Tactical Implementation of Enterprise Risk Management

Presented by:
Glen Cooper

Tactical Implementation of ERM

CONGRATULATIONS …

YOU HAVE SUCCESSFULLY MADE YOUR BUSINESS CASE AND ACHIEVED MANAGEMENT'S APPROVAL TO IMPLEMENT ERM

NOW WHAT?

Tactical Implementation of ERM

- **Define Goals and Terms**
- **Develop Roles & Responsibilities**
- **Evaluate Organization Readiness**
- **Remediate Gaps**
- **Implement**

Tactical Implementation of ERM

- **Define Goals and Terms**
- **Develop Roles & Responsibilities**
- **Evaluate Organization Readiness**
- **Remediate Gaps**
- **Implement**

Define Goals and Terms

ERM goals can differ depending upon an entities culture, management, organizational structure, etc.

Potential Goals

- **Effective and efficient risk management**
- **Clear accountability for risks mitigation**
- **Assigned responsibility for risks and control assessment**

Define Goals and Terms

Sample Goal: To provide effective and efficient Risk Management.

Definition of effective and efficient:

1.Knowledgeable Evaluation of Risks – each risk is assigned to a responsible subject matter expert (SME)

2.Knowledgeable Risk Mitigation - Cost effective Control Design strategies

3.Management Knowledge of weaknesses - Certification of Risks & Controls to Management

Define Goals and Terms

Clearly defining terms is critical to tactical implementation of ERM

Sample Terms

- **Objective / goal**
- **Risk**
- **Control**
- **Risk Mitigation**

Define Goals and Terms

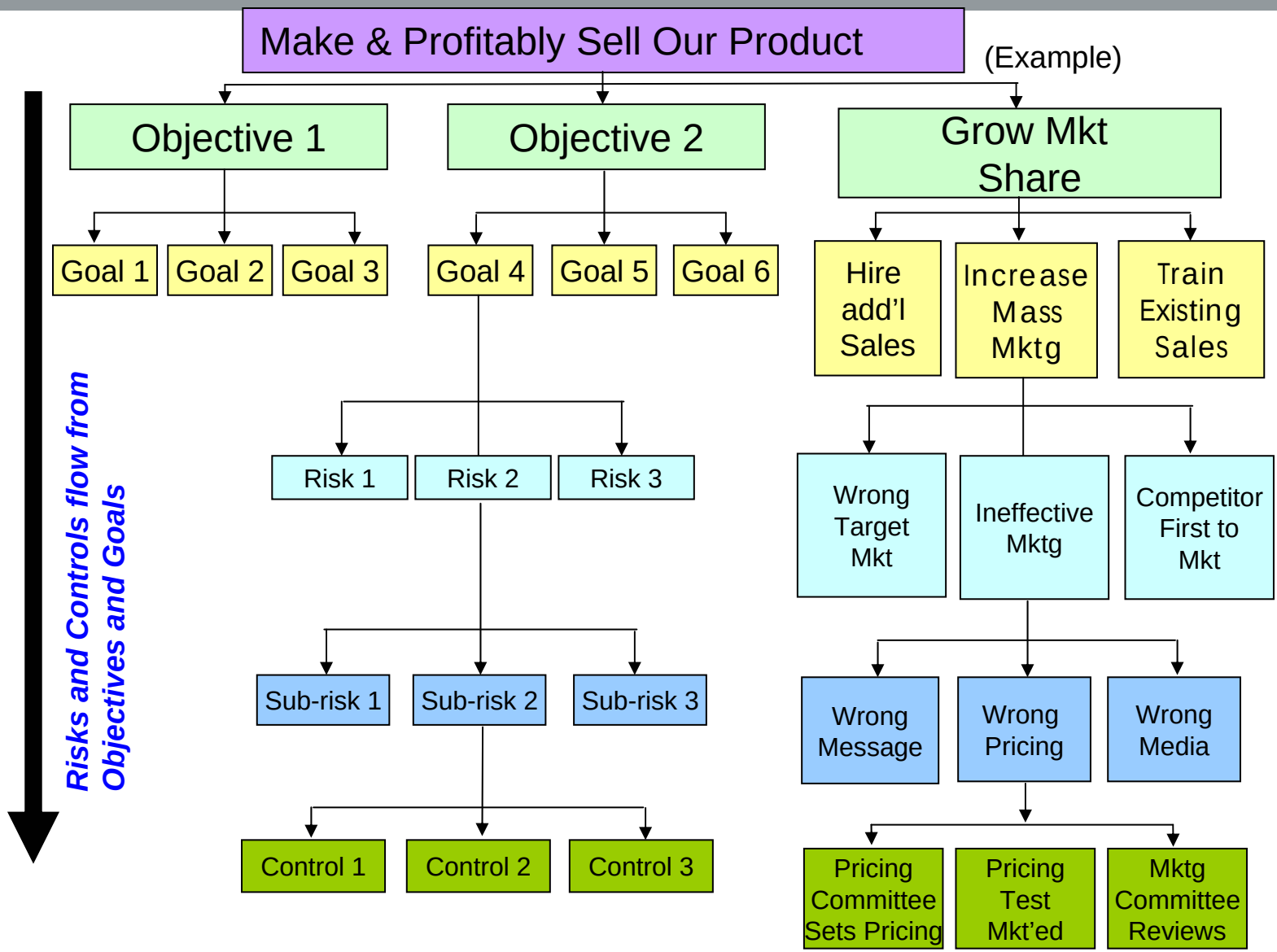
- **Objective / goal - "A business opportunity that an organization sets to achieve or pursue."**

  Every opportunity and goal creates risk

- **Risk - "Anything that can stop business from achieving its stated objectives or goals." Risk flow from objectives and goals and are evaluated pre-control.**

- **Control - "An individual action or series of actions designed to reduce or mitigate risk."**

Define Goals and Terms



Define Goals and Terms

- **Net Risk**

RISK minus CONTROLS
= NET RISK

☺ ☹

Net Risk results from risk mitigation efforts. Net Risk must be evaluated in conjunction with the company's Risk Appetite and consider the cost/benefit of implementing the control to reduce the risk to an acceptable level.

