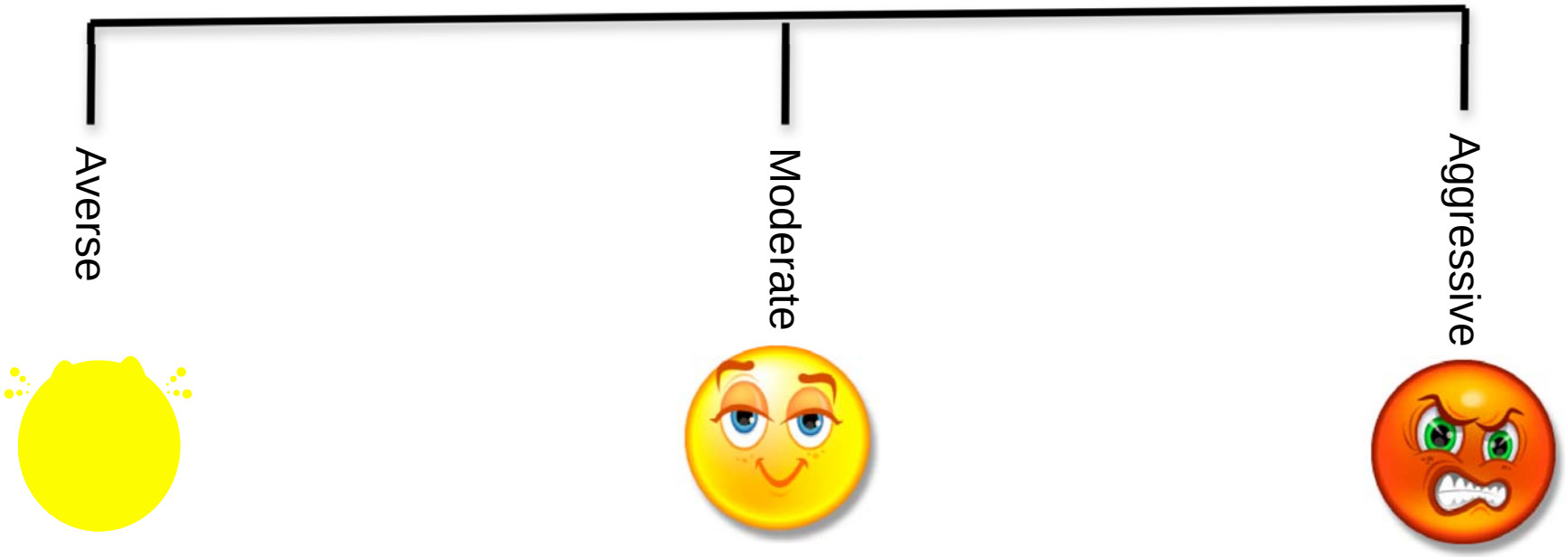
**The guidelines are organized into four areas:**

| 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

# Overview OF ERM
## Risk Appetite

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




What is your Company's Risk Appetite?

# Overview OF ERM
# Evolution Of Risk Management Activities

SLALOM CONSULTING
race to win

| 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 |

# Overview OF ERM
# Benefits OF ERM

SLALOM CONSULTING
race to win

- **Better Understanding of Risk Posture**
- **More Effective Risk Mitigation**
- **Less Business Fear**
- **Greater Corporate Support for Critical Business Ventures**
- **Improved Corporate Governance**

# Overview OF ERM
# Benefits OF ERM

SLALOM CONSULTING
race to win

- **Investors are willing to pay a premium for effective risk management**
- **Ratings agencies are increasing their focus on risk management.**

