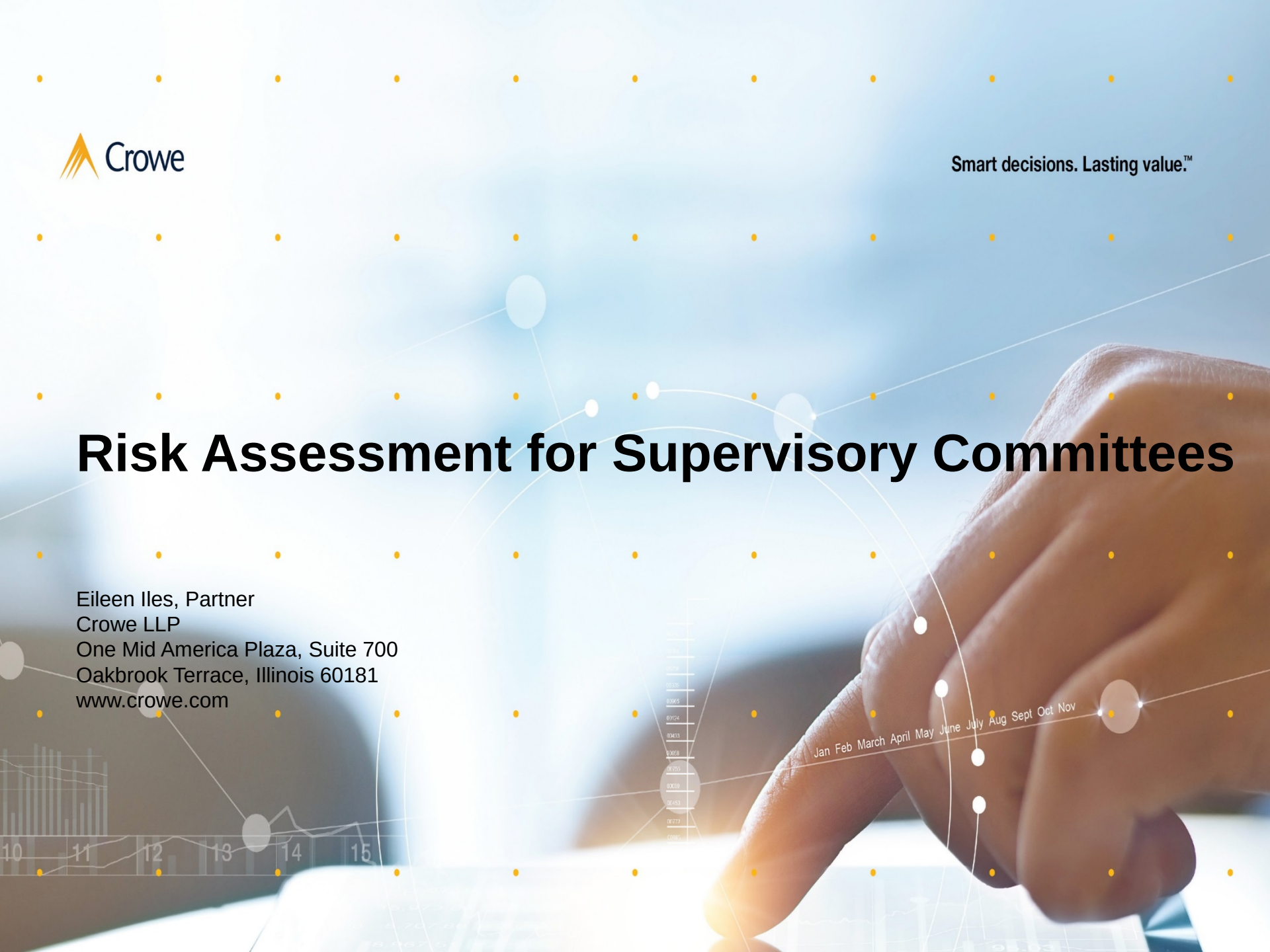
Crowe

Smart decisions. Lasting value.™

Risk Assessment for Supervisory Committees

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



Supervisory Committee Responsibilities

- ✓Oversight of financial reporting and internal controls
- ✓Oversight of independent auditor
- ✓Oversight of internal audit
- ✓Risk oversight
- ✓Ethics
- ✓Compliance

Risk Oversight

Risk Oversight includes but is not limited to:

Overseeing, Reviewing, Challenging management, and Approving enterprise-wide risk elements related identifying, assessing, monitoring, and reporting of risks impacting the credit union. Areas include governance and culture; strategy and objective-setting; performance; information, communications and reporting; and review and revision of practices to enhance performance.