Tactical Implementation of ERM

- Define Goals and Terms
- **Develop Roles & Responsibilities**
- Evaluate Organization Readiness
- Remediate Gaps
- Implement

Develop Roles & Responsibilities

Review organization for best logical fit of ERM roles and responsibilities.

Consider

- **Risk Management Activities**
- **Responsible Parties**
- **Link between Activities and Parties**

Develop Roles & Responsibilities

Sample Risk Management Activities:

Risk Identification

Setting Risk Ratings

Assignment of Risk Responsibility

Risk Documentation

Set Control Quality Targets (Risk Appetite)

Identify & Design Controls

Assign Control Responsibility

Document the Controls

Conduct Control Activity

Evaluate Effectiveness of Controls

Reporting & Analysis

Communication

Develop Roles & Responsibilities

Sample Responsible Parties:

Organizational Unit Functions

- Executive Management
- Governance Structure (committees, groups and meetings)
- Risk Matrix Owners (risk category owner)
- Risk Owners
- Control Owners
- Org Unit Risk Management

Sample Responsible Parties:

Corporate Functions

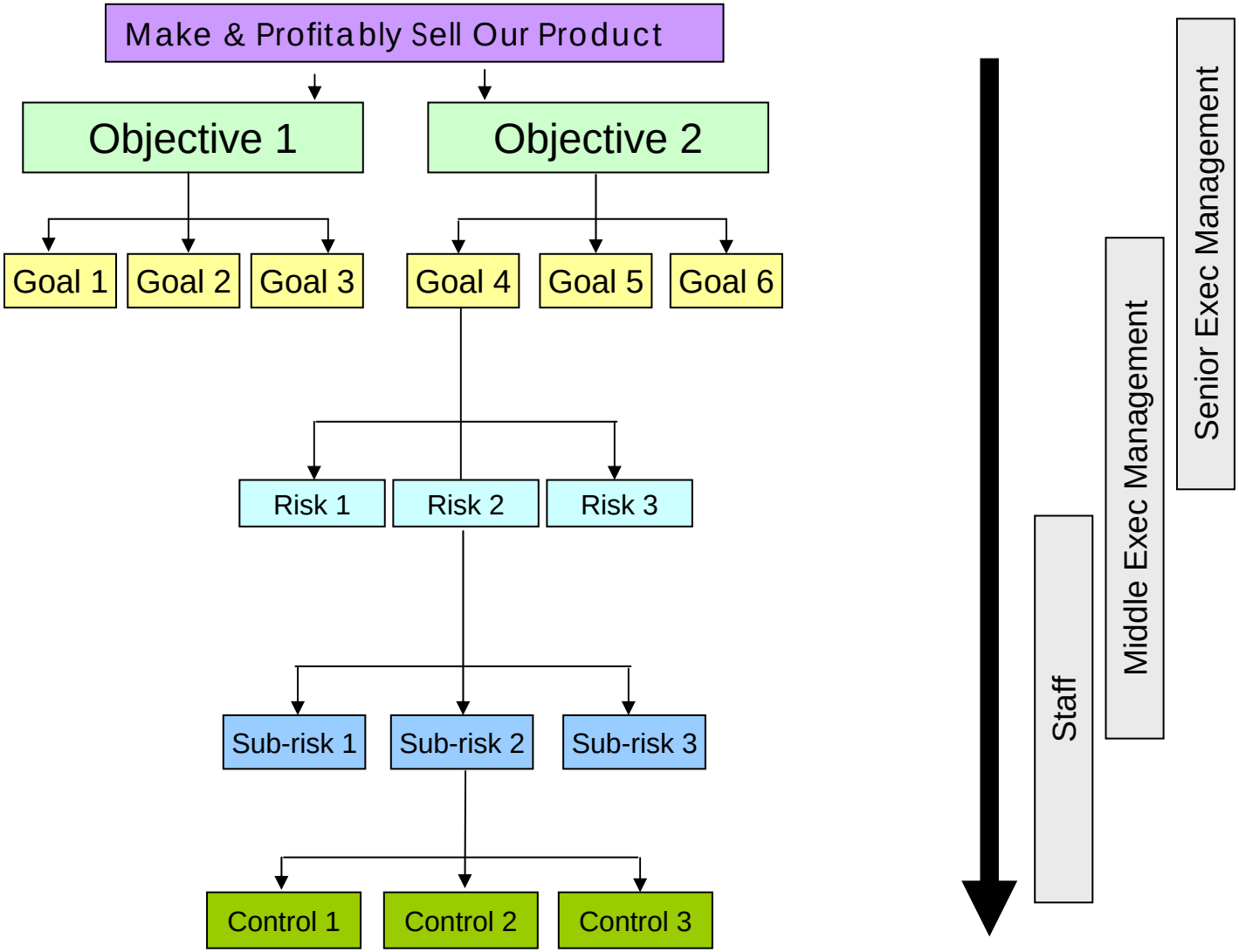
- Internal Audit
- SOX
- Corp ERM

External Entities

- Federal Government
- Regulatory Agencies
- State Governments

Develop Roles & Responsibilities

Sample General Assignments



Develop Roles & Responsibilities

Sample General Assignments

Executive Management responsible for

- **Establishes objectives and goals**
- **Ongoing monitoring of risks and controls (through certification)**
- **Assigns risk and control responsibilities**
- **Supporting risk identification process**

Risk Matrix Owners responsible for

- **Monitoring & mitigating existing risks**
- **Assigning specific risks to owners**
- **Managing controls (supported by Control Owners)**
- **Supporting risk identification process**

Governance responsible for

- **Scanning and identifying new risks and risk changes**
- **Ongoing monitoring of risks and controls**
- **Serving as escalation channel**

Other Governance Functions

- Identified pool of available SMEs by topic
- Mechanism to disseminate info & “tones”
- Documents management decisions