Source – Compliance Week

# Overview OF ERM
## Model Risk Management Process

SLALOM CONSULTING
race to win

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**

# Overview OF ERM
# Key Success Factors

SLALOM CONSULTING
race to win

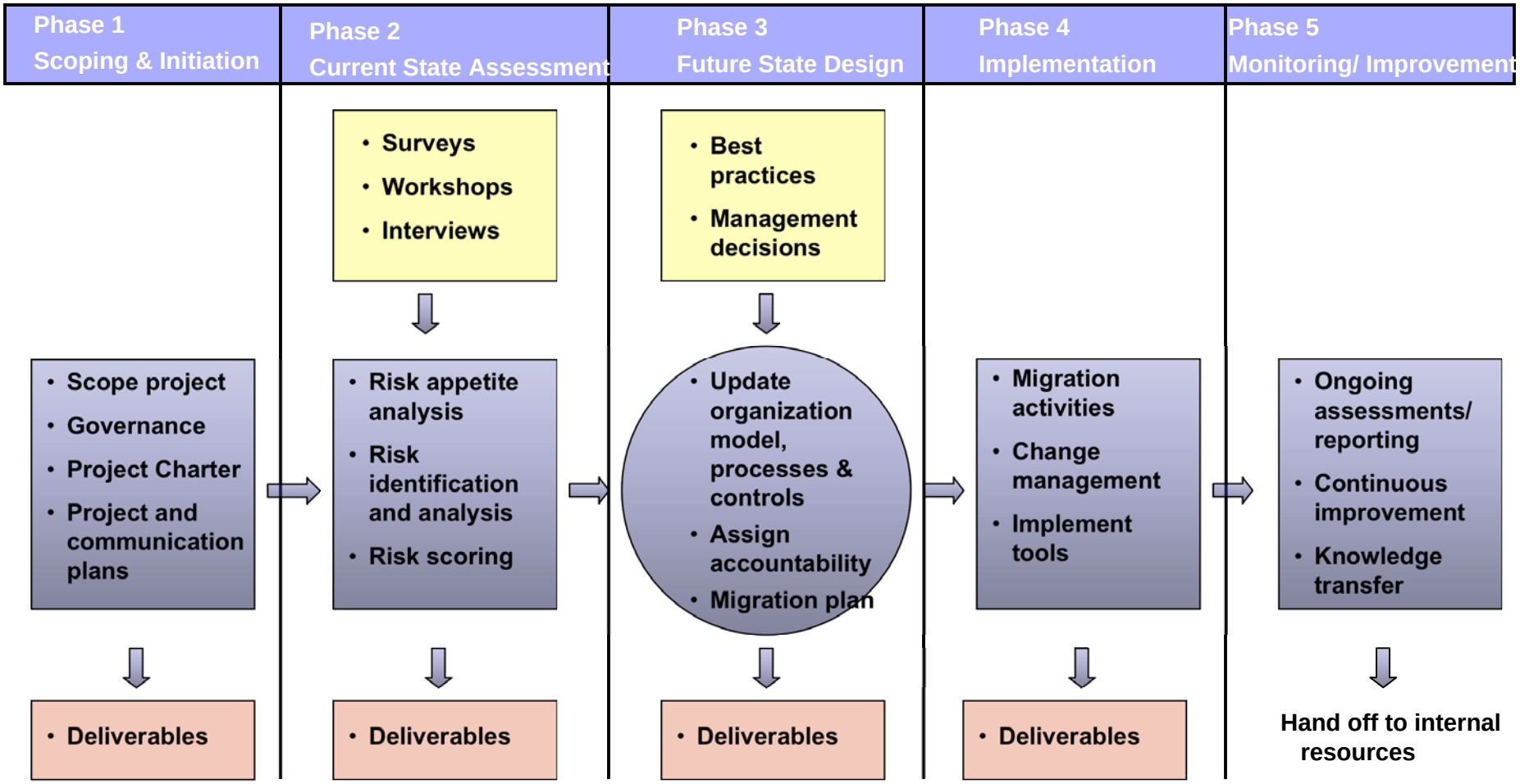
- **Get Executive management Buy-in**
- **Establish the end state**
- **Create a common taxonomy**
- **Evangelize the concept throughout the enterprise**
- **Take on only what you can achieve**
- **Get both top-down and bottom-up perspectives**
- **Get Objective Advice**