Board should determine which risks the Board should monitor versus other risks to be delegated to Board Committees.

What is Risk?

Risk is anything that may potentially impede your organization from achieving its objectives or have an adverse impact on capital or earnings.

Types of risk include:

-Credit risk
-Interest rate risk
-Market risk
-Operational risk
-Liquidity risk
-Strategic risk
-Reputation risk
-Legal risk

Risk management ≠ Risk elimination

How Do We Assess Risk?

How Do We Assess Risk?

- Determine objectives
- What could go wrong?
- Risks?
- Impact (Quantity and Quality)
- Direction of risk
- Assume the risks or mitigate the risks?
- What should we do?

COSO Internal Control-Integrated Framework

- First published in 1992
- Gained wide acceptance following financial control failures of early 2000's
- Most widely used framework in the US
- Also widely used around the world

Original COSO Cube

Obtained from Committee of Sponsoring Organization's December 2011 presentation of *An Update of COSO's Internal Control – Integrated Framework*

COSO Codification of Internal Control Framework Principles

Control Environment	1. Demonstrates commitment to integrity and ethical values. 2. Exercises oversight responsibility. 3. Establishes structure, authority, and responsibility. 4. Demonstrates commitment to competence. 5. Enforces accountability.
Risk Assessment	6. Specifies suitable objectives. 7. Identifies and analyzes risk. 8. Assesses fraud risk. 9. Identifies and analyzes significant changes.
Control Activities	10. Selects and develops control activities. 11. Selects and develops general controls over technology. 12. Deploys through policies and procedures.
Information and Communication	13. Uses relevant information. 14. Communicates internally. 15. Communicates externally.
Monitoring Activities	16. Conducts ongoing and/or separate evaluations. 17. Evaluates and communicates deficiencies.

Note: Companies will need to link their internal controls to the 17 principles.

COSO Internal Control-Integrated Framework

Internal Control Components - 1. Control Environment

- The organization structure of the institution.
- Management's philosophy and operating style
- The integrity, ethics, and competence of personnel.
- The external influences that affect the bank's operations and risk management practices.
- The attention and direction provided by the board of directors and its committees, especially the audit or risk management committees.
- The effectiveness of human resource policies and procedures.

COSO Internal Control-Integrated Framework

Internal Control Components - 2. Risk Assessment

- Risk assessment is the identification, measurement, and analysis of risks, both internal and external, **controllable and uncontrollable**, at individual business levels and for the bank as a whole.
- Management must assess **all risks** facing the bank because uncontrolled risk-taking can prevent the bank from reaching its objectives or can jeopardize its operations.
- Effective risk assessments help determine what the risks are, what controls are needed, and how they should be managed.

COSO Internal Control-Integrated Framework

Why is Risk Assessment Important?

- To ensure “risks” are identified
- To ensure policies exist to mitigate risk
- To ensure compliance with policies
- To most effectively allocate limited resources
- To comply with regulatory guidance

COSO Internal Control-Integrated Framework

Internal Control Components – 3. Control Activities

- Policies, procedures, and practices that help ensure board and management directives are carried out.
- Help ensure that necessary actions are taken to address risks to achievement of the entity's objectives.

COSO Internal Control-Integrated Framework

Internal Control Components - 4. Information and Communication

- Information systems produce reports that make it possible to run and control the business.
- Communication from top management that control responsibilities must be taken seriously.
- A means of communicating upward, and with external parties.

COSO Internal Control-Integrated Framework

Internal Control Components - 5. Monitoring

= A process that assesses the quality of the system's performance over time.