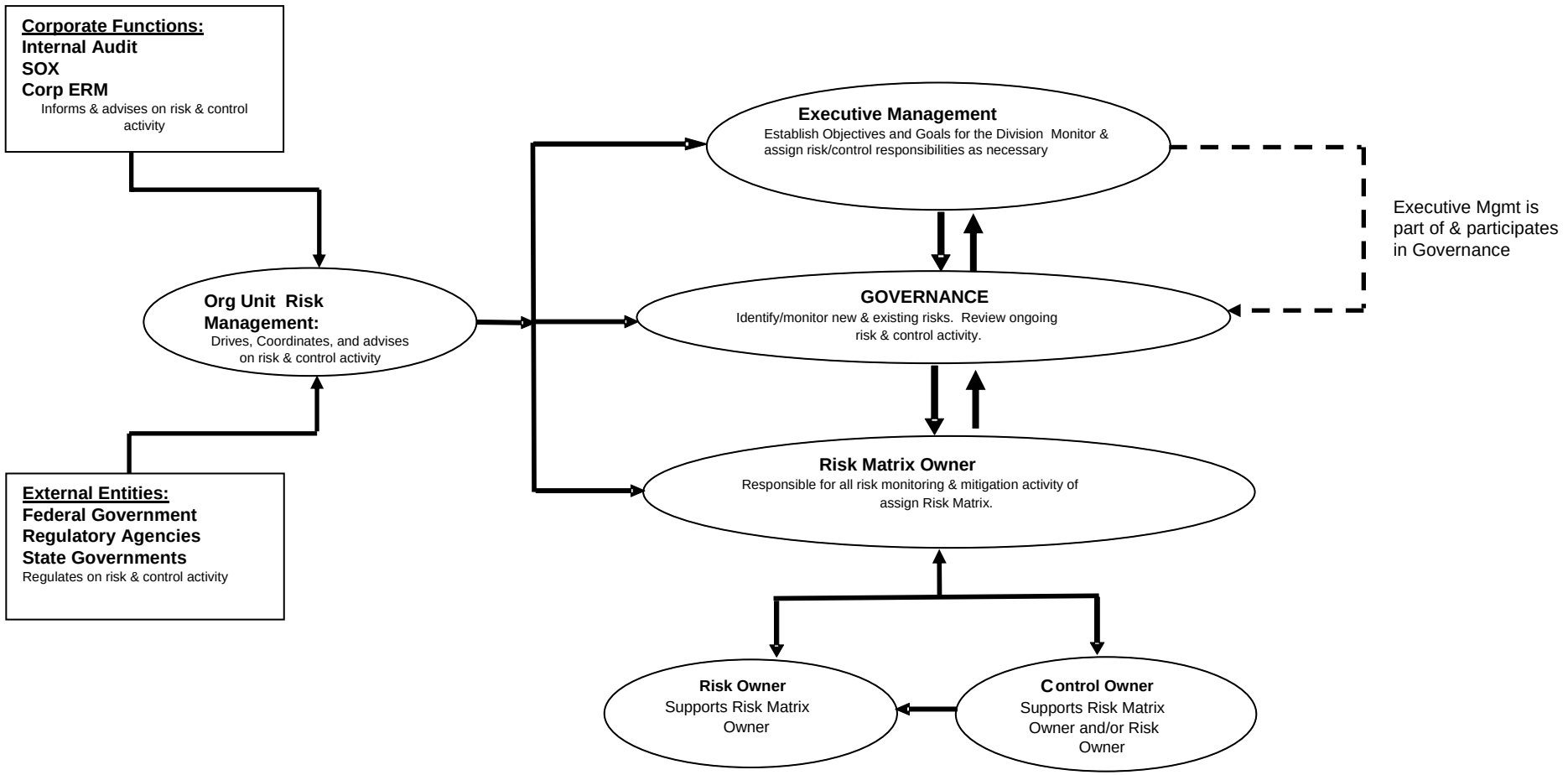
Develop Roles & Responsibilities

Sample linking parties and activities

Role	Executive Mgt	Governance Structure (Committees, Officers, etc.)	Risk Matrix Owner	Risk Owner	Control Owner	Internal Audit	Corp Risk Mgmt	Dept Risk Mgmt
Risk Identification	**Monitor** identification of new material risks. **Monitor** changes in existing material risks. **Communicate** concerns. **Direct** as necessary.	**Identify/Monitor** new material risks as new processes, products, organization, etc are implemented. **Identify/monitor** changes in existing material risks.	**Identify/monitor** changes in existing risks related to assigned risk. **Escalate** any new material risks or changes in existing material risks to governance.	**Assist CORAD Risk Matrix Owner** in the identification/monitoring of changes in existing risks related to assigned risk. **Escalate** any new material risks or changes in existing material risks to the CORAD Risk Matrix Owner or governance.	**Escalate** any new material risks or changes in existing material risks to the CORAD Risk Matrix Owner or governance.	**Escalate** any identified new material risks or identified changes in existing material risks to the Risk Matrix Owner or governance.	**Escalate** any identified new material risks or identified changes in existing material risks to the Risk Matrix Owner or governance.	**Escalate** any identified new material risks or identified changes in existing material risks to the Risk Matrix Owner or governance.
Setting Risk Ratings	**Monitor** assignments of risk ratings. **Communicate** concerns. **Direct** as necessary.	**Review** assignments of risk ratings. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Assign** risk ratings.	**Assist** the CORAD Risk Matrix Owner in assigning risk ratings.	N/A	**Review** the risk ratings through the audit process	**Develop Policies** surrounding risk ratings and confer with CORAD Risk Matrix Owners on setting risk ratings.	**Consult** with the Risk Owner and Risk Matrix Owner in setting proposed Risk Ratings.
Assignment of Risk Responsibility	**Monitor** assignments of risk Matrix Owners. **Assign** Risk Matrix Owners as necessary.	**Review** assignments of material risks. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Assign** risks to Risk Owners.	N/A	N/A	**Review** assignments through the audit process	N/A	**Consult** with the Risk Owner and Risk Matrix Owner in the assignment of Risk Responsibilities.
Risk Documentation	**Monitor** documentation of material risks. **Communicate** concerns. **Direct** as necessary.	**Monitor** documentation of material risks **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Document** risks within assigned risk matrix.	**Assist** in documenting assigned risks in CORAD.	N/A	**Review** risk documentation through the audit process.	**Develop Policies** surrounding the documentation of risks and confer with the CORAD Risk Matrix Owners on documentation.	**Consult and Coordinate** the update of risk documentation with the CORAD Risk Matrix Owner and/or Risk Owner.
Set Control Quality Targets (Risk Appetite)	**Monitor** and **set** overall risk appetite and control quality levels. **Communicate** concerns. **Direct** as necessary.	**Review** risk appetite and control quality levels. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Set** Risk Appetite relative to risks within assigned risk matrix by setting the desired control quality levels.	**Assist** the CORAD Risk Matrix Owner in setting the risk appetite for the risk assigned.	**Support** the development of Control Quality targets.	**Review** the control quality targets through the audit process.	**Develop Policies** surrounding the setting of risk appetites and confer with the CORAD Risk Matrix Owners.	**Consult and Coordinate** the setting of a proposed Risk Appetite with the CORAD Risk Matrix Owner and/or Risk Owner
Identify & Design Controls	**Monitor** control design and adequacy. **Communicate** concerns. **Direct** as necessary.	**Review** control design and adequacy. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Develop, design, and implement sufficient** controls related to risks within assigned risk matrix.	**Support** Control design and **propose** New Controls as necessary.	**Support** the development, design, and implementation of controls assigned.	**Review** the design of internal controls through the audit process.	**Develop Policies** surrounding the identification and design of controls and confer with the CORAD Risk Matrix Owners.	**Consult and Coordinate** on the proper design of new controls with the CORAD Risk Matrix Owner and/or Risk Owner.