# Overview OF ERM
## Key Success Factors

SLALOM CONSULTING
race to win

- **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**

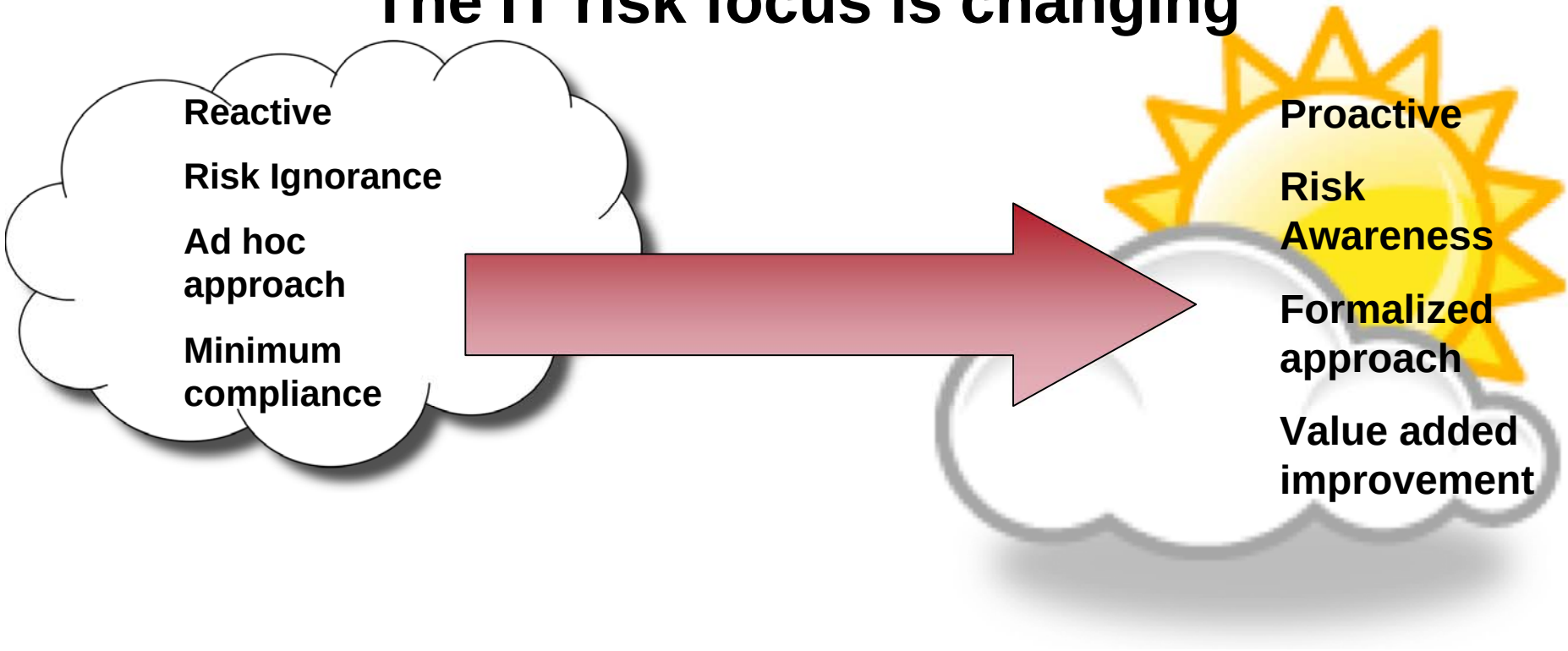
# Overview OF ERM
# An ERM Implementation Project



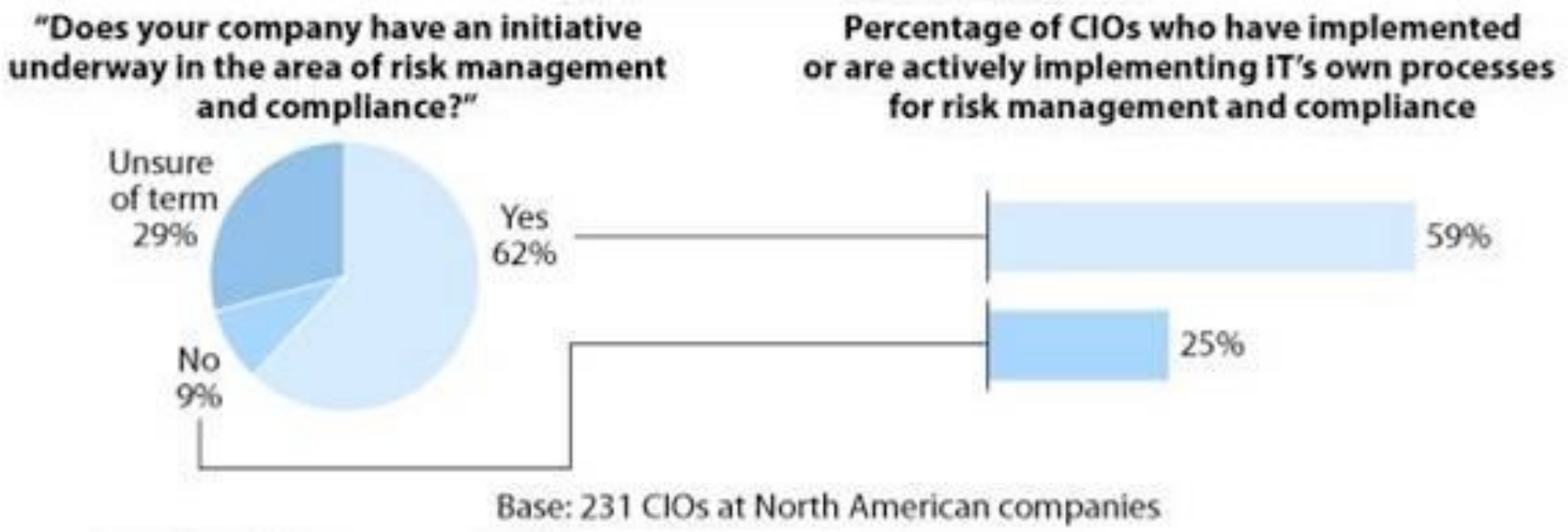
# The Role Of IT
# How Does IT Look At Risk ?