= Bank's own oversight of the control system's performance.

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 Credit Union'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, or unforeseen catastrophes will result in unexpected losses.
- **Fraud risk** is the risk of deliberate deception, misuse, or misapplication of organizational assets or resources in order to take advantage and benefit from personally from such acts.
- **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.
- **Compliance risk** is the potential of regulatory order, fines, or penalties assessed as a result of noncompliance with regulations.
- **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

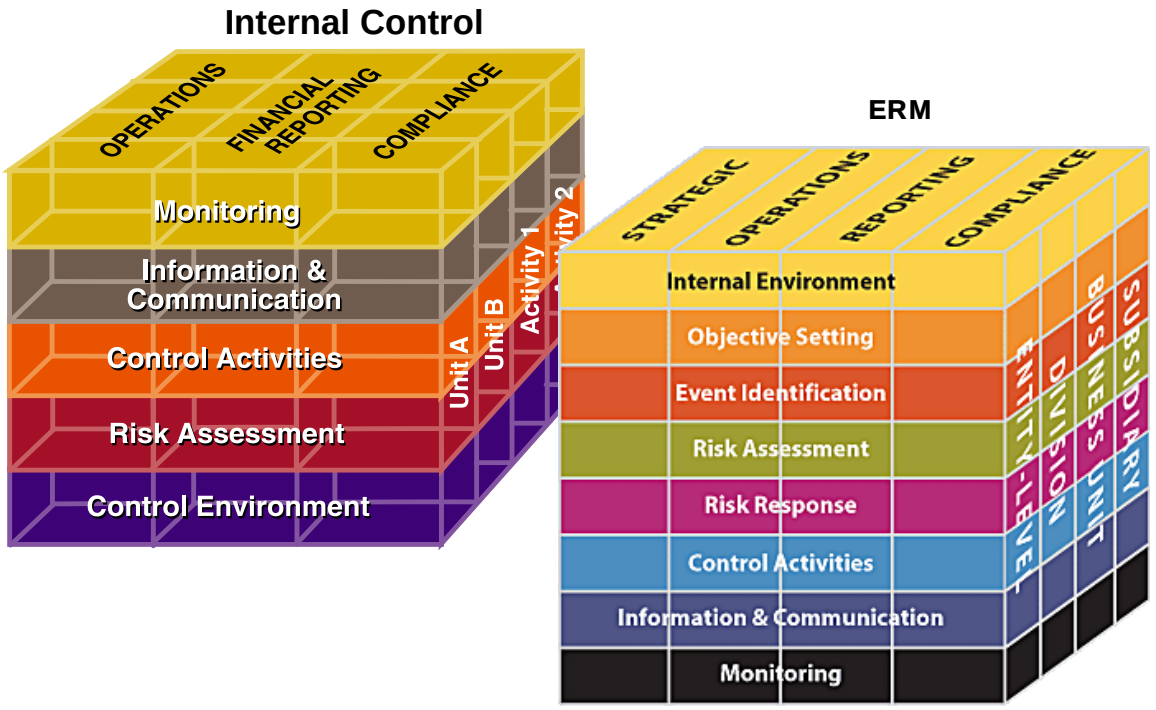
Reputation
Fraud
Ethics
Privacy

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

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 Regulation

Specific Areas of Regulatory Focus

Fair Lending
Adverse Action
Consumer Loan Compliance
Compliance Management Program

Red Flags
BSA/AML Program

AML Customer Risk Rating

Information Technology
All systems, governance, connectivity

General Controls

Network/Cyber Security

Multi-Factor Authentication
Gramm Leach Bliley Privacy
Information Security

Internet Banking
Remote Deposit Capture
Mobile Banking
Wire Transfers
ACH

Operations/Financial
All functions, products, services

Cash Management/Liquidity
Interest Rate Risk

Business Lending
Loan Servicing
Indirect Auto Lending
Trust
Foreclosure and Repossession Processes
Vendor Program Management
Vendor Risk Rating