Assign Control Responsibility	**Monitor** control design and adequacy. **Communicate** concerns. **Direct** as necessary.	**Review** assignments of control owners. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Assign** control owners within assigned risk matrix.	**Support** the assignment of Control Owners.	N/A	**Review** control assignment through the audit process	N/A	**Consult and Coordinate** on the proper assignment of control responsibility with the CORAD Risk Matrix Owner and/or Risk Owner.
Document the Controls	**Monitor** control documentation. **Communicate** concerns. **Direct** as necessary.	**Monitor** control documentation. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Document** controls within assigned risk matrix.	**Support** CORAD Risk Matrix Owner in the documentation of controls related to assigned risk.	**Support** the documentation of controls related to assigned risk.	**Review** control documentation in CORAD through the audit process.	**Develop Policies** surrounding the documentation of controls and confer with the CORAD Risk Matrix Owners.	**Consult and Coordinate** the update of control documentation with the CORAD Risk Matrix Owner and/or Risk Owner.
Conduct Control Activity	N/A	N/A	**Assure** Control Activity conducted.	**Support** the conducting of the Control Activity	**Conducts** the Control Activity	N/A	N/A	N/A
Evaluate the Effectiveness of Controls	**Monitor** the effectiveness and mitigating effect of controls related to material risks. **Communicate** concerns. **Direct** as necessary.	**Monitor** the effectiveness and mitigating effect of controls related to material risks. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Evaluate the effectiveness of controls** within assigned risk matrix.	**Support** CORAD Risk Matrix Owner in the evaluation of the effectiveness of controls related to assigned risk.	**Support** the evaluation of the effectiveness of control assigned.	**Test** the effectiveness of internal controls through the audit process.	**Develop Policies** surrounding the evaluation of the effectiveness of controls and confer with the CORAD Risk Matrix Owners.	**Consult and Coordinate** the verification of the effectiveness of controls documented in CORAD with the CORAD Risk Matrix Owner and/or Risk Owner.
				.				
Reporting & analysis	**Review** reports relative to material risks. **Communicate** concerns. **Direct** as necessary.	**Review** reports relative to material risks and document results of those reviews. **Confer** with Risk Matrix Owners. Escalate issues as considered necessary.	**Develop and review** reports and analysis for risks and controls within the risk matrix. **Support** Governance committees with appropriate reports and analyses.	Report to the Risk Matrix Owners and Governance Committees (as appropriate) on the **effective mitigation** of the assigned risk. Report to CMD Risk Mgmt on any **changes** to the Risk/Control documentation.	Report all significant **control failures** to the appropriate Risk Owners. Report the results of **testwork** performed. Report any **changes/deletions** of assigned controls to the appropriate Risk Owner(s) and ensure that these changes/deletions are properly reflected in CORAD.	Report the results of **internal audits** to management and the BOD (Governance).	**Develop and review** reports and analysis for risks and controls.	Report results of overall **risk management activities** for the division.
Communication	**Set the Tone at the Top** for the identification and assessment of risks and controls	**Communicate** risks/controls issues to all appropriate parties. **Escalate** (report) risks as appropriate to Corporate level governance committees.	**Communicate** risks/controls issues to all appropriate parties. **Escalate** (report) risks as appropriate to Governance committees.	**Support** the Risk Matrix Owner by providing information regarding the mitigation of their assigned risk. **Facilitate** and coordinate communication between all parties significantly affected by their assigned risk.	**Support** the Risk Matrix Owner by providing information regarding the effectiveness of their assigned control. Communicate and coordinate all **proposed changes/deletions** of assigned controls with the appropriate Risk Owners and/or Risk Matrix Owners. Communicate any **changes/deletions** to assigned controls to CMD Risk Mgmt and ensure proper documentation in CORAD.	Communicate the results of **audits** to the appropriate management.	Communicate **standards policies and procedures** related to CORAD Communicate any **regulatory** concerns or trends to the divisions. **Coordinate** communication between the divisions. **Communicate** risks/controls issues to all appropriate parties **Escalate** (report) risks as appropriate to Governance committees.	Communicate the various **roles, responsibilities, and processes** to the appropriate parties and provide training as appropriate. **Facilitate** communications between all defined roles.