SLALOM CONSULTING
race to win

## The IT risk focus is changing

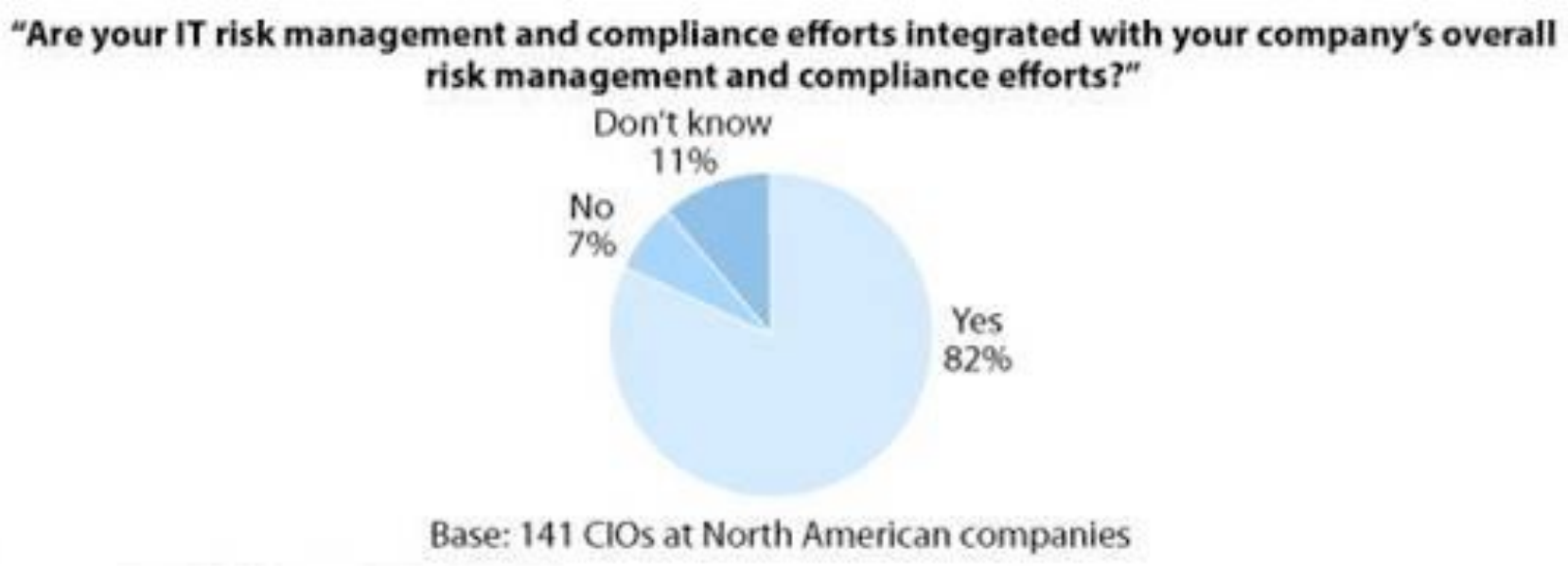


# The Role Of IT
# IT Is Getting Onboard




Source Forrester Research

# The Role Of IT
# IT Is Getting Onboard




Source Forrester Research

# The Role Of IT

Yesterday – Reacting and Firefighting

Today – Some are proactively managing IT risk and compliance

Tomorrow - Risk central nervous system

