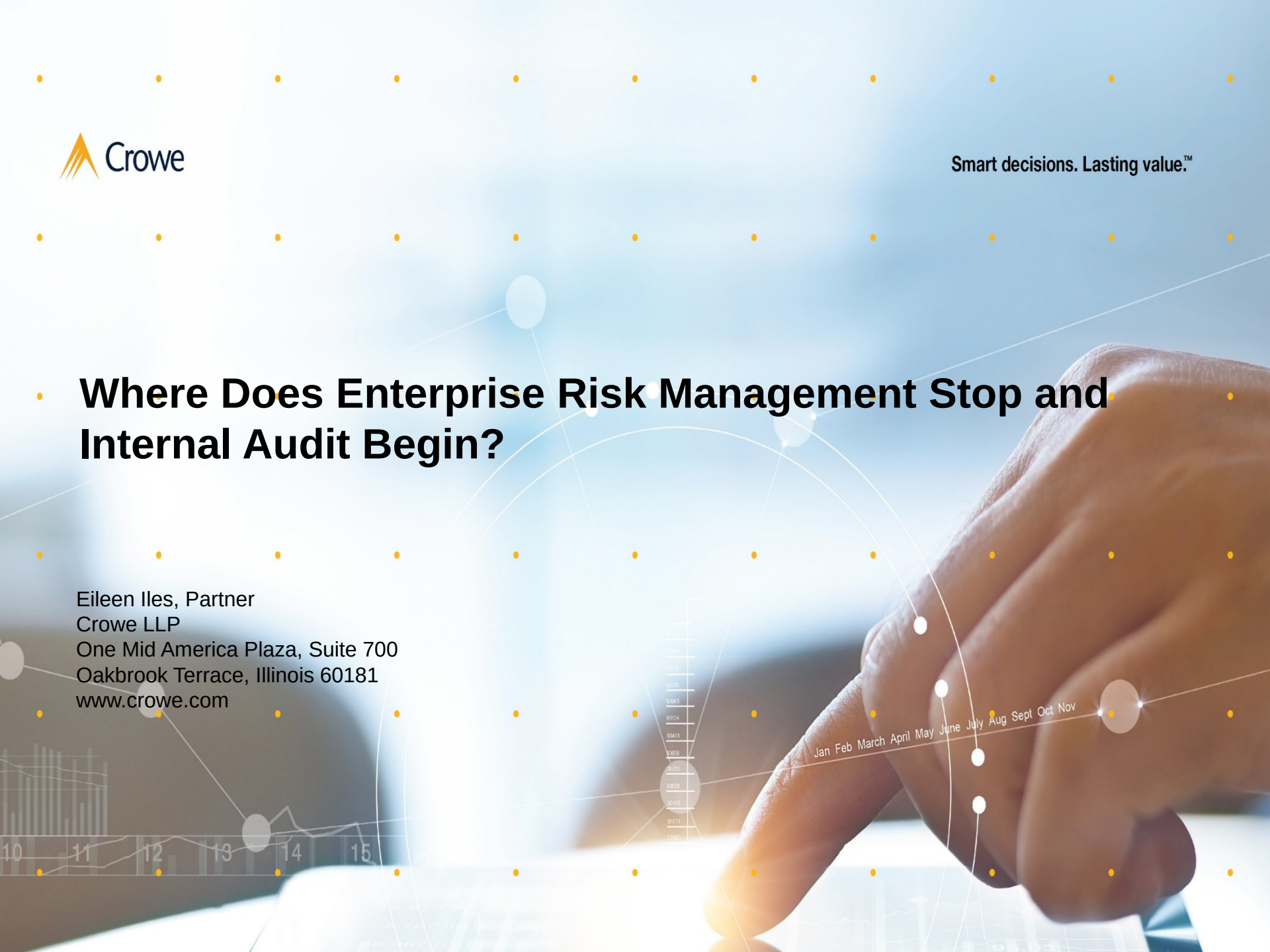
Crowe

Smart decisions. Lasting value.™

# Where Does Enterprise Risk Management Stop and Internal Audit Begin?

Eileen Iles, Partner
Crowe LLP
One Mid America Plaza, Suite 700
Oakbrook Terrace, Illinois 60181
www.crowe.com



# Enterprise Risk Management Update

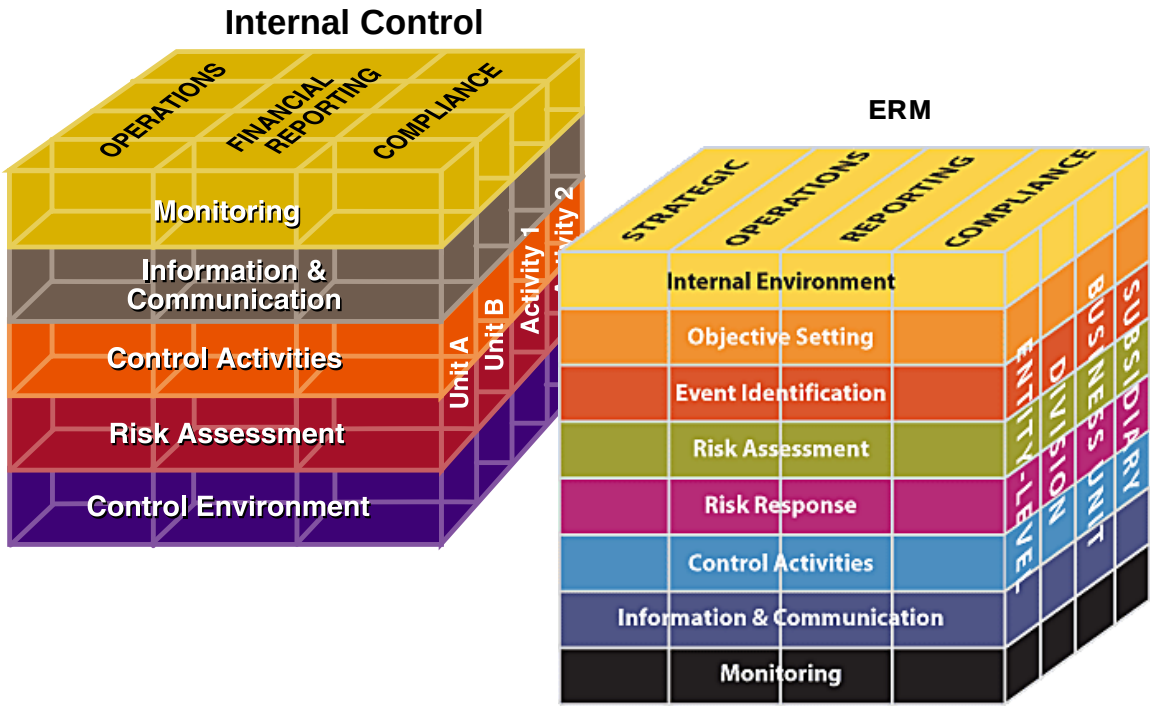
- 2004 COSO Enterprise Risk Management (ERM) Framework has been updated. In June 2017, COSO released Enterprise Risk Management Integrating with Strategy and Performance to clarify the meaning and role of ERM and provides detail guidance.
- Enterprise Risk Management Integrating with Strategy and Performance defines the Board's risk oversight responsibilities including governance and culture, strategy and objective setting, performance, information, communication, and reporting, and review and revision of practices to enhance performance.
- Enterprise Risk Management Integrating with Strategy and Performance Executive Summary is available for download on the internet at no cost. The full framework may be purchased from COSO.