Loan Stress Test

Capital Stress Test

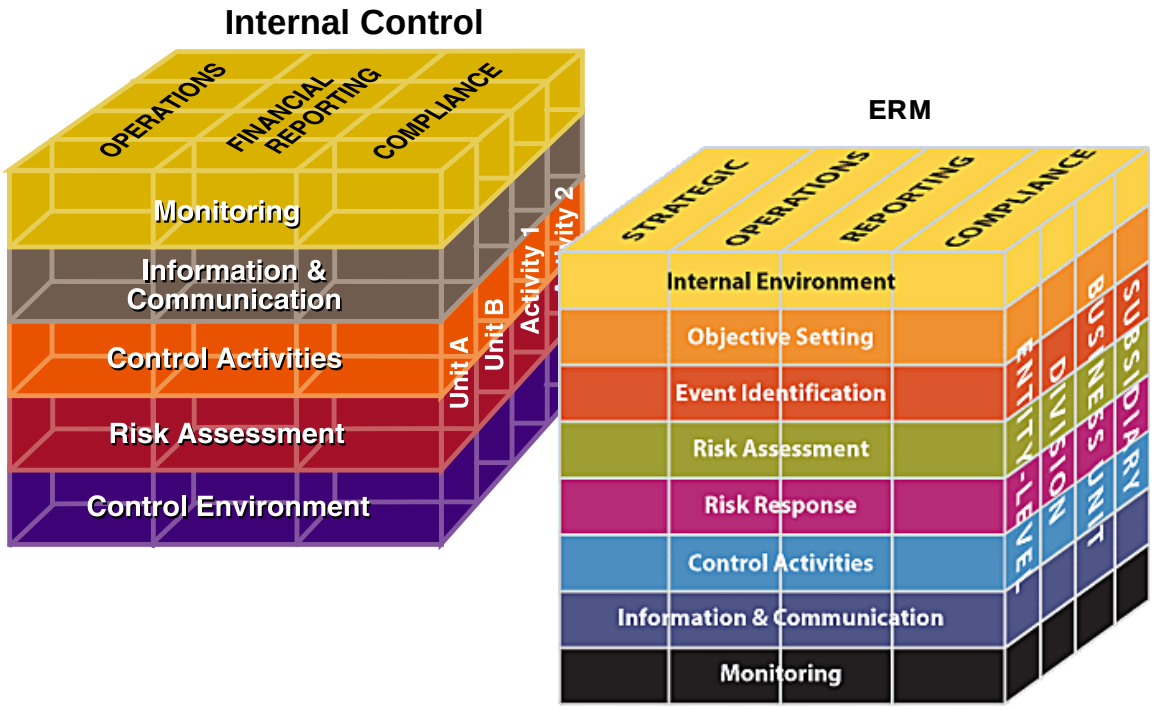
Sample New Product Risk Assessment Format

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

Internal Control v ERM Model



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 Credit Unions 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