Develop Roles & Responsibilities

Sample Coordination between Parties



Tactical Implementation of ERM

- Define Goals and Terms
- Develop Roles & Responsibilities
- **Evaluate Organization Readiness**
- Remediate Gaps
- Implement

Evaluate Organization Readiness

Evaluation of organizational readiness should flow from the development of the ERM goals and the development of the roles and responsibilities.

Sample Considerations

- **Support Resources**
- **Culture**
- **Management & staff knowledge**
- **Organizational structure**
- **Governance maturity**
- **Systems and processes infrastructure**

Evaluate Organization Readiness

Are the necessary support resources available to implement ERM?

Sample Questions

- **Are the Corp and Org Unit level resources available to fill responsibilities?**
- **Do they have the right skill sets?**
- **Is there a champion?**

Evaluate Organization Readiness

Sample Org Unit Risk Management Dept Mission Statement

- Act as a value added service department responsible for the continual development of a world class risk management control environment through the application of an organization-wide strategy to **assist** the Org Unit and its departments in 1) successful compliance with applicable laws and regulations, 2) reliable financial reporting, and 3) effective and efficient operational control systems.

Sample Org Unit Risk Management Dept General Responsibilities

- Collaborately analyze and respond to key risk areas
- Liaison with and coordinate the activities of
  - Internal Audit
  - Corp ERM
  - External Auditors
  - Regulatory agencies
  - Accounting/SOX
- Promote effective and efficient operational, compliance and financial controls
- Act as Risk Management Champion
  - Train department mgrs on risk identification & control development
  - Creatively incorporate risk management themes into business unit culture

Evaluate Organization Readiness

What is the current culture and how will it need to be modified to implement ERM

Sample Questions

- **Is the culture entrepreneurial and unfamiliar with controls?**
- **Is culture very bureaucratic?**

Evaluate Organization Readiness

How familiar is management and staff with ERM concepts?

Sample Actions

- **Conduct survey to assess management and staff knowledge**
- **Interview management**

Evaluate Organization Readiness

Sample Survey

	Very Familiar	Somewhat Familiar	Not Very Familiar	Not at all Familiar
Please rate your familiarity with risk management software	25%	25%	25%	25%
Please rate your familiarity with COSO.	25%	25%	25%	25%
Please rate your familiarity with SOX.	25%	25%	25%	25%
Please rate your familiarity with the internal audit process.	25%	25%	25%	25%
Please rate your familiarity with privacy regulations.	25%	25%	25%	25%
Please rate your familiarity with fraud prevention and detection processes.	25%	25%	25%	25%
Please rate your familiarity with risk management methodologies.	25%	25%	25%	25%
How familiar are you with the risks that face your area of responsibility.	25%	25%	25%	25%
How familiar are you with risk assesstment.	25%	25%	25%	25%

Evaluate Organization Readiness

What is the current organizational structure?

Sample Questions

- **Is organization matrixed?**
- **Is the matrix structure strong, weak, or in between**
- **Is organization strictly functional?**

Evaluate Organization Readiness

How mature is the governance (committee, meetings, etc) structure?

Sample Questions

- **Is management aware of what meetings are being held?**
- **Does every meeting have a charter?**
- **Are minutes maintained?**

Evaluate Organization Readiness

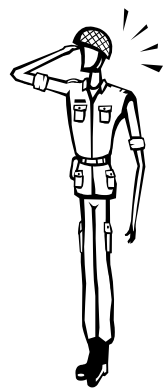
Are there existing systems and processes for risk management?

Sample Questions

- **Any risk management software in use?**
- **Any sign-off or certification processes in place?**

Tactical Implementation of ERM

- Define Goals and Terms
- Develop Roles & Responsibilities
- Evaluate Organization Readiness
- **Remediate Gaps**
- Implement



Remediate Gaps

Once the evaluation of organizational readiness is complete it can be compared to the ERM goal and developed roles and responsibilities, any gaps should then be remediated.

Consider

- **Gap analysis**
- **Communication plan**
- **Training plan**

Remediate Gaps

Sample Gap Analysis

Color Key	Value Scale
Know the message	5-6
Be familiar with the message	3-4
General awareness of the message	1-2
No messaging needed	0

		DESIRED STATE										CURRENT STATE									
		Role					Risk Mgt Methods			Systems			Role					Risk Mgt Methods			Systems	
Audiences	Topic	Role of Org Unit RM	Role of Internal Audit	Role of Corp ERM	Governance Strategy	Individuals Role covering areas of RM	Risk/Control Assessment Methodology	Internal Control Design	Risk & Control Monitoring Methods	Risk Mgt Sys	SOX System	Compliance System	Role of Org Unit RM	Role of Internal Audit	Role of Corp ERM	Governance Strategy	Individuals Role covering areas of RM	Risk/Control Assessment Methodology	Internal Control Design	Risk & Control Monitoring Methods	Risk Mgt Sys	SOX System	Compliance System
Executive Mgt	General risk management vocabulary, topic areas, and control solution approaches.	5.5	3.5	3.5	5.5	5.5	3.5	3.5	3.5	1.5	1.5	1.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5
Middle Mgt	Detail risk management vocabulary, topic areas, and control solutions approaches.	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5
Lower Middle Mgt	Detail risk management vocabulary, topic areas, and solutions approaches. Practical position specific strategies to risk management and controls.	3.5	3.5	3.5	3.5	5.5	5.5	5.5	5.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5
Risk Matrix Owners	Detail risk management vocabulary, topic areas, and solutions approaches. Practical position specific strategies to risk management and controls.	5.5	3.5	5.5		5.5	5.5	5.5	5.5	5.5	1.5	1.5	3.5	3.5	3.5		3.5	3.5	3.5	3.5	3.5	3.5	3.5
Control Owners	Detail risk management vocabulary, topic areas, and solutions approaches. Practical position specific strategies to risk management and controls.	5.5	1.5	3.5		5.5	1.5	5.5	5.5	5.5	1.5	1.5	3.5	3.5	3.5		3.5	3.5	3.5	3.5	3.5	3.5	3.5
Operations Senior Mgt	Detail risk management vocabulary, topic areas, and control solutions approaches.	3.5	3.5	3.5	3.5	5.5	5.5	5.5	5.5	1.5			3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5		
Other Admin & Production Mgt	General awareness of risk management vocabulary, topic areas, and control solution approaches.					5.5	1.5	3.5									3.5	3.5	3.5				
Corp Governance	Existence of Risk Mgt Dept and its role in managing Division risk.	5.5											3.5										