# Enterprise Risk Management Misconceptions

- ✓ Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.
- ✓ Enterprise risk management is more than a risk listing. It requires more than taking an inventory of all the risks within the organization. It is broader and includes practices that management puts in place to actively manage risk.
- ✓ Enterprise risk management addresses more than internal control. It also addresses other topics such as strategy-setting, governance, communicating with stakeholders, and measuring performance. Its principles should be applied at all levels of the organization and across all functions.
- ✓ Enterprise risk management is not a checklist. It is a set of principles on which processes can be built or integrated for a particular organization, and it is a system of monitoring, learning, and improving performance.
- ✓ Enterprise risk management can be used by organizations of any size. If an organization has a mission, a strategy, and objectives—and the need to make decisions that fully consider risk—then enterprise risk management can be applied. It can and should be used by all kinds of organizations, from small businesses to community-based social enterprises to government agencies to Fortune 500 companies.

*Enterprise Risk Management Integrating with Strategy and Performance, June 2017*

# COSO Internal Control v ERM Model



# Enterprise-wide Risk Assessment – this is one part of ERM

## Sample Enterprise-wide Risk Assessment & Planning Summary

| Function | Credit Risk | Market Risk | Operational Risk | Technology Risk | Compliance Risk | Strategic Risk | External Risk | Aggregate Inherent Risk | Effectiveness of Internal Controls | Residual Risk | Audit Cycle (Years) | Direction of Risks | Reputation Risk |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Business Lending | High | High | High | High | High | Moderate | Moderate | High | Adequate | High | 1 | ⟷ | ✓ |
| Mortgage Lending | Moderate | Moderate | Moderate | High | High | Moderate | Moderate | High | Adequate | High | 1 | ⟷ | ✓ |
| Consumer Lending | Low | Low | Low | Low | Low | Low | Low | Low | Strong | Low | 3 | ⟷ | ✓ |
| Collections | N/A | N/A | Low | High | Moderate | Low | Low | Low | Adequate | Low | 3 | ⟷ | ✓ |
| Call Center | N/A | N/A | Moderate | High | Low | Moderate | Low | Moderate | Adequate | Moderate | 2 | ⟷ | ✓ |
| Share Operations | N/A | N/A | Moderate | High | Moderate | Moderate | Moderate | Moderate | Adequate | Moderate | 2 | ⟷ | ✓ |
| Branches | Low | N/A | Moderate | High | Moderate | Moderate | Moderate | Moderate | Adequate | Moderate | 2 | ⟷ | ✓ |
| Human Resources | N/A | N/A | Moderate | Moderate | Moderate | Low | Moderate | Moderate | Strong | Low | 2 | ⟷ | ✓ |
| Marketing | N/A | N/A | Low | Moderate | Moderate | Moderate | Moderate | Moderate | Adequate | Moderate | 2 | ⟷ | ✓ |
| Accounting | N/A | N/A | Moderate | High | Moderate | High | Low | Moderate | Adequate | Moderate | 2 | ⟷ | ✓ |
| Compliance | | | Moderate | High | High | Moderate | High | Moderate | Adequate | Moderate | 2 | ⟷ | ✓ |

# Risk Assessments – Activity Level

Enterprise-wide

| Compliance by Reg | Information Technology | Operations/Financial |
|---|---|---|
| Fair Lending | General Controls | Cash Mgt/Liquidity |
| ACH | Network Security | Loan Portfolio |
| Red Flags | Multi-Factor Authentication | Indirect Lending |
| BSA/AML Program | Gramm Leach Bliley: | Trust |
| | Security | Foreclosure Process |
| | Vendor Program Mgmt | |
| | Internet Banking | Business Member |
| | Remote Deposit Capture | Loan Stress Test |
| | Mobile Banking | |
| AML Customer Risk | Rating Vendor Risk Rating | Capital Stress Test |

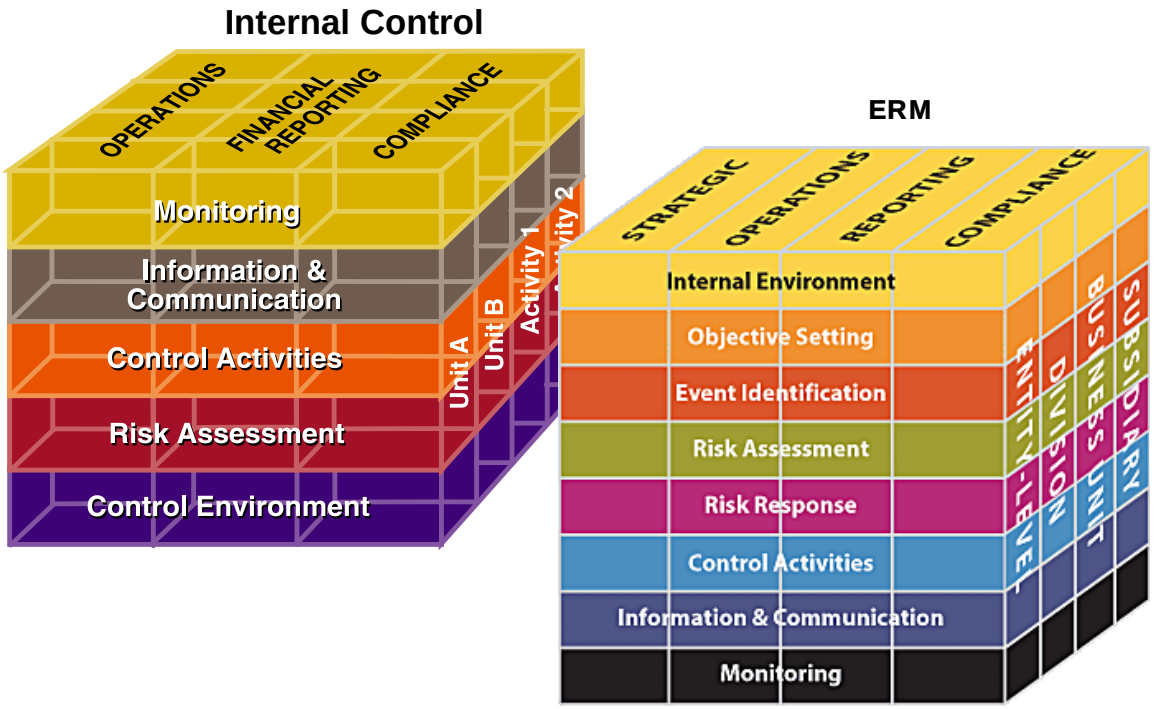
# Sample New Product Risk Assessment Format