Enterprise Risk Management Misconceptions

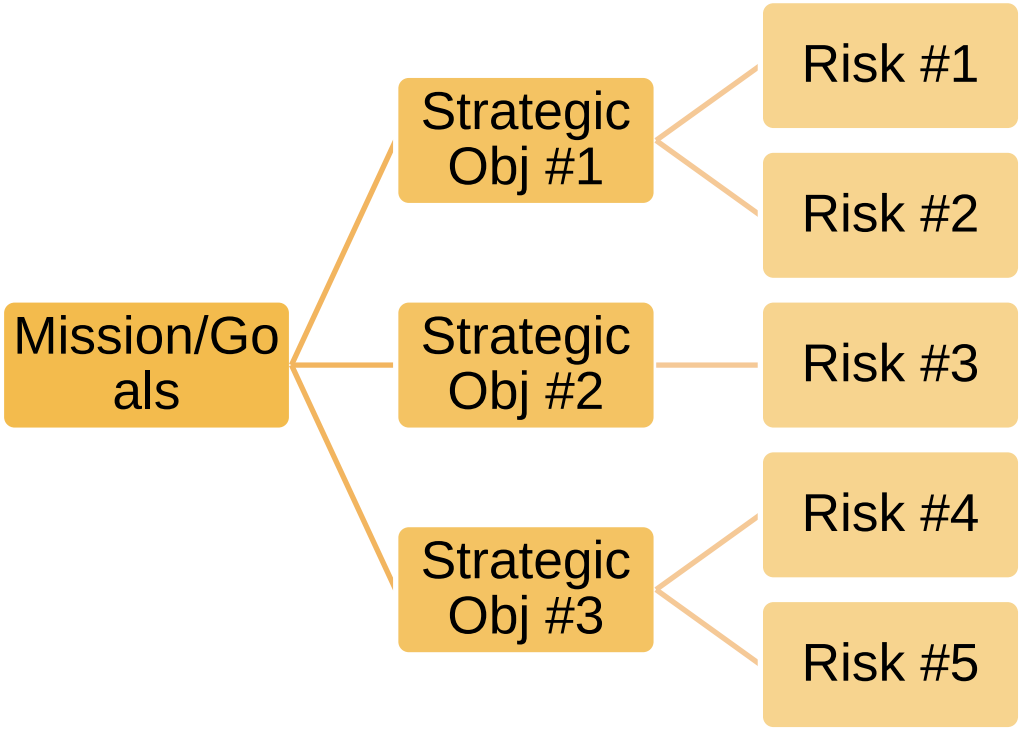
- ✓ Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.
- ✓ Enterprise risk 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

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.**

Link Strategy to Strategic Objectives and Risks – Strategic Risk Assessment



Supervisory Committee and Risk Assessment v Risk Oversight

- Supervisory Committee's responsibility is risk oversight
- Management (1st and 2nd lines of defense) is responsible for assessing risk
- Management (1st and 2nd lines of defense) owns the risk assessment process for activity and ERM assessments
- Internal Audit provides effective challenge and feedback to (Management 1st and 2nd lines of defense) completeness and types of significant risks, assessment of risks, direction of risks.

Three Lines of Defense 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 functions: 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).

Risk Oversight

- Oversight to determine that appropriate risk management processes are implemented and effective.
- Is aware of and concurs with the Credit Union's risk appetite.
- Reviews the Credit Union's portfolio view of risk and considering it against the entity's risk appetite.
- Is apprised of the Credit Union's most significant risks and risk mitigation efforts implemented by management.

Risk Oversight

While Management is responsible for assessing and managing the Credit Union's exposure to risk, the Risk Oversight (Supervisory Committee or separate 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 Risk Committee also reviews capital usage and actual risk management performance versus plan.

Risk Oversight

(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 Credit Union 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.