Remediate Gaps

Sample Communication Plan

Audiences
Executive Mgt
Middle Mgt
Lower Middle Mgt
Risk Matrix Owners
Control Owners
Operations Senior Mgt
Other Admin & Production Mgt
Corp Governance

Messages
ROLE
Individuals Role covering areas of RM
Role of Internal Audit
Role of Corp ERM
Governance Strategy
RISK MANAGEMENT METHODS
Risk/Control Assessment Methodology
Internal Control Design
Risk & Control Monitoring Methods
STATUSING & REPORTING
SYSTEMS
Risk Mgt System
SOX System
Compliance System

Best Communication Channel

Individualized → Generalized

Audiences	Enforced Procedures	Mandatory Training	Employee On Boarding	Flyers - Informational	Gift/Desktop Messaging	Optional Training	Survey	Email Messaging	Ad Hoc Communications	Posters	Stickers	Internet messaging
Executive Mgt					X	X			X			
Middle Mgt	X	X			X	X			X			
Lower Middle Mgt	X	X	X	X	X		X	X	X	X	X	
Risk Matrix Owners	X	X	X	X	X	X	X		X	X	X	X
Control Owners	X	X						X				
Operations Senior Mgt	X	X						X				
Other Admin & Production Mgt	X	X						X				
Corp Governance	X	X						X				

Remediate Gaps

Sample Training Curriculum

TRAINING CURRICULUM SUMMARY

TYPE	COURSES	HRS	PURPOSE	TOPICS ADDRESSED	TARGET AUDIENCE
OVERVIEW	RM 101 - Risk Management Overview	1	Introduce key Risk Management concepts and set the tone for future training sessions.	Terminology; Roles/Responsibilities; Methodology; Risk and Control Statements; and Systems	Senior and middle management
	RM 201 - Corporate Governance	1	Introduce the roles and responsibilities that Corporate Governance plays to effectively manage risk.	Risk identification and evaluation; internal controls, monitor on-going control effectiveness; remediation; Discuss roles and responsibilities of various committees, management, process owners, control owners, and use of risk system as an administrative tool.	Senior and middle management
	RM 301 - Risk Management Culture	1	Increase awareness of bus unit's own risk management culture by assessing the current environment and identifying opportunities for improvement	Why is having a strong risk management culture important and what are some common characteristics; methods to establish a risk management culture; and an exercise to assess the current culture and identify improvements.	Senior and middle management
RISK	Risk 101 - Risk Overview	1	To provide the audience with a basic understanding of risk related topics which will be discussed in greater detail in subsequent training courses.	Definition; Speed & Vulnerabilities, Categories; Examples; Identification Techniques; Risk Owner Definition, Roles and Responsibilities; key Risk Sys Screens; Risk Statements; Concept of Gross Risk vs. Net Risk, Risk Assessment and Risk Significance; and a Group Exercise	Middle management
	Risk 102 - Risk Identification	1	To provide the audience with specific tools to be utilized in the identification of risks related to their areas of responsibilities.	Process to be used to identify risk; Methods to be used in risk identification; List of reference materials and websites that can be referred to when brainstorming about potential risk; and an exercise to identify risks contained in a certain process and draft a risk statement. Risk Layers/Sub-Risks	Middle management
	Risk 201 - Risk Evaluation	1	To provide the audience with an understanding of how once the risks have been identified to determine the significance of each risk by assessing its likelihood and impact as well as the assessment methodology and available tools.	Define risk assessment and discuss benefits; Present the Bus Unit process including the supporting tools to be utilized when performing a risk assessment; Determine the risk rating/significance and decide action (accept, reject, share, reduce) based upon the risk rating; and introduce key Risk Sys risk assessment related screens.	Middle management
	Risk 202 - Financial Exposure & Impact Analysis	1	To provide the audience with a detailed understanding of how financial risk exposure and impact plays an important part in determining the risk significance and ultimately management's decision as to the best course of action to take to mitigate the risk.	Exposure and Impact Analysis benefits; How to describe the exposure and impact; Financial, Operational, and Compliance exposures; and introduce Risk Sys specific risk exposure and impact related screens.	Middle management
CONTROL	Control 101 - Control Overview	1	To provide the audience with a basic understanding of control related topics which will be discussed in greater detail in subsequent training courses.	Define internal control and types of controls; Examples of common controls; overlapping controls (Financial, Operational, Compliance, and SOX); control identification techniques; control statement elements; control owner roles and responsibilities; CORAD related control screens; control cost vs. benefit; Group exercise; need to assess the control design adequacy and operational effectiveness; and control failure (design, operational, significance, documentation).	Middle and lower middle management
	Control 201 - Control Design	1	To provide the audience with the basic knowledge and tools required to design and evaluate the control environment and provide guidance when a design deficiency has been identified. John Calhoun to Develop and Deliver in Q2 2007	Define what is and why we need to evaluate the internal control design; Science vs. Art; Define net risk; 4 key questions to ask; process to evaluate internal control design and assess the net risk; Risk Control Matrix tool; what to do if a design gap is identified, CORAD specific design evaluation screens; and an exercise to evaluate the controls to ensure the risks are mitigated and objectives achieved.	Middle and lower middle management
	Control 301 - Operational Effectiveness Evaluation	1	To provide the audience with the basic knowledge and tools needed to test the operational effectiveness of critical controls and provide guidance when an operational deficiency has been identified.	Determine what controls to test; define 3 types of testing strategies; how to test controls that don't leave an audit trail; discuss inquiry, observation, reperformance and optimal timing to perform the testing; define test scripts; sampling methodologies; testing documentation; how do you know if a control is operating effectively and what to do if it is not; CORAD specific operational effectiveness screens; and a group exercise to develop test scripts and determine if the control is operating effectively or not.	Middle management