## NEW PRODUCT RISK ASSESSMENT

**PRODUCT:** Indirect Loan Participation

| Risks | Likelihood | Impact | Aggregate Inherent Risk |
|---|---|---|---|
| | | | |
| Strategic | Moderate | High | High |
| Credit | Moderate | High | High |
| Market | Moderate | High | High |
| Operational | Low | Moderate | Moderate |
| External | High | High | High |
| Technological | Low | Moderate | Moderate |
| Legal | Low | Moderate | Low |
| Compliance | Low | Low | Low |
| Reputation | Low | Low | Low |
| Concentration | Low - TBD | Low -TBD | Low - TBD |
| Liquidity | Low | Low | Low |
| Aggregate | Moderate | High | High |

# COSO Internal Control v ERM Model



# Enterprise Risk Management Integrating with Strategy and Performance


*Enterprise Risk Management Integrating with Strategy and Performance, Committee of Sponsoring Organizations, June 2017*

# Enterprise Risk Management Integrating with Strategy and Performance


*Enterprise Risk Management Integrating with Strategy and Performance, Committee of Sponsoring Organizations, June 2017*

# Typical Regulatory Risks

- **Credit risk** arises from the potential that a borrower or counterparty will fail to perform on an obligation.
- **Market risk** is the risk to a financial institution's condition resulting from adverse movements in market rates or prices, such as interest rates, foreign exchange rates, or equity prices.
- **Liquidity risk** is the potential that an institution will be unable to meet its obligations as they come due because of an inability to liquidate assets or obtain adequate funding (referred to as "funding liquidity risk") or that it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions ("market liquidity risk").
- **Operational risk** arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses.
- **Legal risk** arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of an organization.
- **Reputational risk** is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.
- **Strategic risk** is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation.

# Sample Risk Universe

**External**
Regulatory/Legal
Investor Relations
Competitor
Financial Markets
Catastrophic Loss
Sovereign/Political

**Market**
Valuation (on and off BS)
Foreign Exchange

**Interest Rate Risk**
Re-pricing
Yield Curve
Basis
Options/swaps

**Legal**
Compliance
Litigation
Contractual/Obligations
Fiduciary


**Strategic**
Corporate Governance
Leadership
Alignment
Strategy
Strategic Objectives
Strategic Execution
Decision Making

**Reputation**
Fraud
Ethics
Privacy

**Credit**
Traditional (Cash Flow)
Portfolio
Products
Geographies
Concentrations

**Liquidity**

**Operational**
Accounting
Technology
Member Loyalty/Retention
Performance Measurement
Budgeting and Planning
Financial Reporting
Product Development and Pricing
Human Resources
Third Party Relationships
Business Interruption
Policy/Procedure Compliance

# Strategic Risk

**Strategic risk relates to strategy, strategic objectives, and execution of the strategy.**

**Risk of poor business decisions, from the substandard execution of decisions, from inadequate resource allocation, or from failure to respond well to changes in the business or economic environment.**

***Businessdictionary.com***

# Strategic Risk

Strategic risk often confused with Operational risk

**Operational** risk = **Doing Things** right

**Strategic** risk = Doing the **Right Things**

# Strategic Risk

## Strategic risk may be impacted by:

- Merger and acquisition
- Competition, other regulated financial institutions and financial services companies
- New markets, products, services
- Changing demand for products and services
- Emerging and changing technology
- Legal and regulatory change
- Competing priorities
- Stakeholder, cost, profitability pressure
- Constrained resources

# Strategic Risk Thinking

1. **Where are we now? Define mission, vision, risk philosophy, culture.**
2. **Where do we want to go? What do we want to be? ~ Define, communicate Strategy in light of Who are we?, define risk appetite.**
3. **Identify, prioritize, and time business opportunities and threats.**
4. **How will we get there? ~ Set SMART (specific, measurable, actionable, realistic, time-based) Strategic Objectives in light of How much risk are we willing to take on? ~ the organization's tolerance/risk limits.**
5. **How do we know if we are progressing? ~ Establish key performance indicators (KPIs) focused on measuring the attainment of strategic performance objectives.**
6. **What could hinder us from achieving our goals/strategic objectives? ~ Identify risks or events that could hinder the progress of attaining strategic objectives.**
7. **Establish key risk indicators (KRIs). KRIs monitor potential risk exposures. Exposures exceeding a reasonable range may require action and/or escalation.**
8. **How will we know when we have successfully attained the strategy? ~ Monitor short and long-term progress, KPIs, KRIs, and attainment of strategic objectives and strategy.**

# Risk Appetite

**Risk Appetite** is the aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

Pursuit of risk and the criteria taken into consideration for the credit union to decide whether or not to assume risk. It defines what types of risks the credit union will pursue; including types of markets, products, services, suppliers, and customers it will target.

RIMS "Exploring Risk Appetite and Risk Tolerance"

Risk appetite considers the residual risks ( risk remaining after taking into consideration effectiveness of internal controls).

# Risk Appetite Statement

Strategic objectives should not be developed, agreed and implemented in isolation or without consultation and consideration of the risk appetite statement.

Align risk appetite with risk philosophy and culture.

Risk Appetite Statement is the aggregate level and types of risk that the credit union is willing to accept, or to avoid, in order to achieve its business objectives. It includes qualitative statements as well as quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate. It should also address more difficult to quantify risks such as reputation and conduct risks as well as money laundering and unethical practices.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

# Risk Appetite Statement

According to the Committee of Sponsoring Organizations (COSO) of the Treadway Commission a risk appetite statement should effectively set the tone for risk management. “Understanding and Communicating Risk Appetite” stresses the importance of effective communication and monitoring.

For Risk Appetite to be applied effectively, it must be specific so that it may be measured and monitored by management. Risk Appetite may be expressed depending on complexity:

- An overall, broad risk statement;
- A risk appetite for each major class of organizational objective; and/or
- A risk appetite for each category of risk.

