Tactical Implementation of Enterprise Risk Management

Presented by: Glen Cooper
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
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

Make & Profitably Sell Our Product

Objective 1

Goal 1
Risk 1
Sub-risk 1
Control 1
Risk 2
Sub-risk 2
Control 2
Risk 3
Sub-risk 3
Control 3

Objective 2

Goal 2
Goal 4
Risk 2
Sub-risk 2

Goal 3
Goal 5
Risk 3
Sub-risk 3

Goal 4
Goal 6

Grow Mkt Share

Hire add'l Sales
Wrong Target Mkt
Wrong Message
Wrong Pricing
Wrong Media

Increase Mass Mktg
Ineffective Mktg

Train Existing Sales
Competitor First to Mkt

Pricing Committee Sets Pricing
Pricing Test Mkt'ed
Mktg Committee Reviews

Risks and Controls flow from Objectives and Goals
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
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

Make & Profitably Sell Our Product

Objective 1
- Goal 1
- Goal 2
- Goal 3

Objective 2
- Goal 4
- Goal 5
- Goal 6

Risk 1
- Risk 2
- Risk 3

Sub-risk 1
- Sub-risk 2
- Sub-risk 3

Control 1
- Control 2
- Control 3

Middle Exec Management

Senior Exec Management

Staff
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

<table>
<thead>
<tr>
<th>Role</th>
<th>Expected Output</th>
<th>Sample Linking Parties and Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Identification</strong></td>
<td>Risk Identification and prioritization of new material risks.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Setting Risk Events</strong></td>
<td>Assigning assignments of risk events.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Assignment of Risk Responsibilities</strong></td>
<td>Setting risk responsibilities.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Risk Documentation</strong></td>
<td>Documenting risk documentation.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Risk Communication</strong></td>
<td>Communicating risk communication.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Risk Execution</strong></td>
<td>Executing risk execution.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Managing Risk Data</strong></td>
<td>Managing risk data.</td>
<td>Committees, Officers, etc.</td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td>Communicating risk communication.</td>
<td>Committees, Officers, etc.</td>
</tr>
</tbody>
</table>
Sample Coordination between Parties

Corporate Functions:
- Internal Audit
- SOX
- Corp ERM
  Informs & advises on risk & control activity

External Entities:
- Federal Government
- Regulatory Agencies
- State Governments
  Regulates on risk & control activity

Org Unit Risk Management:
- Drives, Coordinates, and advises on risk & control activity

GOVERNANCE
- Identify/monitor new & existing risks. Review ongoing risk & control activity

Risk Matrix Owner
- Responsible for all risk monitoring & mitigation activity of assign Risk Matrix

Executive Management
- Establish Objectives and Goals for the Division. Monitor & assign risk/control responsibilities as necessary

Executive Mgmt is part of & participates in Governance

Risk Owner
- Supports Risk Matrix Owner

Control Owner
- Supports Risk Matrix Owner and/or Risk Owner
Tactical Implementation of ERM

- Define Goals and Terms
- Develop Roles & Responsibilities
- Evaluate Organization Readiness
- Remediate Gaps
- Implement
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?
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
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?
How familiar is management and staff with ERM concepts?

Sample Actions

- Conduct survey to assess management and staff knowledge
- Interview management
### Sample Survey

<table>
<thead>
<tr>
<th>Question</th>
<th>Very Familiar</th>
<th>Somewhat Familiar</th>
<th>Not Very Familiar</th>
<th>Not at all Familiar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please rate your familiarity with risk management software</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Please rate your familiarity with COSO.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Please rate your familiarity with SOX.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Please rate your familiarity with the internal audit process.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Please rate your familiarity with privacy regulations.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Please rate your familiarity with fraud prevention and detection processes.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Please rate your familiarity with risk management methodologies.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>How familiar are you with the risks that face your area of responsibility.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>How familiar are you with risk assessment.</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
</tbody>
</table>
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?
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

