How Internal Audit Can Help Promote Effective ERM

Alan N. Siegfried, MBA, CPA, CIA, CISA, CBA, CRMA, CFSA, CCSA, CITP, CGMA, CSP

June 18, 2014

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Alan Siegfried Professional Bio

- Principal and Managing Director, Quetzal GRC, LLC
- Over 30 years of private and public sector experience in accounting, internal auditing, risk management, internal controls, information technology auditing processes, operations, and business processes and strategy
- Board and Audit Committee member Bon Secours Health System, Audit Committee member UNICEF
- Former Internal Audit Partner at Ernst & Young, Deloitte and Grant Thornton
- Former Director of Internal Audit Bank-Fund Staff FCU
- Former Auditor General Inter-American Development Bank and Chief Audit Executive First Maryland Bancorp
- Former Chairman of Board and member of the IIA's North American Board and member of the IIA's Professional Certification Board
- Widely published and frequent speaker at international internal auditing and risk management events, teach graduate internal audit courses U of MD
- Holds 11 professional auditing, risk management and accounting related designations and certifications

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Presentation Topics

- Risk and Risk Management
- Characteristics of Effective Risk Management
- Role of Internal Audit
- Consultant vs. Evaluator
- Conclusions

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Credit Union ERM – Why we are here

- Enterprise Risk Management is becoming top of mind for many credit unions
  - Board/supervisory committee members
  - Senior management
  - Regulatory examiners
  - External auditors
- Credit unions want to more clearly understand:
  - The benefits of ERM
  - The goals, objectives, and deliverables of ERM
  - The most efficient way to implement ERM

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Risk Management Related Trends

And, they are interconnected – with a cascading impact

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

What is Driving ERM?

- Huge changes in the operating environment
  - Margins are eroding
  - Delinquencies & charge-offs have increased drastically
  - Fee income is steadily becoming more important
  - Regulations are changing
  - GAAP is inadequate and may very likely change
  - IT Risk management requirements will increase
- Efficiency (output/input) is critical
- Less room for errors and surprises – i.e. risk
- Regulators are extending risk management requirements

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Key Risk Data

NC State University study found:

- 91% of respondents felt at least somewhat strongly that the number and complexity of risks has increased over the last 5 years
- 69% of respondents have experienced a significant operational surprise over the last 5 years

Source: NC State University's ERM Initiative
"Report on the Current State of Enterprise Risk Oversight"

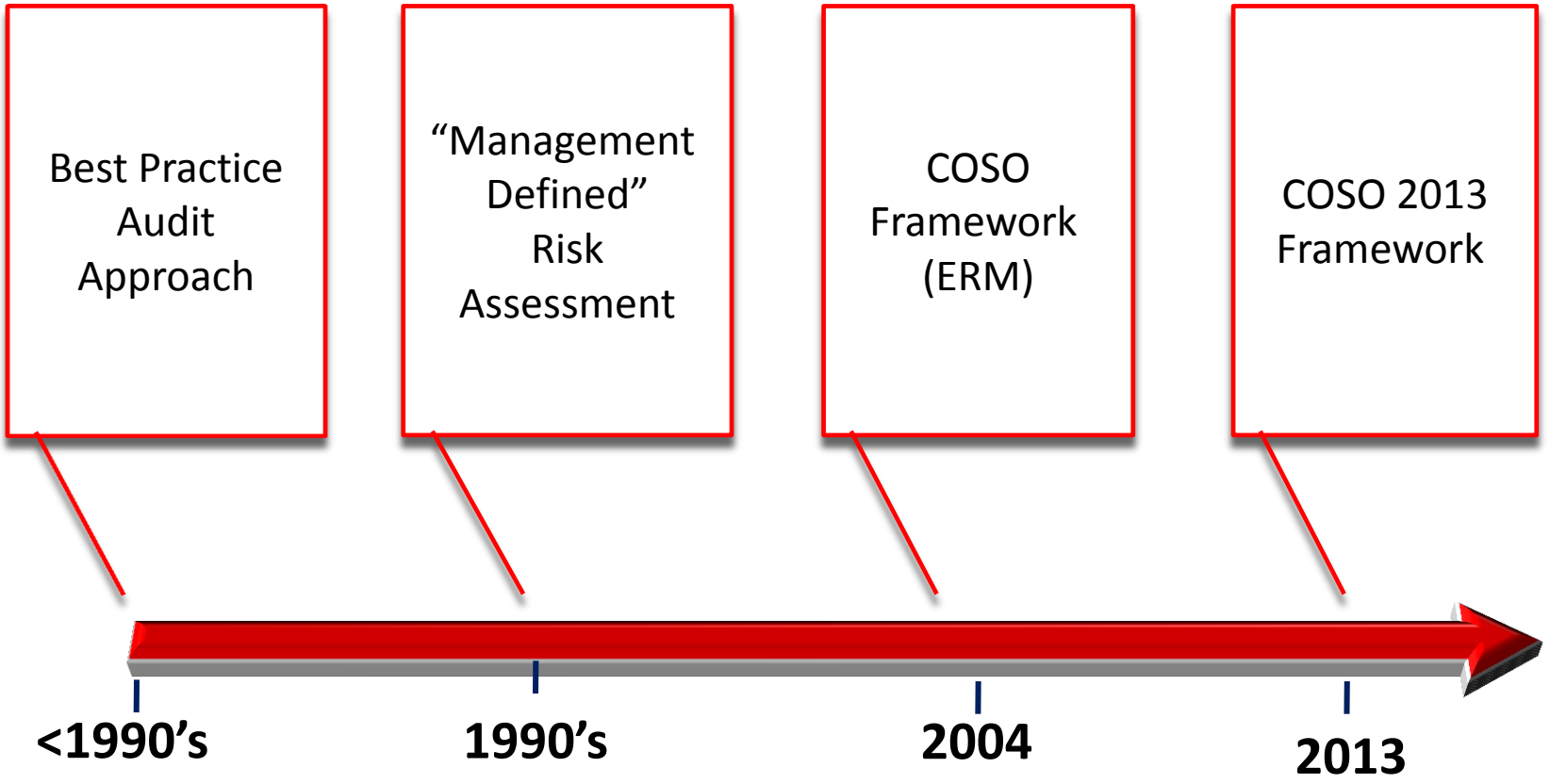
QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