# Risk Appetite Statement – Quantitative Elements

**Quantitative elements of risk appetite statement may address:**

- Maximum tolerance for market, credit and operational losses
- Minimum credit rating level
- Minimum economic and regulatory capital surplus
- Economic value at risk
- Maximum earnings volatility
- Attainment of budgeted earnings
- Minimum excess liquidity resources to meet peak stressed liquidity requirements without the need to liquidate assets
- Required increase of capital to meet regulatory capital

# Risk Appetite Statement – Qualitative Elements

**Qualitative elements of risk appetite statement may address:**

- Type and level (high, moderate, low) of risks credit union is willing to assume
- Business requirements
- Functions and products
- Risks in decision making of new products, services, or business opportunities
- Risk tolerance, may be zero or % of risk compliance, such as 100% compliance with regulations

# Risk Appetite Statement - Examples

Some organizations approach risk statements with overall organizational statements, such as:

- Assume risks that the credit union can manage in order to maximize returns for the credit union
- Balance risk and reward with the impact of risks and the cost of managing those risks for the credit union
- Accept potential loss of X% of earnings for a X% probability of increasing earnings by X%
- Avoid risks that negatively impact the credit union’s reputation

# Risk Appetite Examples

*(Business risk)* The credit is conservative and the credit union offers only low-risk traditional products.

*(Strategic risk)*The credit union's strategic risk is moderate as the credit union plans to acquire certain assets this year.

*(Growth risk)* The credit union has a high risk appetite for organic or acquired growth.

*(Employee turnover of HR risk)*The credit union has a low risk appetite for employee turnover, given its strategic objective of growth.

# Effective Risk Appetite Statement

**An effective Risk Appetite Statement should**

1) include key background information and assumptions that form strategic and business plans at the time they were approved;
2) be linked to short- and long-term strategic, capital and financial plans, as well as compensation programs;
3) establish the amount of risk the financial institution is prepared to accept in pursuit of its strategic objectives and business plan, taking into account the interests of its customers (e.g. depositors, policyholders) and the fiduciary duty to shareholders, as well as capital and other regulatory requirements;
4) determine for each material risk and overall the maximum level of risk that the financial institution is willing to operate within, based on its overall risk appetite, risk capacity, and risk profile;
5) include quantitative measures that can be translated into risk limits applicable to business lines and legal entities as relevant, and at group level, which in turn can be aggregated and disaggregated to enable measurement of the risk profile against risk appetite and risk capacity;
6) include qualitative statements that articulate clearly the motivations for taking on or avoiding certain types of risk, including for reputational and other conduct risks across retail and wholesale markets, and establish some form of boundaries or indicators (e.g. non-quantitative measures) to enable monitoring of these risks;
7) ensure that the strategy and risk limits of each business line and legal entity, as relevant, align with the institution-wide risk appetite statement as appropriate; and
8) be forward looking and, where applicable, subject to scenario and stress testing to ensure that the financial institution understands what events might push the financial institution outside its risk appetite and/or risk capacity.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

# Risk Appetite Framework

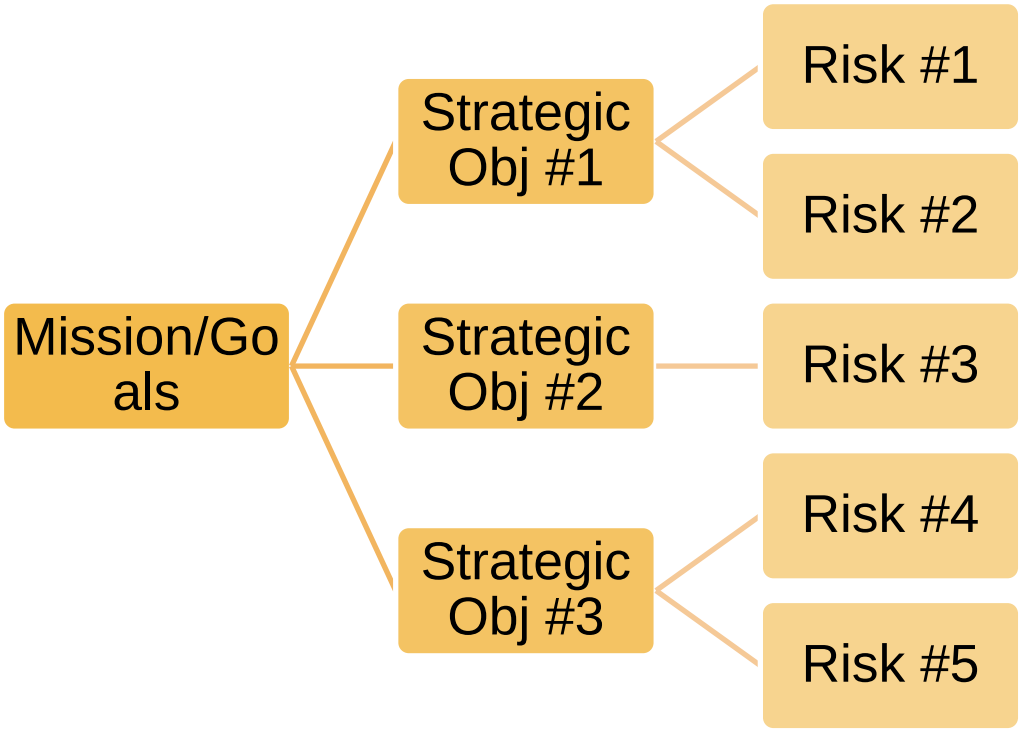
**Risk Appetite Framework** is the overall approach including policies, processes, limits, controls, and systems through which risk appetite is established, communicated and monitored.

- Develop a high level risk appetite and tolerance dashboard and for major business units with detailed appendices covering all relevant risk categories.
- Develop monitoring within business units and risk management function.
- Risk appetite and tolerance adherence should be embedded in all risk-related policies and guidelines.
- Risk appetite statement should be aligned with risk philosophy and culture.
- Define clear responsibility for setting, approving, and reviewing risk appetite and tolerances.
- Establish and communicate escalation mechanisms and consequences for noncompliance with tolerances.

The Risk Appetite Framework should be aligned with the business plan, strategy development, capital planning and compensation schemes.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

# Link Strategy to Strategic Objectives and Risks



# Risk Tolerance

**Risk tolerance** can be measured as an acceptable/unacceptable range of variation relative to the achievement of a specific objective or to the aggregated risk appetite. Risk tolerance provides constraints around the level of risk, which may have upper boundaries (e.g., tolerate no more than) and lower boundaries (e.g., tolerate at a minimum or not tolerate a return less than x based on the risk assumed).