# The Role Of IT
# Drivers For Change

SLALOM CONSULTING
race to win

**There are many interdependent IT risks**

**Increased liability and regulatory oversight**

**Companies are formalizing IT risk and compliance**

**IT is a core component of operational risk**

SLALOM CONSULTING
race to win

# Huge adoption of IT governance, security and operational frameworks

# The Role Of IT

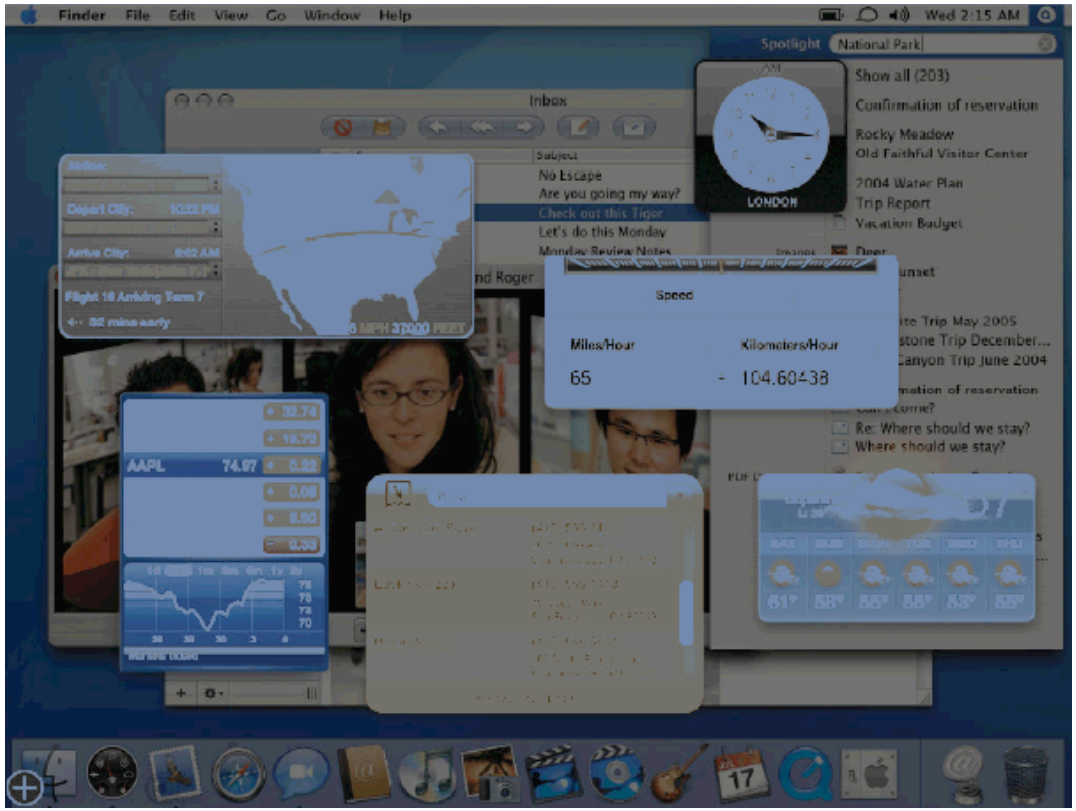
IT is leveraging:

- Better integration
- Tools & Templates
- Incentives

# The Role Of IT

SLALOM CONSULTING
race to win

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



# The Role Of IT
# Developing A Governance Model

SLALOM CONSULTING
race to win

- **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**

SLALOM CONSULTING
race to win

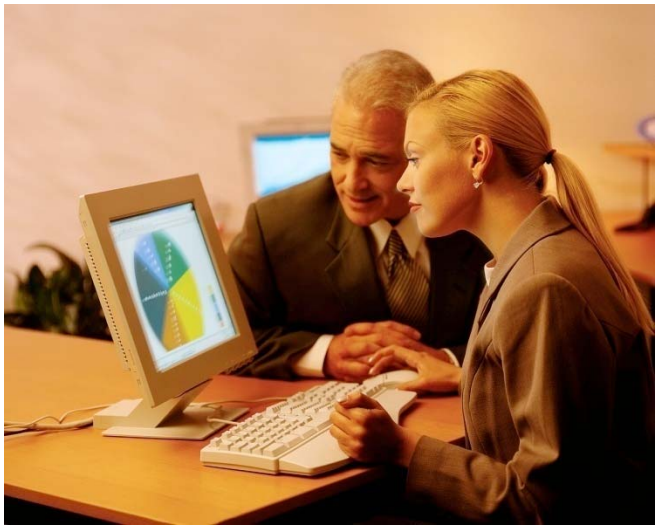
# Role Clarification Is Key

| 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 |

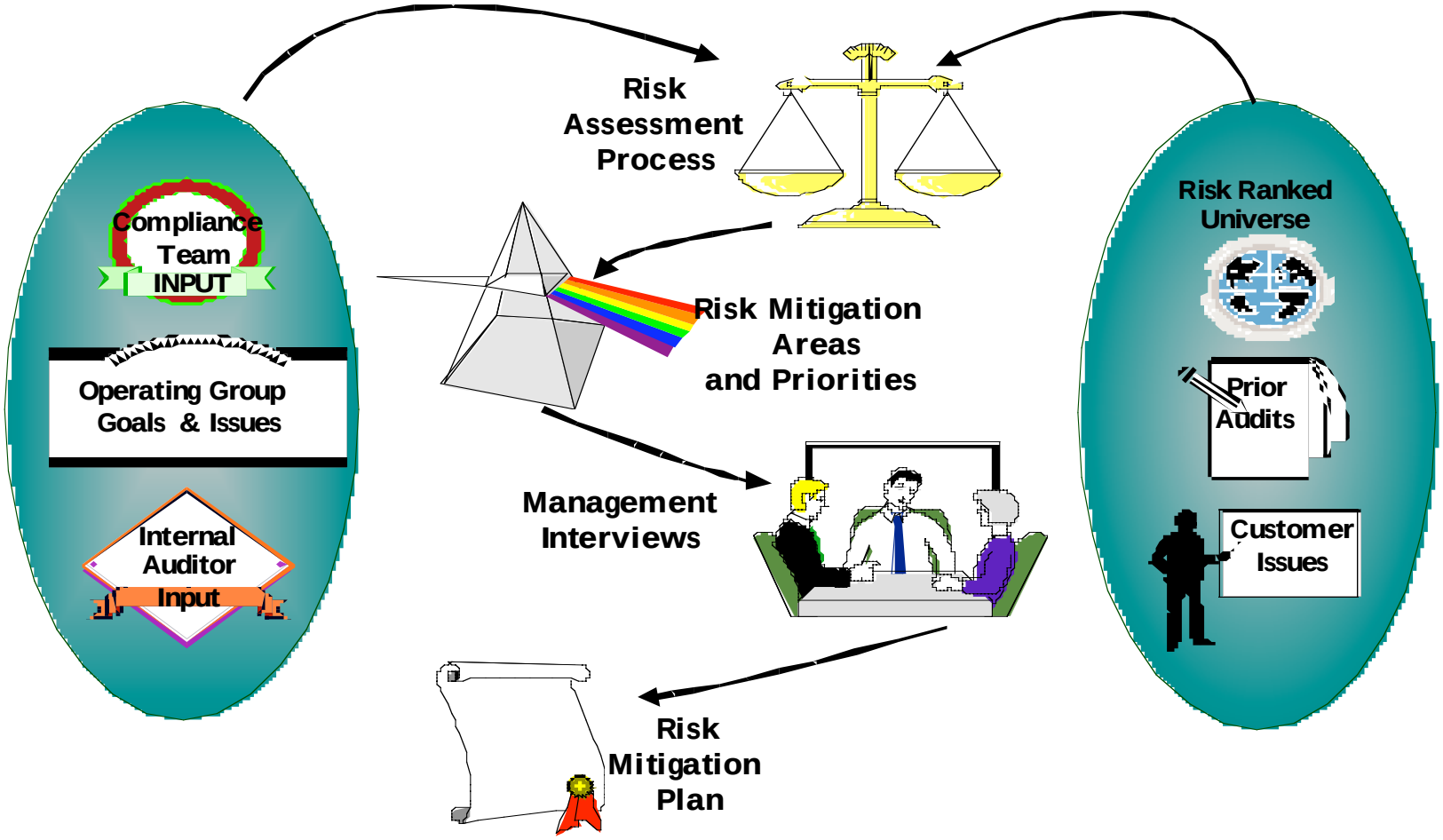
# The Role Of IT
## How Do You Approach IT Risk Assessments ?