What's Different About ERM?

Criteria	IT Security	Internal Audit	Compliance	ERM
"Customer"	•IT, NCUA	•Supervisory Committee, Board of Directors	•NCUA, Regulatory Agencies, Governments	•Board, executive management, members, employees
Scope	•Information Technology	•Operations, financial reporting, IT	•Various	•Strategy, operations, policy
Goals	•Privacy, Confidentiality Survivability	•Assurance, operational efficiency, deficiency reporting & mitigation	•Avoid fines and legal costs. "Pass the test". Preset standards	•Understand goals, proactively guide actions to achieve them
Standards	•COBIT, NIST, OCTAVE	•IIA, AICPA	•Various	•COSO 2013, ISO 31000
Penalties	•Fines, Legal costs, member costs, NCUA actions, Reputation	•Management reputation, undetected control deficiencies	•Fines, legal costs, corrective action costs	•Poor business decisions. Ineffective business practices
Documents	Automated and Compiled	Manual and Detailed	Mixed and Detailed	"Just Enough"

Evolution of Audit & ERM



QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

What is Risk?

*The **possibility** of an event occurring that will have an impact on the achievement of objectives.*

A Prerequisite to any risk discussion in an organization:

You must know

……the organization's objectives

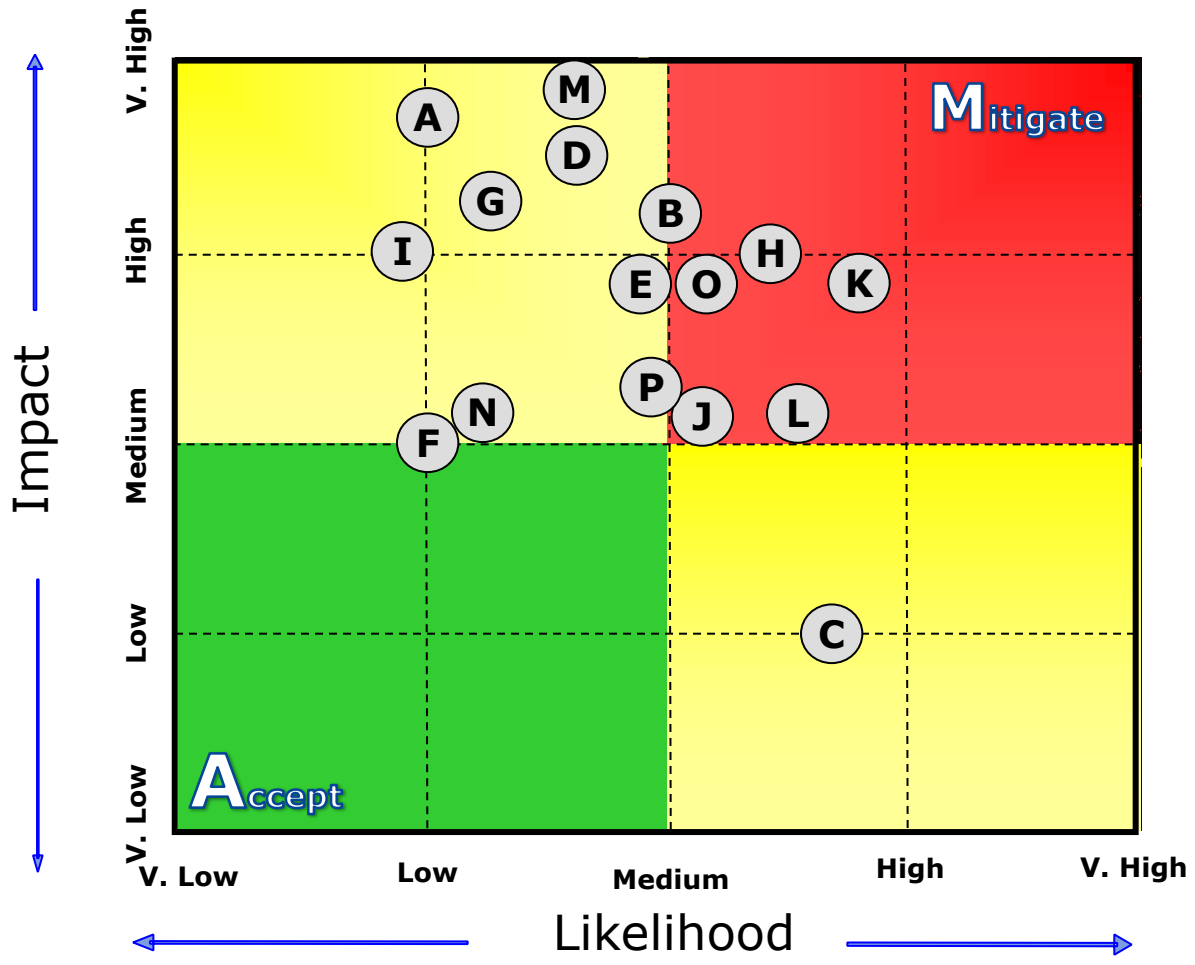
Risk is measured in terms of impact and likelihood.