It may be measured using the same units as the related objective.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

# Some More Risk Definitions

**Risk Capacity** is defined as the maximum amount or level of risk the credit union can assume given its current level of resources before breaching constraints determined by regulatory capital and liquidity needs, the operational environment (e.g. technical infrastructure, risk management capabilities, expertise) and obligations, also from a conduct perspective, to depositors, policyholders, shareholders, fixed income investors, as well as other customers and stakeholders.

**Risk limits** are quantitative measures based on forward looking assumptions that allocate the credit union's aggregate risk appetite statement (e.g. measure of loss or negative events) to business lines, legal entities as relevant, specific risk categories, concentrations, and as appropriate, other levels.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

# Risk Capacity Example

For a new product the credit union is seeking to offer to its members, risk capacity considerations would include…

People, skills knowledge - Does the credit union have enough people? People with the right knowledge and expertise?

System - Does the credit union have the system necessary to track, transact, report the new product?

Infrastructure - Does the credit union have the necessary marketing to promote and sell the new product?

Financial - Does the credit union have sufficient capital to support the new product?

Reputation - Will the product be well-received by its members? Has the credit union offered new products before successfully?

Regulatory, Legal - Are there any regulations that need to be complied with in regards to offering the new product?

# Risk Tolerance Examples

*(Risk Appetite)*The credit union is conservative and the credit union offers only low-risk traditional products. *(Tolerance)* The credit union will only offer new products with an internal risk assessed value of X.

*(Risk Appetite)*The credit union's strategic risk is moderate as the credit union plans to acquire certain assets this year. *(Tolerance)* The credit union may acquire credit union assets of less than $X.

*(Risk Appetite)*The credit union has a high risk appetite for organic or acquired growth, *(Tolerance)* as it desires a growth rate of X-Y% this year.

*(Risk Appetite)*The credit union has a low risk appetite for employee turnover, given its strategic objective of growth. *(Tolerance)* Employee turnover will remain at X% or lower this year.

# Other Risk Tolerance Examples

The credit union will not have a business loan concentration exceeding X%.

Commercial real estate loans will not exceed X% of the loan portfolio in any single geographic markets.

The credit union will continue to expand its operations with branches in locations where competition does not have market share over X%.

Loan servicing efficiency will remain above peers, X%.

The credit union will complete all compliance monitoring as scheduled, by year-end.

# Risk Limits

Risk limits should

1) be set at a level to constrain risk-taking within risk appetite, taking into account the interests of customers (e.g. depositors, policyholders) and shareholders as well as capital and other regulatory requirements, in the event that a risk limit is breached and the likelihood that each material risk is realized;

2) be established for business lines and legal entities as relevant and generally expressed relative to earnings, capital, liquidity or other relevant measures (e.g. growth, volatility);

3) include material risk concentrations at the credit union or group-wide, business line and legal entity levels as relevant (e.g. counterparty, industry, country/region, collateral type, product);

4) although referenced to market best practices and benchmarks, should not be strictly based on comparison to peers or default to regulatory limits;

5) not be overly complicated, ambiguous, or subjective; and

6) be monitored regularly.

*Financial Stability Board "Principles for an Effective Risk Appetite Framework," November 18, 2013.*

# Risk Tolerance

Risk appetite and tolerance are created by management and approved by the Credit Union's Board of Directors. Risk limits are identified by management for business units, functions, products to align with risk tolerance.

Amount of risk appetite and risk tolerance is a risk return trade off.

Generally,

- Greater risk appetite leads to focusing on greater earnings and return
- Lesser risk appetite leads to focusing on stable earnings and stable growth

The level of risk appetite leads to approaching competition, acquisition and merger, expansion, new products, and markets differently.

# Key Performance Indicators

KPIs measures the progress of an organization achieving its strategic objectives by measuring particular activities in which it engages. Often success is simply the repeated, periodic achievement of some levels of operational goal (e.g. sales, volume, zero defects, customer satisfaction, etc.)

KPIs should follow the SMART criteria.

# Key Performance Indicators

Which performance indicators are key?

How many KPIs should I monitor and report?

- KPIs should be identified consistent with the credit union's strategic objectives.
- The number of KPIs should be sufficient to effectively monitor the credit union's strategic objectives.
- KPIs may be financial and/or nonfinancial.

# Sample KPIs

Profitability

Cash flow

Loan paydown and payoff

Total loans (by loan type)

Accounts payable balance

Total compensation costs

Total expenses

Technology costs per employee

Loan growth (#, $, %)

Debt to equity

Innovation spending

% of investments

Return on assets

Net interest margin

#, % employees hired

Total interest by loan type

Investment income by investment type

New loans per loan officer

No new loans processed per loan processor

# Establishing KPI Framework

1. Identify KPIs focusing on significant performance activities.
2. KPI data should be collected on a consistent basis such as daily, weekly, monthly, quarterly.
3. KPIs should follow the SMART criteria.
4. Select a mix of leading and lagging indicators.
5. Link KPIs to strategic objectives.
6. KPIs should be calculated on a consistent basis. Compare KPIs with budget, strategic objectives, action plans.
7. KPIs should be reported to management, department managers, and the Board timely. Identify trends.
8. Develop/identify risk mitigation and escalation based if KPIs are not within a reasonable range of budget, strategic objectives, action plans.
9. Track risk mitigation and escalation. Establish action plans, resolution dates, and responsible party.
10. Report risk mitigation and escalation to management, department managers, and the Board timely.

# Key Risk Indicators

KRIs are a measure used in management to indicate how risky an activity is. **KRIs** are metrics used by organizations to provide an early signal of increasing **risk** exposures in various areas of the credit union. **KRIs** are measures of the possibility of future adverse impact.

**KRIs are an early warning system as alerts and predictors of unfavorable events.**

KRIs provide **information** as risk develops through its life, from root cause(s), through event(s) to final impact(s), red flags, symptoms, etc. and turns the information into **intelligence**.

Credit union should identify KRIs, related to people, processes, and systems.

# Sample KRIs

System
- number of IT system outages per month
- average length of time per incident system is down
- number of IT security breaches per month / year
- number of IT virus caused outage per month / year
- number of virus incidents
- systems that do not have current patches

People
- percentage of staff appraisals below “satisfactory”
- results of staff surveys
- actual and projected turnover rates
- actual versus budgeted FTE
- average length of service per member of staff

Members
- number of member complaints
- number of accounts per member or household
- average member survey rating(s)

Process and Products
- number / percentage of accounts with outstanding / incomplete customer documentation
- number / percentage of member accounts with significant change in volume or dollars
- Average time to setup share accounts
- Average time to approve auto loans
- Impact of projected unemployment on loan delinquency
- ALLL per loan (by loan type)
- Fair lending indicators (% loans approved, % loans denied – by loan officer, geography)
- Interest rate risk such as net economic value, impact of rising interest rate scenario on capital and assets
- Comparison of credit union to peer benchmarks

# Establishing KRI Framework

1. Identify KRIs focusing on significant risks.
2. KRI data should be collected on a consistent basis such as daily, weekly, monthly, quarterly.
3. KRIs should follow the SMART criteria.
4. Select a mix of leading and lagging indicators.
5. Link KRIs with risk appetite, tolerance, and limits. Risk appetite, tolerance, and limits should be approved by the Board.
6. KRIs should be calculated on a consistent basis. Compare KRIs with tolerance/limits.
7. KRIs should be reported to management, department managers, and the Board timely. Identify trends.
8. Develop/identify risk mitigation and escalation based on risk impact (severity) and frequency.
9. Track risk mitigation and escalation. Establish action plans, resolution dates, and responsible party.
10. Report risk mitigation and escalation to management, department managers, and the Board timely.