Tactical Implementation of ERM

- Define Goals and Terms
- Develop Roles & Responsibilities
- Evaluate Organization Readiness
- Remediate Gaps
- **Implement**

Implement

When the organization is ready:

IMPLEMENT

Consider

- **Establishing governance**
- **Defining major risk categories and assigning responsibility**
- **Evaluating which risk and controls to manage**
- **Certification process**

Implement

Considerations in establishing governance

- **Identifying governance meetings**
- **Creating charters**
- **Training chairs and members**
- **Establishing governance document repository**
- **Developing reports**

Sample major risks and scope statements

#	Risk Matrix	Proposed Risk Matrix Scope/Responsibility	Proposed Risk Matrix Owner
1	Sales Mgmt	Responsible for all risks and controls surrounding the sales management process: sales personnel qualifications, performance, current and future staffing levels, leadership development, and organization.	Risk Mgr 1
2	Pricing & Product Development	Responsible for all risks and controls associated with ensuring that the business unit has competitive products and pricing that provide sufficient margins to meet revenue related strategic goals.	Risk Mgr 2
3	Credit Risk	Responsible for all risks and controls associated with credit risk for the business unit. Includes exposure to monetary losses associated with inadequate collateral and inadequate financial stability.	Risk Mgr 3
4	Vendor Mgmt	Responsible for all of the risks and controls associated with the business unit's vendor relationships, including the timely and accurate delivery of products, payments, reporting, etc.	Risk Mgr 4
5	Business Continuity	Responsible for all of the risks and controls associated with the inability of the business unit to recover from a natural disaster or other uncontrollable event in a timely manner, in order to prevent loss of business, loss of life, loss of assets, loss of data, and/or loss of confidence by the market/customers.	Risk Mgr 5

Implement

Sample factors and requirements used in identifying which risks to manage

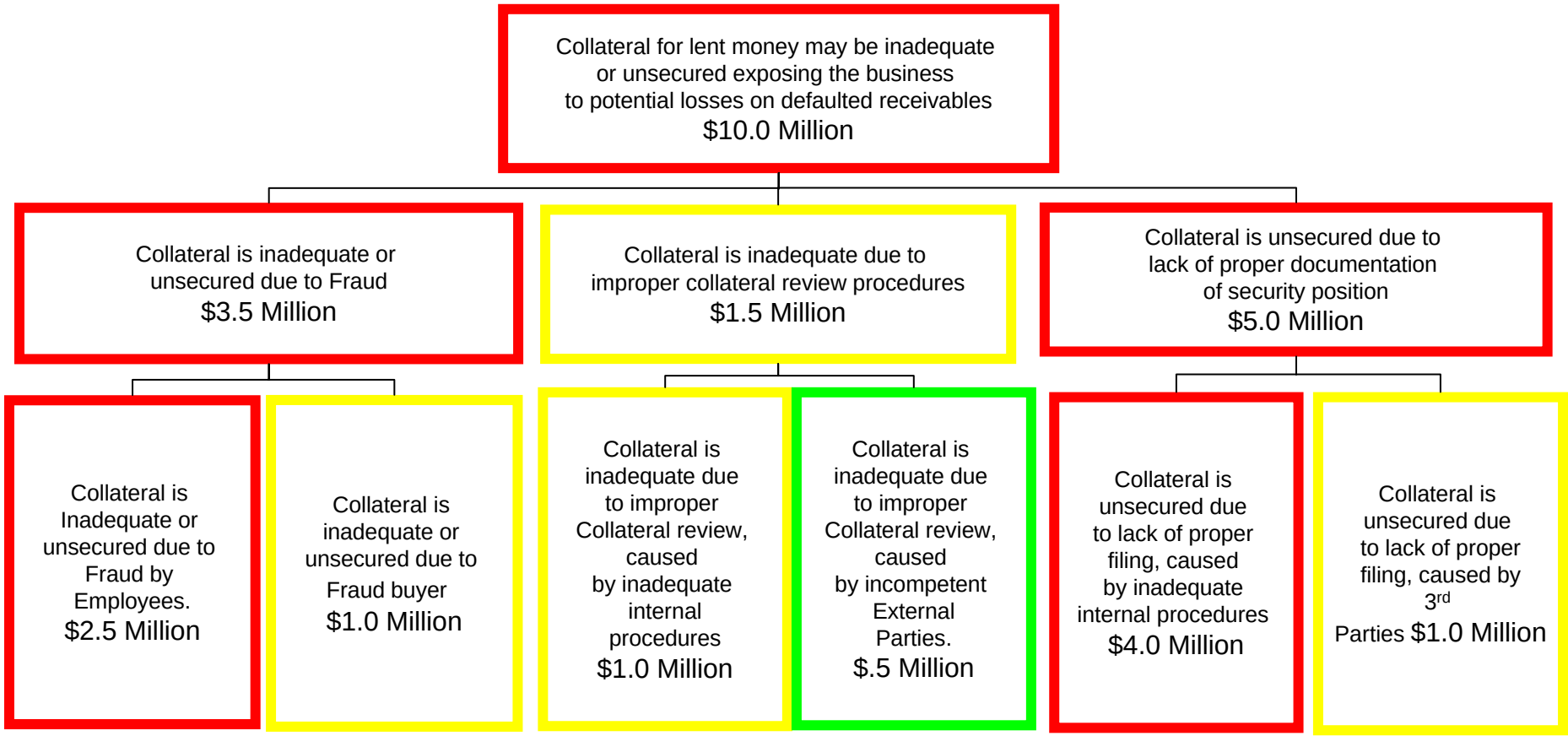
- Risks
  - Financial exposure / opportunity loss
  - Qualitative Factors
  - Definitional requirements
- Controls
  - Mitigation requirement
  - Manageability requirement
  - Definitional requirements

Example of Quantitative Risk Documentation Thresholds

- Risks >$2 Mil MUST be documented
  - Sub-risks should be documented
- Risks >$750,000 SHOULD be documented
  - Sub-risk may be documented
- Risks >$0* MAY be documented

Implement

Sub-risks Quantitative Review



Sample Qualitative Risk Documentation Factors:

- Regulatory Impact – even if financial exposure is low, a regulatory impact may suggest risk should be documented.
- Emerging growth area –anticipated risk expansion may suggest monitoring and documenting.
- Liquid assets – Risk involves access to cash or other liquid assets may suggest documenting.
- Links to other risks – Some risks are linked to other risks that may impact decision to document.
- Strategic Alignment – If a risk is tied to the achievement of a strategic objective then documenting may be warranted.
- Management Prerogative –If management wants to monitor a risk for any business reason the risk system is a tool for that purpose.