The Institute of Internal Auditors (IIA)

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Risk Heat Map

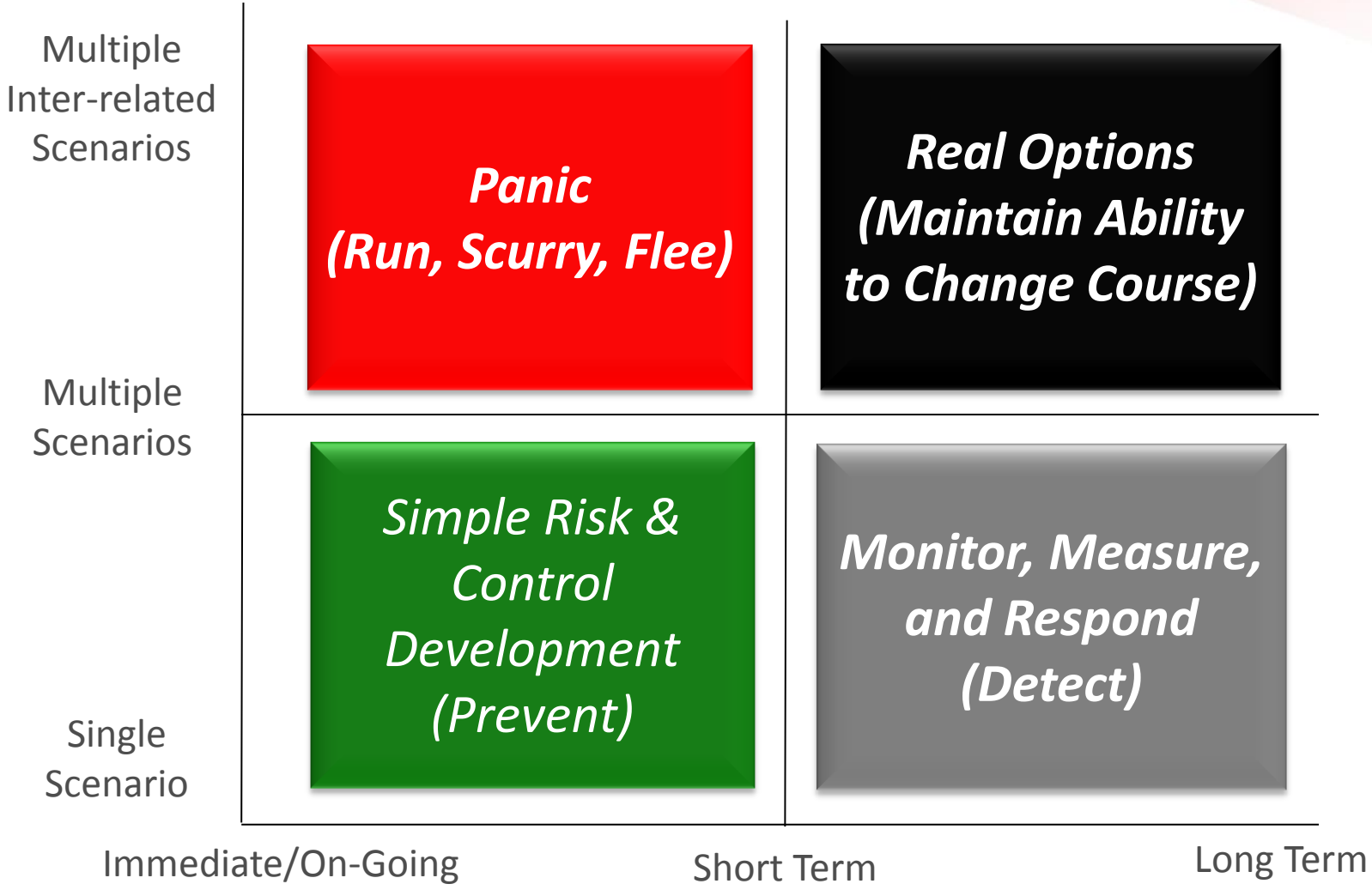


Key Risks	
A	Perception of financial soundness
B	Lack of business continuity plan
C	Attract profitable member relationships
D	Risk of loss of member data
E	Ability to build brand (penetration)
F	Innovate products for customers
G	Systematically meet regulatory requirements
H	Manage instances of internal fraud
I	Manage instances of external fraud
J	Third-party/vendor risk
K	Lack of robust internal control system
L	Ability to meet customer demands for credit
M	Ability to manage market risk
N	Ability to manage credit risk
O	Ability to access capital
P	Ability to grow operations in current environment