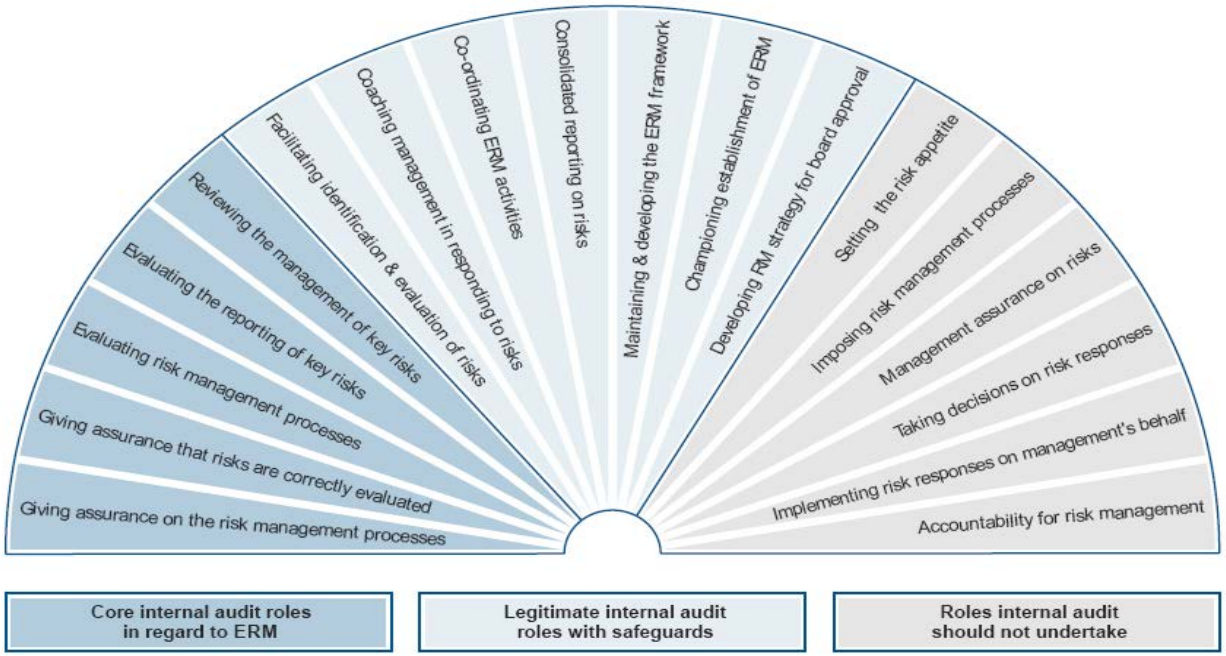
# Risk Appetite and Risk Management

- Once risk appetite has been established, management should implement internal controls to mitigate and monitor residual risk falls within the credit union’s risk appetite.
- Risk appetite can then be incorporated in strategic and business planning and other activities leading to a more risk aware culture.
- Risk appetite should be monitored and compliance with policy to the Board of Directors.

# Roles and Responsibilities – Three Lines of Defense Model for Risk Accountability

- **First line** – Risk management strategy at each business unit. Business units must own the risks associated with their activities.
- **Second line** – Risk management and compliance organization: this line focuses on the coordination and development of policies, the reporting structures and the monitoring of compliance with statutory rules and internal policies. Typically overseen by the risk management department and/or executive management committee.
- **Third line** – Internal audit function: Internal audit performs regular internal auditing of key controls (or risk-based plan).

# Internal Audit Model Functions Within ERM




**IIA 2004 Position Statement: The Role of Internal Audit in Enterprise-Wide Risk Management**

# Risk Appetite and Internal Audit

- Risk appetite falls within the scope of Internal Audit. Internal Audit's role includes evaluating the effectiveness and contribution to the improvement of risk management processes, Institute of Internal Auditors Standard 2120.
- Risk appetite may be included in internal audits to support the Board's statement on the credit union's risk management and control systems. This may result in a broader review of risk management.
- Internal Audit may consider reviewing the credit union's risk appetite and whether significant risks are identified and assessed with an appropriate risk response aligned with the credit union's Risk Appetite.
- Internal Audit may also assess the maturity of the credit union's risk management and definition, identification, communication of risk appetite throughout the credit union. Additionally, Internal Audit may also assess monitoring and whether risk appetite is updated as risks and strategic objectives change.

# Board Risk Oversight

Board's role includes but is not limited to:

Overseeing, Reviewing, Challenging management, and Approving ERM elements related to governance and culture; strategy and objective-setting; performance; information, communications and reporting; and review and revision of practices to enhance performance.

Some Considerations:

- How may significant business decisions impact performance, risk, strategy, culture, etc.?
- Does the credit union evaluate alternative strategies and the impact of risk?
- Does the credit union have a process to monitor and respond to significant changes in business, environment, risk, deviations from etc.?
- Are strategy and business objectives aligned with mission, vision, and core values?
- Has the credit union assessed its risk and identified the behaviors that exhibit its desired organizational culture?
- Is the credit union monitoring deviations from its core values?
- In the credit union's review of performance, does it consider risk, risk appetite, tolerance, limits, and risk response?
- How is risk, culture and performance reported?
- Has the credit union identified its risk appetite?
- Does the credit union use its systems to gather and obtain current and future needed data to assess, monitor, and re-evaluate risk impact, risk appetite, etc?
- Has the credit union determine whether its current system has the capabilities to obtain, store, report future needed data?