**The same way as enterprise risk**

**IT should influence the strategic opportunities and benefits identified by the enterprise**

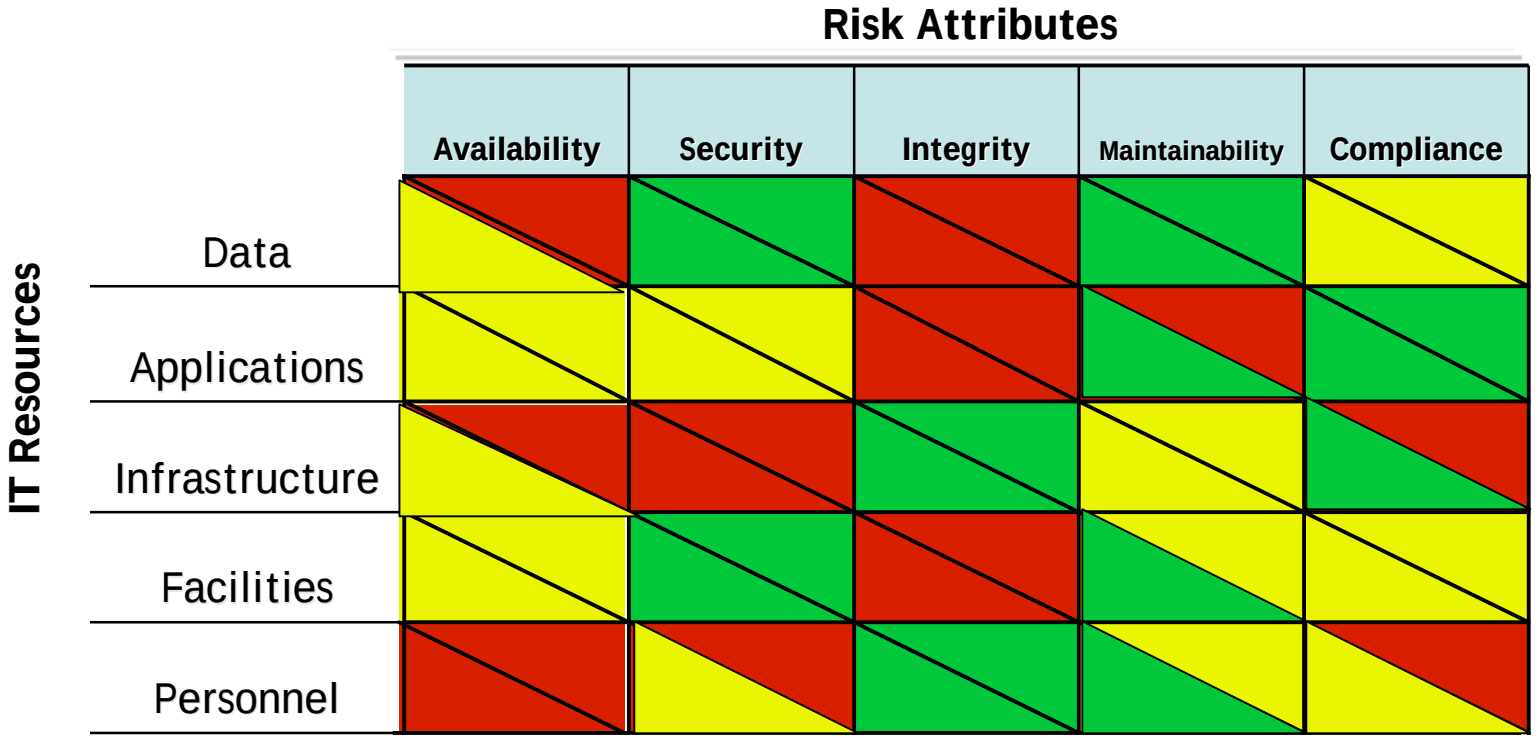


# ERM Planning Methodology

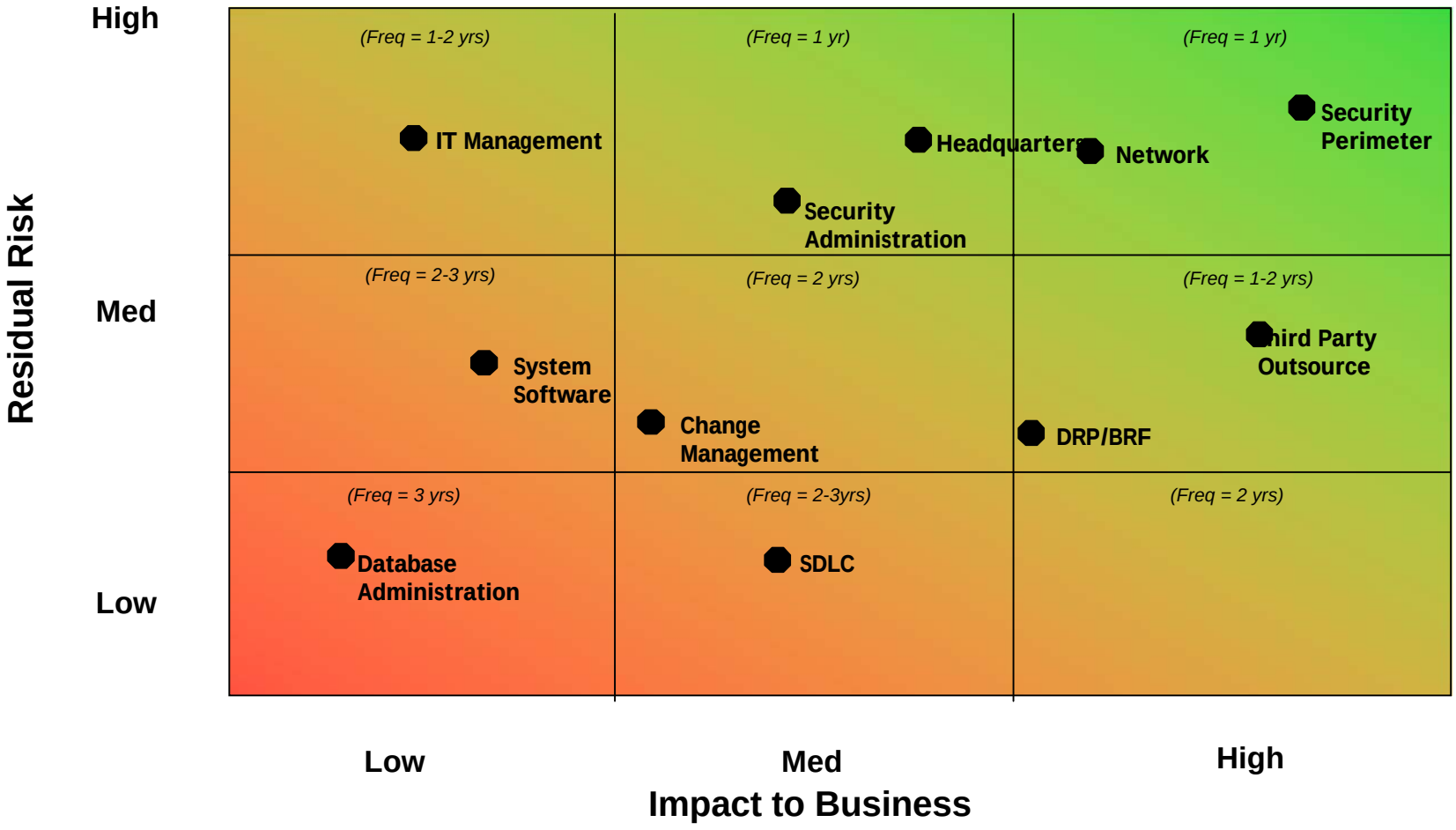


# IT Risk Assessment Dashboard

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



# IT Risk Mitigation Frequency Map



# How IT Auditors Add Value
# Be The In-house Expert on Risk

SLALOM CONSULTING
race to win

- **Education on IT risk frameworks**
- **Determine levels of process maturity**
- **Leverage prioritization and continuous process improvement**

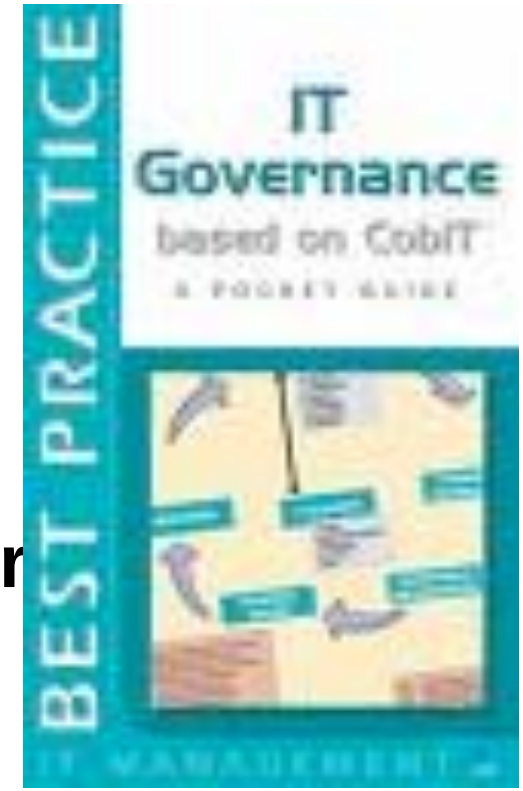
# How IT Auditors Add Value
## Be A Facilitator

SLALOM CONSULTING
race to win

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

# How IT Auditors Add Value
## 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 understand and better manage risks associated with IT**



# How IT Auditors Add Value
## Integrating frameworks into the IT Audit function

- **Map framework to regulatory guidelines**
- **Map scheduled audits to detailed control objectives**
- **Analyze, document and validate results**
- **Report to stakeholders on controls and risks**

# 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: |
| Quadrant III: Urgent and Not Important | Quadrant IV: Not Urgent and Not Important |
| To Do: | To Do: |

ERM

## Q&A – Contact information

# Thank You for your time

Gary Ross
garyr@slalom.com

Scott Perry
Scott.perry@slalom.com