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

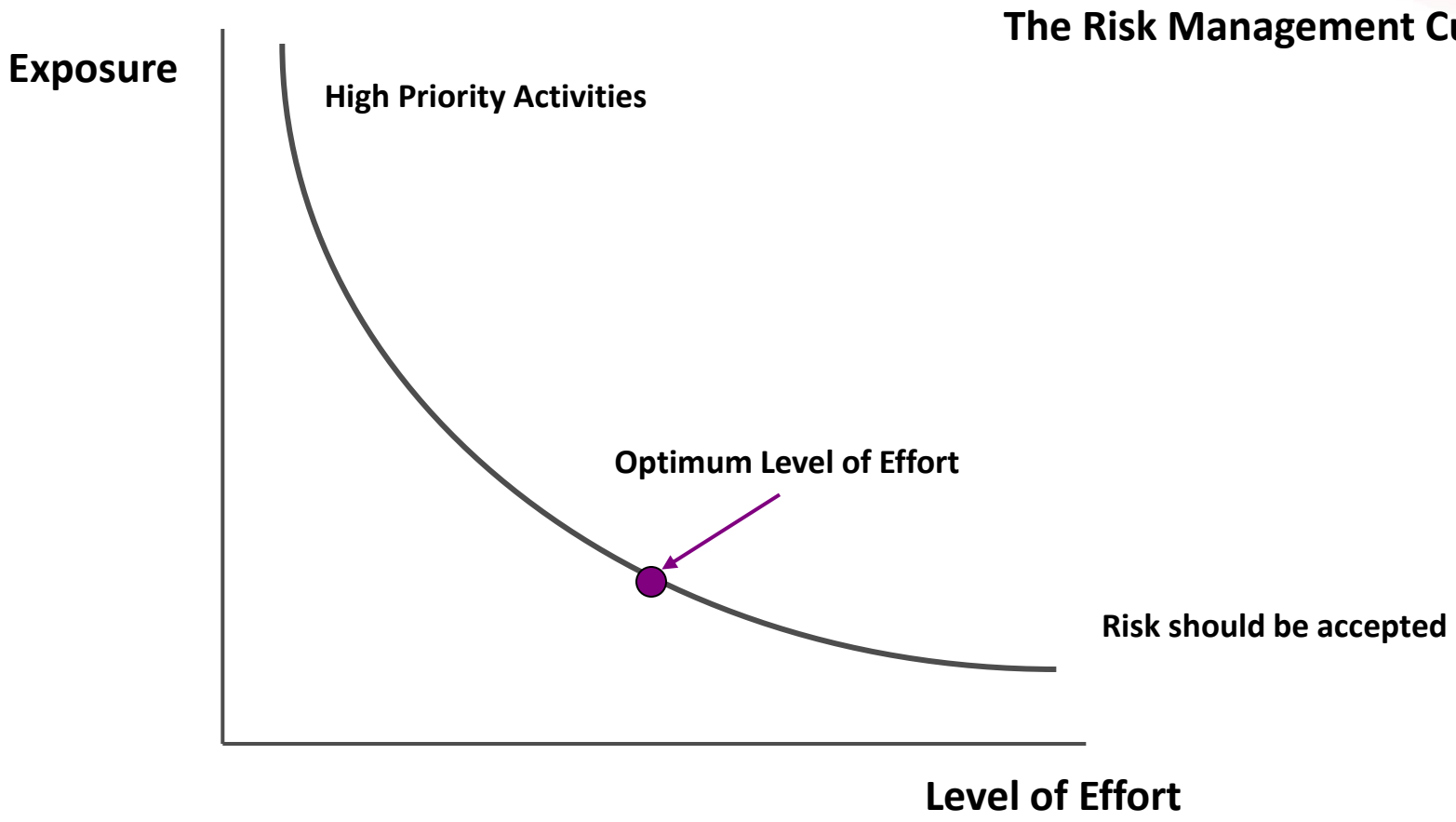
Risk Management Decision Matrix



QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Risk and Cost Relationship



QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

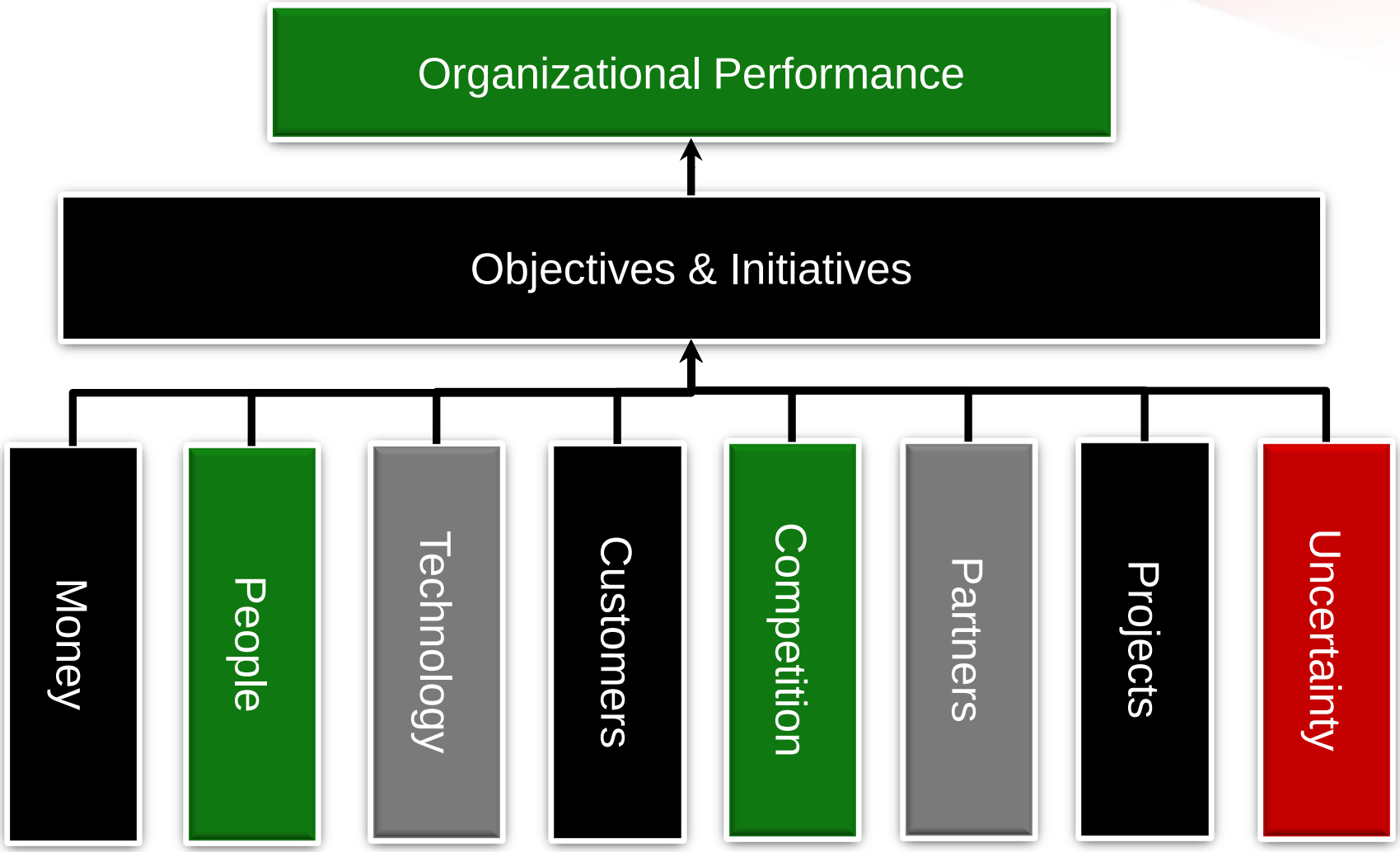
What is Risk Management?

The processes performed and actions taken by management to understand and deal with uncertainties (i.e., risks and opportunities) that could affect the organization's ability to achieve its objectives.

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Managing Performance



QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

COSO Definition of ERM

*ERM is a **process**, effected by an entity's **board** of directors, **management**, and other personnel, applied in **strategy** setting and across the **enterprise**, designed to **identify** potential events that may affect the entity, **manage** risks to be within its **risk appetite**, to provide reasonable assurance regarding the achievement of entity **objectives**.*

Committee of Sponsoring Organizations of the Treadway Commission

(COSO 2004) (see www.coso.org)

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Risk Management Principles

- State your objectives
- Identify most critical areas of risk (risk assessment)
  - Keep in mind that you may not have seen the impact yet!
- Gather and analyze the relevant data
- Exercise sound judgment
- Identify potential root causes (WCGW)
- Determine best response
- Document and train
- Monitor, audit, and assure (and measure)

Assess Risk

Manage Risk

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

What is ERM supposed to do?