# Current Risk Topics Impacting Financial Institutions

- Speed of financial technology disruption, innovation, and automation
- Emerging and changing technology
- Cyber threats and cybersecurity
- Privacy and information security
- Third party risk management
- Mergers and acquisitions
- Regulatory changes and consumer compliance
- Political uncertainty
- Succession
- Talent
- Corporate Culture – flexibility, agility
- Sustaining member loyalty
- Millennials as employees and
- Millennials as members (customers)
- Growing the membership
- Economic conditions
- Possible interest rate rise and impact on deposits and capital
- Fee-based products and services
- Cost pressure
- How to identify emerging risks

- Big data analytics
- Alignment of strategy, risk, and performance
- Nonbank companies competing with financial institutions
- Examiner focus of new, growing areas/products/services; signs of credit easing, BSA/AML, ALM, readiness for CECL
- Current expected credit losses (CECL)

# The Role of the Board of Directors/Audit/Supervisory Committee

Provides monitoring, guidance, and direction.

Defines what it expects in regards to integrity and ethical values.

Through its oversight, determines whether expectations are being met.

# The Role of the Board of Directors/Risk Committee

Oversight to determine that appropriate risk management processes are implemented and effective.

Is aware of and concurs with the Financial Institution's risk appetite.

Reviews the Financial Institution's portfolio view of risk and considering it against the entity's risk appetite.

Is apprised of the Financial Institution's most significant risks and risk mitigation efforts implemented by management.

# The Role of the Risk Committee

While Senior Mgmt is responsible for assessing and managing the Financial Institution's exposure to risk, the Risk Committee is responsible for guidelines and policies that govern the process of risk assessment and risk management.

**"Risk" Committee Charter should address the Committee's duties and responsibilities.**

- It addresses enterprise-wide risks, and sets performance measure goals, risk limits, risk tolerances, and key risk indicators for those risks.
- It is responsible for capital allocations, capital planning, and risk capital allocation and overrides.
- The committee also reviews capital usage and actual risk management performance versus plan.

# The Role of the Risk Committee

**(example) Objectives**

- Ensure that management understands and accepts its responsibilities for identifying, assessing, and managing risk;
- Management are focused on enterprise-wide risk strategy;
- Leading tools and processes are provided to the businesses to facilitate achievement of their Risk Management responsibilities;
- Business unit risk assessments are performed periodically and completely;
- Business unit risk mitigation activities are successful in:
  - safeguarding assets
  - maintaining appropriate standards regarding the environment and health and safety issues
  - meeting legal and regulatory obligations
  - reinforcing the values of the Financial Institution by focusing on stakeholder needs
- Proper accounting records are being maintained, appropriate accounting policies have been adopted and financial information is comprehensive and accurate; and
- Effective risk mitigation/control testing programs are in place and the results evaluated and acted upon.

# The Role of the Risk Committee

**(example) Responsibilities**

- Oversee development of and participation in an annual enterprise-wide risk strategy analysis
- Develop and refine the enterprise-wide appetite/tolerance for risk
- Provide direction and oversight to the Chief Risk Officer and the Global Risk Leaders
- Evaluate material risk exposures and report to Board
- Evaluate enterprise-wide risk exposure report
- Evaluate enterprise-wide risk trending report and ensure corporate strategy is responsive to issues raised
- Oversee the role and responsibilities of the Internal Audit Team
- Review semi-annual and annual consolidated accounts

# The Role of the Risk Committee

**(example) Structure and Membership**

- Members of the Committee will be appointed by resolution of the Board
- The Committee will comprise four non-executive Board directors, one of whom will be appointed to chair the Committee

**(example) Meetings**

- Meetings will be held quarterly prior to Board meetings
- The General Counsel & Secretary will attend all Committee meetings and will act as Committee Secretary. The Chief Risk Officer and the CFO will also attend all Committee meetings
- A report of the meeting will be presented to the next Board meeting following each Committee meeting

# Enterprise Risk Management Policy – Items to Consider

Purpose

**The purpose of the organization's enterprise risk management is as follows:**

- Maintain an ERM program consistent with the COSO ERM Framework.
- Ensure that current significant and emerging risks are identified, understood, and evaluated.
- Effective risk management systems and processes are implemented to manage, monitor, and report these risks.

Goals

**Potential value capabilities of enterprise risk management include the following:**

- Aligning the financial institution's risk appetite with its strategic and related operational, compliance, and reporting objectives;
- Enhancing risk response decisions;
- Reducing operational deficiencies and possible losses;
- Identifying and managing interrelated risks;
- Providing integrated responses to multiple risks;
- Seizing opportunities; and
- Improving deployment and allocation of capital.

# Enterprise Risk Management Policy – Items to Consider

Objectives

The enterprise risk management approach focuses on the financial institution at the enterprise and business level and the achievement of enterprise strategic, operational, compliance, and reporting objectives. Business level objectives focus on why the particular business or business unit exists, how the business affects the financial institution's strategy, earnings, reputation, and other key success factors, and whether the business level objectives are aligned with the enterprise objectives.

**Specific objectives of establishing an enterprise risk management process include the following:**

- Creating a holistic view of risk in which risk is considered comprehensively and consistently communicated, utilizing the *Common Risk Language* and documented in decision making;
- Centralizing the risk management oversight of risk management activities;
- Creating an awareness of all risks facing the financial institution by defining the financial institution's risks that will be addressed by the enterprise and each functional area or business unit;
- Establishing and maintaining systems and mechanisms to comprehensively identify, assess, and measure risks that may impact the financial institution's ability to achieve its business objectives;
- Creating a process that ensures that for all new lines of business and new product decisions that management evaluate the expertise needed and comprehensively assess risk;
- Establishing and maintaining systems and mechanisms to monitor risk responses;
- Developing risk occurrence information systems to provide early warning of events or situations that may occur or already exist which create risk for the financial institution;
- Creating and maintaining risk management tools such as policies, procedures, controls, and independent testing;
- Instituting and reviewing risk measurement techniques within the financial institution that management may use to establish the institution's risk tolerance, assess risk likelihood and impact, and analyze risk monitoring processes; and
- Establishing appropriate management reporting systems regarding the financial institution's risk exposures and allocation of capital.

# Enterprise Risk Management Policy – Items to Consider

Objectives

**Other objectives of this policy are as follows:**

- Identify key responsibilities of the Board of Directors, Risk (Management) Committee, Chief Risk Officer, and management.
- Establish the organization's risk appetite and identify the organization's method of establishing and complying with key risk indicators.
- Communicate required reporting to the Board of Directors, Risk Committee, and management, including content, format, and frequency.
- Maintain an environment of risk management.
- Review of organization's enterprise risk management framework, risk environment, and identified risks to determine if any changes are necessary.