<table>
<thead>
<tr>
<th>Color Key</th>
<th>Value Scale</th>
<th>DESIRED STATE</th>
<th>CURRENT STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red: Not familiar with the message</td>
<td>5-6</td>
<td>Role</td>
<td>Risk Mgmt Methods</td>
</tr>
<tr>
<td>Green: No messaging needed</td>
<td>0</td>
<td>Role</td>
<td>Risk Mgmt Methods</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audiences</th>
<th>Topic</th>
<th>Role</th>
<th>Risk Mgmt Methods</th>
<th>Systems</th>
<th>Role</th>
<th>Risk Mgmt Methods</th>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Mgt</td>
<td>General risk management vocabulary, topic areas, and control solution approaches.</td>
<td>5.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>1.5</td>
<td>1.5</td>
</tr>
<tr>
<td>Middle Mgt</td>
<td>Detail risk management vocabulary, topic areas, and control solutions approaches.</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Lower Middle Mgt</td>
<td>Detail risk management vocabulary, topic areas, and solutions approaches. Practical position specific strategies to risk management and controls.</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Risk Matrix Owners</td>
<td>Detail risk management vocabulary, topic areas, and solutions approaches. Practical position specific strategies to risk management and controls.</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Control Owners</td>
<td>Detail risk management vocabulary, topic areas, and solutions approaches. Practical position specific strategies to risk management and controls.</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Operations Senior Mgt</td>
<td>Detail risk management vocabulary, topic areas, and control solutions approaches.</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Other Admin &amp; Production Mgt</td>
<td>General awareness of risk management vocabulary, topic areas, and control solution approaches.</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>3.5</td>
<td>3.5</td>
</tr>
<tr>
<td>Corp Governance</td>
<td>Existence of Risk Mgmt Dept and its role in managing Division risk.</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>5.5</td>
<td>3.5</td>
<td>3.5</td>
</tr>
</tbody>
</table>
# 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**
  - Risk Mgt System
  - SOX System
  - Compliance System

### Best Communication Channel

<table>
<thead>
<tr>
<th>Audiences</th>
<th>Individualized</th>
<th>Generalized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Mgt</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Middle Mgt</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Lower Middle Mgt</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Risk Matrix Owners</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Control Owners</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Operations Senior Mgt</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Other Admin &amp; Production Mgt</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Corp Governance</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
**Sample Training Curriculum**