- Quickly identify emerging risks and problem areas ***before*** they escalate and cause serious harm
- Reduce the incidence of serious negative surprises that undermine stakeholder confidence
- Enable the organization to more ***effectively take advantage of opportunities***
- Reduce response time for emerging risks
- Demonstrate to stakeholders that reasonable risk management processes are in place
- Provide an efficient way to manage and measure risks consistently across the enterprise

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

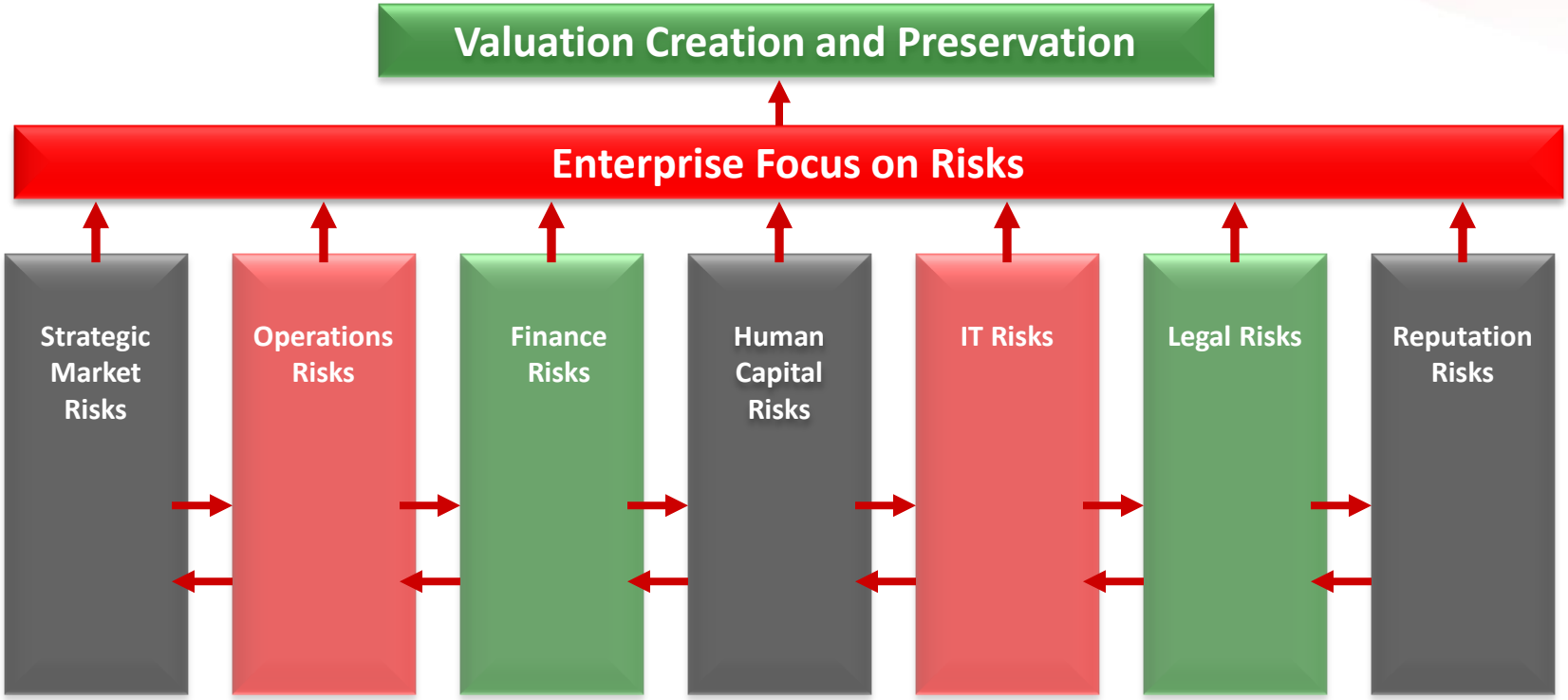
Traditional Risk Management Approach

“Silo” or “Stove-Pipe” Risk Management

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

ERM Brings Risks Together



Key Message:

Senior Management is facilitating the aggregation and interactions of those risk exposures to evolve from Risk Management to Risk Intelligence

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

What is ERM NOT supposed to do?

- Be just one more audit

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Risk Management Compared to Audit

Audit	Risk Management
Independent from Management	Part of Management (like HR, Accounting, IT)
Assurance	Support
Evaluators & Recommenders	Deciders & Implementers
Protects Assets	Seeks Profit
High Likelihood/Low Impact	Low Likelihood/High Impact
Evaluates Controls	Is a Control

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

What is ERM NOT supposed to do?