# Enterprise Risk Management Policy – Items to Consider

Guidelines

**The *COSO ERM Framework* describes eight interrelated components that enterprise risk management comprises. The components are as follows:**

- ***Internal environment*** - The internal environment sets the tone of the financial institution and sets the basis for how risk is viewed and addressed by personnel. The internal environment includes risk management philosophy, risk appetite, integrity and ethics, and the environment in which personnel operate.
- ***Objective setting*** – Objectives must be identified before management can identify events that may affect its ability to achieve its business objectives. The objectives should be aligned with and support the financial institution's strategy within its risk appetite. Business objectives include the financial institution's strategic and related operational, compliance, and reporting objectives.
- ***Event identification*** – Event identification refers to the identification of internal and external events that can affect the financial institution's ability to achieve its objectives. Events may represent risks or opportunities.
- ***Risk assessment*** – Risk assessment is the analysis of risks to determine how they may be managed. The likelihood and impact of the risks are considered within the analysis. Risks are assessed on an inherent and residual basis. Because many risks may be identified during the risk assessment stage, management should consider focusing on the key risks that may materially impact the financial institution.
- ***Risk response*** – Risk response refers to the risk strategies available to management. Risk responses include avoiding the risk, transferring the risk, reducing the impact of the risk, or accepting the risk.
- ***Control activities*** – Control activities are the policies and procedures established to ensure that risk responses are carried out effectively.
- ***Information and communication*** – Relevant information is identified, captured, and communicated timely to enable personnel to fulfill their risk management responsibilities.
- ***Monitoring*** – Once risk management activities have been implemented, management should monitor these activities to ensure that they continue to operate as intended. Forms of effectively monitoring risk management activities include key risk and performance measures, periodic self-assessments by key risk owners, and periodic, independent audits.

# Enterprise Risk Management Policy – Items to Consider

Responsibilities

**The Board of Directors is responsible to perform the following:**

- Oversee ERM program.
- Ensure that processes are in place to identify current significant and emerging risks.
- Understand the nature, likelihood, and impact of significant risks impacting the organization.
- Annually review organization's strategies and risk management policies to ensure that the policies, risk tolerances, key risk indicators continue to appropriately reflect the organization's strategies and risk appetite.
- Authorize Risk Committee to approve ERM policy.

**The Risk Committee is responsible to perform the following:**

- Report to the Board of Directors of significant risks, risk exposure, gaps, etc
- Review management's and/or Risk Management Committee's identification of current significant and emerging risks.
- Review and approve ERM policy.
- Ensure that management has implemented enterprise-wide processes and controls to measure, manage, monitor, and mitigate significant risks.
- Appoint Chief Risk Officer as the individual within management to be responsible for identifying, managing, monitoring, mitigating significant risks.

# Enterprise Risk Management Policy – Items to Consider

**Risk Management Committee/Chief Risk Officer is responsible to perform the following:**

- Ensure appropriate management processes have been implemented to measure, monitor, mitigate risk.
- Recommend risk tolerances, key risk indicators to the Risk Committee/Board of Directors.
- Determine risk responses to mitigate risk to an acceptable level.
- Ensure that appropriate resources are allocated to ERM.
- Communication to and training for employees occurs timely and is effective.

**Other Committees that Manage risk:**

<Describe how the Risk (Management) Committee will work with the other committees.>

**Management is responsible to perform the following:**

- Identify, measure, manage, monitor, mitigate significant risks to an acceptable level.
- Ensure that appropriate resources are allocated to ERM.
- Review and evaluate ERM processes and activities. This may be performed by an independent function or outside party. The results of such review should be communicated to the Risk Management Committee/CRO and Risk Committee.

# Enterprise Risk Management Policy – Items to Consider

**Risk Owners are responsible for the following:**

- Risk owners are responsible for the development, implementation, operation, and monitoring of the financial institution's risk management capabilities and activities.
- Specifically, in order to successfully develop, implement, operate, and monitor the financial institution's risk management activities, risk owners must:
- Understand the financial institution's changing risk profile, as well as the Board's and senior management's tolerance levels, to ensure the risk management activities under their responsibility are designed to manage risks consistent with the corporate governance direction and tolerance levels;
- Reassess whether the current design of risk management activities continues to provide reasonable assurance that the risks will be managed within the stated tolerance levels;
- Evaluate whether the necessary capabilities continue to exist to execute the risk management activities;
- Monitor the risk management activities to ensure that they are operating as designed and achieving the desired result; and
- Provide senior management with information regarding the effectiveness of activities to manage the business within risk tolerance levels.

**Internal Audit is responsible for the following:**

- Internal auditors are responsible for planning their audit activities to periodically reassess the design and operation of key risk management processes and make periodic evaluations of the ongoing accuracy and effectiveness of the communications from risk owners to senior management, and from senior management to the Board of Directors.

# Enterprise Risk Management Policy – Items to Consider

Risk Appetite and Key Risk Indicators

The organization's risk environment and appetite are <conservative, moderate, risky. The terms used should be defined and the definition should be based on the key risk indicators and risk tolerances identified. <Key risk indicators and risk tolerances should be identified for each risk event deemed to significantly impact the organization.>

# Enterprise Risk Management Policy – Items to Consider

Reporting

**Quarterly the CRO will present to the Risk Committee the following:**

- Any completed independent reviews of ERM and findings and recommendations, along with management's action plan for resolution.
- Status of identification and risk assessment of current, changing, and new significant risks.
- Emerging risks including risk assessment and plan for risk mitigation.
- Risks that exceed risk limits and tolerances and/or trends thereof.
- Any recommendations for improvement.
- Any exceptions to this policy.

**Quarterly, the Risk Committee will then update the Board of Directors regarding the items above.**

Review of ERM Program

The organization's ERM framework and program will be reviewed and evaluated. Recommendations will be reported to the Risk Committee and Board of Directors.

# ERM Checklist

- Survey practices according to ERM components.
- Determine maturity of ERM practices.
- Develop action plan to implement outstanding components or improve upon existing practices.
- Strategic Planning – are strategies defined such that strategic objectives can be measured and monitored?
- Identify risk categories pertinent and significant to strategic objectives.
- Identify risk events for each strategic objective.
- Identify likelihood and impact for each risk event.
- Identify key risk indicators, risk limits, risk tolerance for each significant risk event.
- Establish processes to monitor risk indicators, risk limits, risk tolerances.
- Assign risk owners.
- Establish reporting processes.
- Define committee(s) and assign committee members.
- Develop Risk (Management) Charter.
- Develop ERM policy.
- Provide ERM training to employees.
- Communicate ERM policy to employees.
- Engage internal audit to review practices of high importance to ERM.
- Perform risk assessment for new products and services.
- Evaluate and re-evaluate ERM program.

## ERM Internal Audit

- Governance
- Policy
- Program
- Risk Appetite
- Risk Statement
- Action Plan / CHecklist
- Monitoring and Exception Approvals
- Training
- Communication
- Reporting
- Internal Controls
- Procedures

# Thank YOU!

Eileen Iles
Crowe LLP
eileen.iles@crowe.com