<table>
<thead>
<tr>
<th>TYPE</th>
<th>COURSES</th>
<th>HRS</th>
<th>PURPOSE</th>
<th>TOPICS ADDRESSED</th>
<th>TARGET AUDIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>RM 101 - Risk Management Overview</td>
<td>1</td>
<td>Introduce key Risk Management concepts and set the tone for future training sessions.</td>
<td>Terminology; Roles/Responsibilities; Methodology; Risk and Control Statements; and Systems</td>
<td>Senior and middle management</td>
</tr>
<tr>
<td></td>
<td>RM 201 - Corporate Governance</td>
<td>1</td>
<td>Introduce the roles and responsibilities that Corporate Governance plays to effectively manage risk.</td>
<td>Risk identification and evaluation; Internal controls; monitoring ongoing control effectiveness; remediation; Discuss roles and responsibilities of various committees, management, process owners, control owners, and use of risk system as an administrative tool.</td>
<td>Senior and middle management</td>
</tr>
<tr>
<td></td>
<td>RM 301 - Risk Management Culture</td>
<td>1</td>
<td>Increase awareness of bus unit’s own risk management culture by assessing the current environment and identifying opportunities for improvement</td>
<td>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.</td>
<td>Senior and middle management</td>
</tr>
<tr>
<td>TRAINING</td>
<td>Risk 101 - Risk Overview</td>
<td>1</td>
<td>To provide the audience with a basic understanding of risk related topics which will be discussed in greater detail in subsequent training courses.</td>
<td>Definition; Speed &amp; Vulnerabilities; Categories; Examples; Identification Techniques; Risk Owner Definition; Roles and Responsibilities; Key Risk Sys Screen; Risk Statements; Concept of Gross Risk vs. Net Risk; Risk Assessment and Risk Significance; and a Group Exercise.</td>
<td>Middle management</td>
</tr>
<tr>
<td></td>
<td>Risk 102 - Risk Identification</td>
<td>1</td>
<td>To provide the audience with specific tools to be utilized in the identification of risks related to their areas of responsibilities.</td>
<td>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</td>
<td>Middle management</td>
</tr>
<tr>
<td></td>
<td>Risk 201 - Risk Evaluation</td>
<td>1</td>
<td>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.</td>
<td>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.</td>
<td>Middle management</td>
</tr>
<tr>
<td></td>
<td>Risk 202 - Financial Exposure &amp; Impact Analysis</td>
<td>1</td>
<td>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.</td>
<td>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.</td>
<td>Middle management</td>
</tr>
<tr>
<td>CONTROL</td>
<td>Control 101 - Control Overview</td>
<td>1</td>
<td>To provide the audience with a basic understanding of control related topics which will be discussed in greater detail in subsequent training courses.</td>
<td>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).</td>
<td>Middle and lower middle management</td>
</tr>
<tr>
<td></td>
<td>Control 201 - Control Design</td>
<td>1</td>
<td>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.</td>
<td>Define what is and why we need to evaluate the internal control design; Science vs. Art: Defines 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.</td>
<td>Middle and lower middle management</td>
</tr>
<tr>
<td></td>
<td>Control 301 - Operational Effectiveness Evaluation</td>
<td>1</td>
<td>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.</td>
<td>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, performance 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.</td>
<td>Middle management</td>
</tr>
</tbody>
</table>
Tactical Implementation of ERM

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

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Matrix</th>
<th>Proposed Risk Matrix Scope/Responsibility</th>
<th>Proposed Risk Matrix Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sales Mgmt</td>
<td>Responsible for all risks and controls surrounding the sales management process: sales personnel qualifications, performance, current and future staffing levels, leadership development, and organization.</td>
<td>Risk Mgr 1</td>
</tr>
<tr>
<td>2</td>
<td>Pricing &amp; Product Development</td>
<td>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.</td>
<td>Risk Mgr 2</td>
</tr>
<tr>
<td>3</td>
<td>Credit Risk</td>
<td>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.</td>
<td>Risk Mgr 3</td>
</tr>
<tr>
<td>4</td>
<td>Vendor Mgmt</td>
<td>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.</td>
<td>Risk Mgr 4</td>
</tr>
<tr>
<td>5</td>
<td>Business Continuity</td>
<td>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.</td>
<td>Risk Mgr 5</td>
</tr>
</tbody>
</table>
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

Collateral for lent money may be inadequate or unsecured exposing the business to potential losses on defaulted receivables $10.0 Million

Collateral is inadequate or unsecured due to Fraud by Employees. $2.5 Million

Collateral is inadequate due to improper collateral review procedures $1.5 Million

Collateral is inadequately due to lack of proper documentation of security position $5.0 Million

Collateral is inadequate or unsecured due to Fraud buyer $1.0 Million

Collateral is inadequate due to improper Collateral review, caused by inadequate internal procedures $1.0 Million

Collateral is inadequate due to improper Collateral review, caused by incompetent External Parties. $.5 Million

Collateral is unsecured due to lack of proper filing, caused by inadequate internal procedures $4.0 Million

Collateral is unsecured due to lack of proper filing, caused by 3rd Parties $1.0 Million
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.
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.
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.
Sample Certification Process

**Executives**
Gov meetings and executives review & act upon certification results

- **Risk Matrix Owner Certification**
  - **Risk Owner Certification**
  - **Control Owner Certification**

- **Risk Matrix Owner Certification**
  - **Risk Owner Certification**
  - **Control Owner Certification**

- **Risk Matrix Owner Certification**
  - **Risk Owner Certification**
  - **Control Owner Certification**
Questions