- Be just one more audit
- Be just one more compliance exercise
- Be done by ONLY audit or risk management
  - Risk management is part of the decision making process
- Prevent healthy risk taking
  - A good risk manager is a good risk taker

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Rewarded Versus Unrewarded Risks

Rewarded Risks (Opportunities to take risk)

- Risks that are expected to bring some benefit if properly managed
- Interest Rate Risk
- Credit Risk
- Liquidity Risk
- Strategic Risks

Unrewarded Risks

- Those for which there is only a downside
- Transaction Risk
- Compliance Risks
- Reputation Risk
- Financial Reporting (Accounting) Risk

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Managing Three Types of Risk

Risks that impact the entire CU Industry

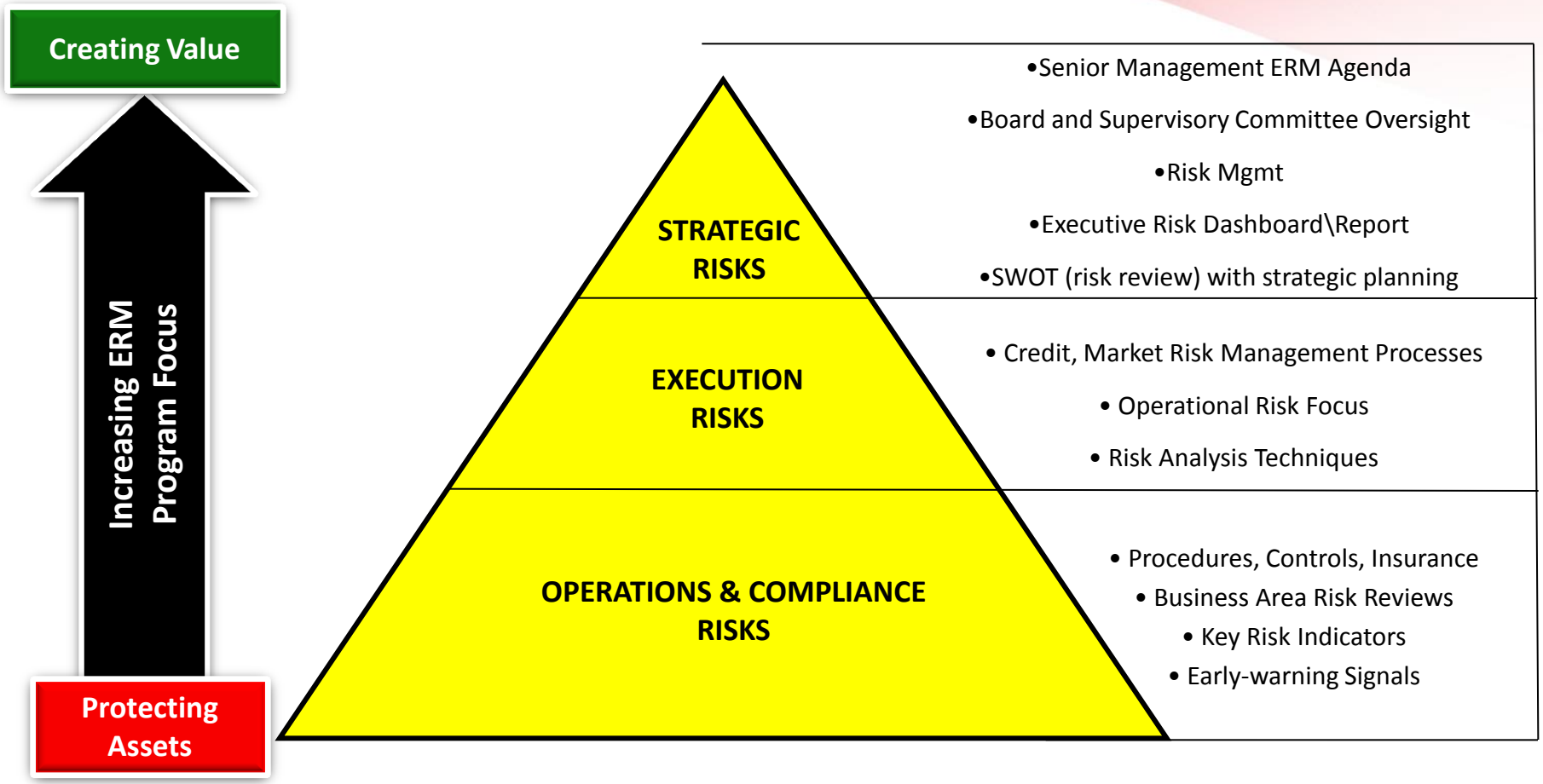
Risks that threaten the entire Credit Union

Risks that threaten a part of the credit uniion

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Maintaining a Balanced Focus on Risk



- The ERM program should help the organization to maintain a balanced focus on value creation (rewarded risk taking) as well as value protection (unrewarded risk mitigation). The program must be periodically assessed for effectiveness and continuously improved

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

NCUA/AICPA to COSO Mapping

NCUA/AICPA Risk Category	COSO Category
Strategy	Strategy
Reputation	Strategy
Interest Rate	Financial
Transaction	Operations
Credit	Strategy
Liquidity	Financial
Compliance	Compliance
Accounting	Reporting
Fraud	Operations
Information Technology	Operations