Implement

Sample Risk definitional requirement:

Risks should be defined in a way that allows the risks and associated controls to be understood in relationship to each other.

- If a risk is defined at too high a level then there will be many controls applied against it and the meaning of an individual control may be lost.
- If a risk is defined at too low a level then there may be only one associated control applied against it, creating clutter.

Risk Level Guidelines:

1. If a risk has over 10 controls, it is likely that it can be split into sub-risks.
2. If a risk has less than 3 controls, it is likely that it can be combined with other risks.
3. If a risk has sub-risks that require different types of controls, then it should generally be split into sub-risks.
4. If it is unclear as to how a control addresses a risk, due to the fact that the control addresses only one aspect of the risk, then consideration should be given to splitting the risk into sub-risks.
5. If there are multiple risks which are essentially only different due to a single factor (e.g. location, time, nature of peril, etc) they should be combined.

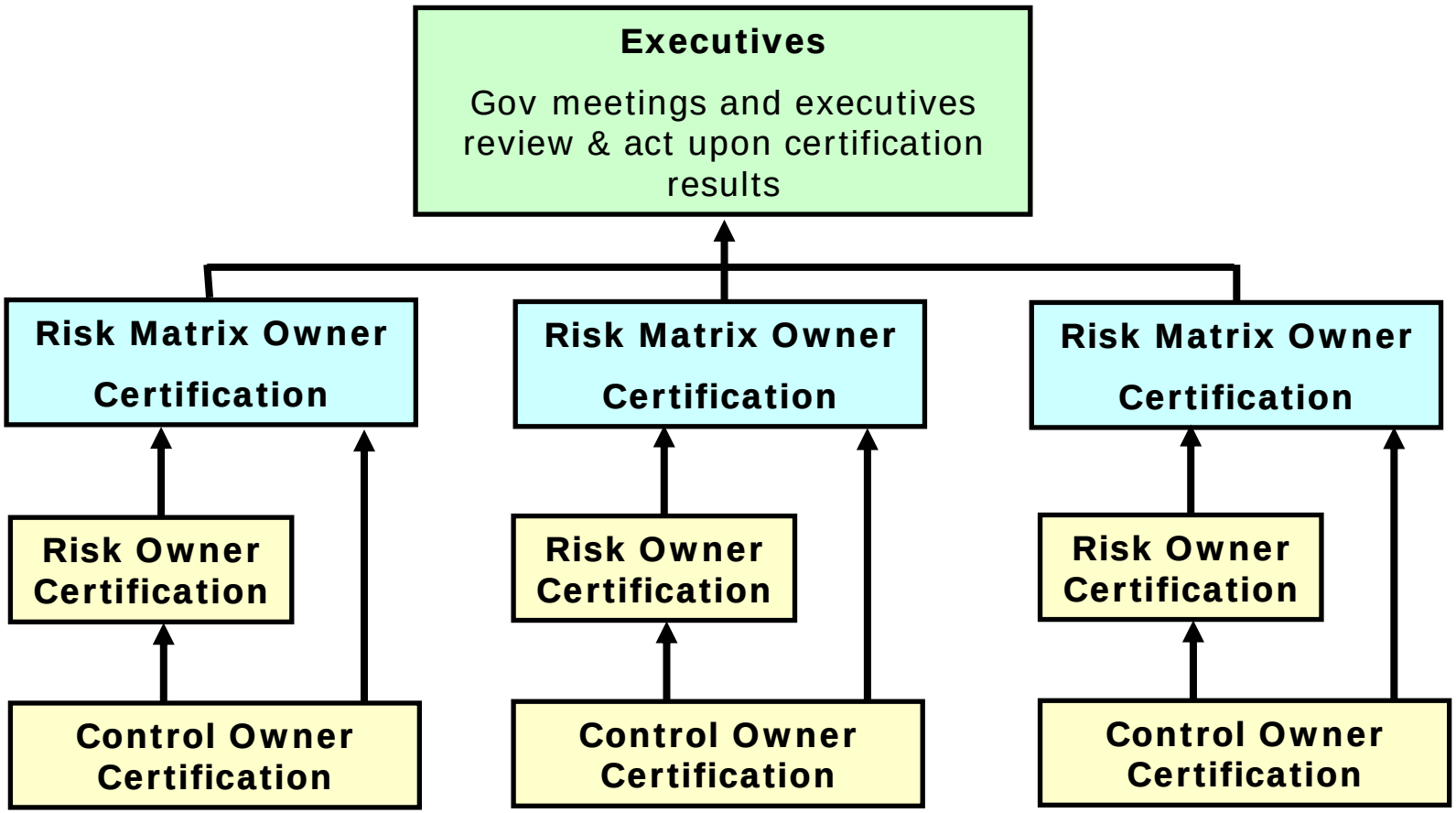
Implement

Sample Control Documentation Issues:

- **Mitigation – Enough controls should be documented to adequately mitigate the associated risk.**
- **Control Management - In documenting controls consideration should be given to the desire to assure that control is properly functioning over time through a testing and certification process.**
- **Definitional Requirement - Controls should be documented in such a way as they can be understood in relationship to the risk which they mitigate.**

Implement

Sample Certification Process



Questions

?