QUETZAL™ GRC

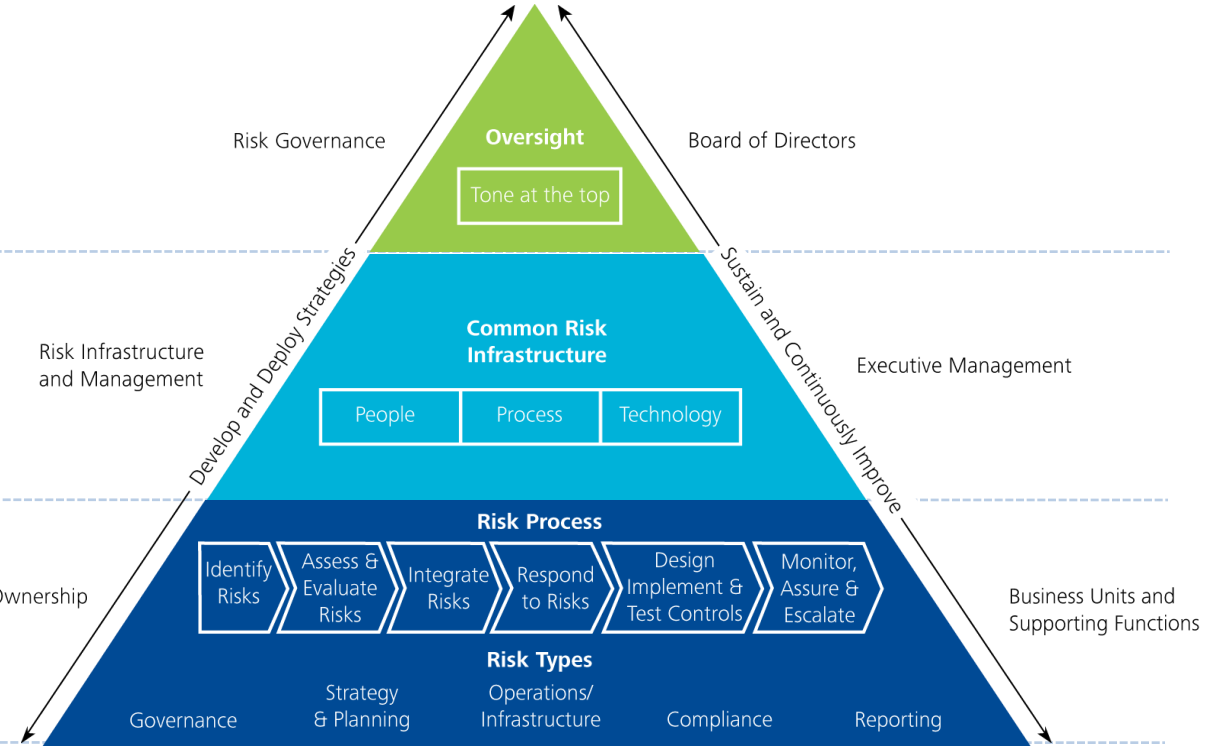
©2013 Quetzal, Inc. All Rights Reserved.

Effective Enterprise Risk Management

Nine Principles for Building a Risk Intelligent Enterprise

- Common Definition of Risk
- Common Risk Framework
- Roles & Responsibilities
- Transparency for Governing Bodies
- Common Risk Infrastructure
- Executive Management Responsibility
- Objective Assurance and Monitoring
- Business Unit Responsibility
- Support of Pervasive Functions

The Risk Intelligent Enterprise



QUETZAL™ GRC

Copyright © 2009 Deloitte Development LLC. All rights reserved.
©2013 Quetzal, Inc. All Rights Reserved.

ERM Organizational Maturity

QUETZAL™ GRC

Copyright © 2009 Deloitte Development LLC. All rights reserved.
©2013 Quetzal Inc. All Rights Reserved.

Internal Audit's Role in ERM

Core internal audit roles in regard to ERM	Legitimate IA roles with safeguard	Roles internal audit should not undertake
Assurance on the risk management processes	Facilitating identification & evaluation of risks	Setting the risk appetite
Assurance that risks are correctly evaluated	Coaching management in responding to risk	Imposing risk management processes
Evaluating risk management processes	Coordinating ERM activities	Management insurance on risks
Evaluating the reporting of key risks	Consolidated reporting on risks	Taking decisions on risk responses
Reviewing management of key risks	Maintaining & Developing ERM framework	Accountability for risk management
	Developing RM strategy for board approval	Implementing risk responses
	Championing establishment of ERM	

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Internal Audit's Role in ERM

Advisor or Evaluator

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.

Questions

Alan N. Siegfried, CPA, CIA, MBA
Managing Director Quetzal GRC
Alan.Siegfried@QuetzalGRC.com
410-570-5400

QUETZAL™ GRC

©2013 Quetzal, Inc. All Rights Reserved.