Risk Oversight

(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

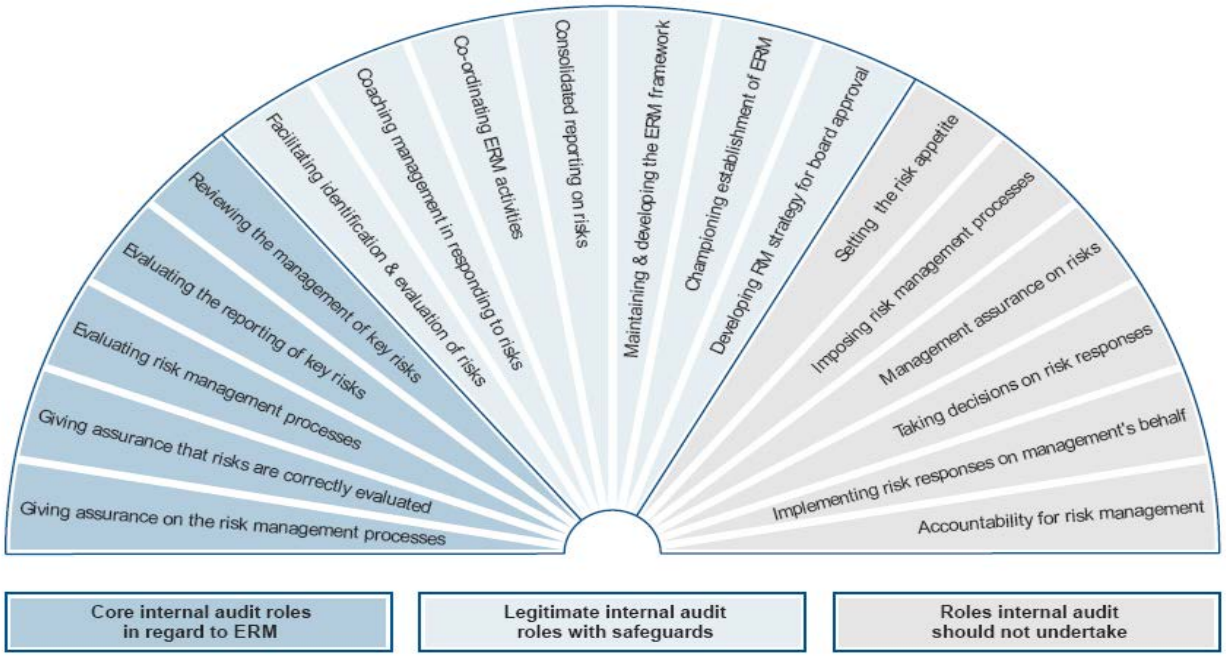
Risk Oversight Questions to Ask

- Does the credit union have a defined governance structure?
- Does the credit union have a list of all enterprise-wide risks?
- Are all enterprise-wide risks assigned to a Board level Committee for oversight?
- How do the Board Committees oversee risk?
- Who has the authority to take risk on behalf of the Credit Union?
- Does the Credit Union have an enterprise risk management policy?
- Does the Board/Supervisory Committee need to seek outside resources for assistance?
- How may significant business decisions impact performance, risk, strategy, culture, etc.?
- Does the credit union evaluate alternative strategies and the impact of risk?
- What are the risks associated with attaining the credit union's strategy?
- 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?

Risk Oversight Questions to Ask

- 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?
- Does management provide adequate information for the Board to oversee the credit union's risk management program?
- How do we know that the information reported regarding risks and risk management is accurate and complete?
- Have expectations been effectively communicated to senior management concerning the Credit Union's risk management process, and is there a clear understanding of those expectations, including the information we expect to receive?
- Has management assigned risk owners?
- Does the credit union have policy and processes to identify, assess, and monitor enterprise-wide risks?
- Are the credit union's compensation program aligned with financial performance? Is the Supervisory Committee aligned with these risks?
- How does the credit union identify and monitor emerging risks?
- How is technology assessed and evaluated in the credit union's risk management program?
- Are cyber and compliance risk on the Supervisory Committee agenda?

Internal Audit Role in ERM



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

Current Risk Topics Impacting Credit Unions

- Speed of financial technology disruption, innovation, and automation
- Emerging and changing technology
- Cyber threats and cybersecurity
- Privacy and information security
- Third and fourth 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 Credit Unions
- Examiner focus of new, growing areas/products/services; signs of credit easing, BSA/AML, ALM, readiness for CECL
- Current expected credit losses (CECL)
- Compensation programs

Evolving risks = Need for additional risk assessment and risk oversight

Supervisory Committee Responsibilities

- ✓Oversight of financial reporting and internal controls
- ✓Oversight of independent auditor
- ✓Oversight of internal audit
- ✓Risk oversight
- ✓Ethics
- ✓Compliance

How is risk assessment a component of each of the responsibilities above?

Enterprise Risk Management 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?
- ❑Perform enterprise-wide and strategic risk assessments.
- ❑Perform risk assessment for new products and services.
- ❑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 and risk owners.
- ❑Establish reporting processes.
- ❑Define committee(s) and assign committee members.
- ❑Develop and Approve Risk (Management) Charter.
- ❑Develop and Approve ERM policy.
- ❑Approve risk indicators, risk limits, risk tolerances, risk owners, and reporting.
- ❑Provide and Approve ERM training to employees.
- ❑Communicate ERM policy to employees.
- ❑Engage internal audit to review practices of high importance to ERM.
- ❑Evaluate and re-evaluate ERM program.

Risk assessment
Risk Oversight

Questions??

Thank YOU!

Eileen Iles
Crowe LLP
eileen.iles@crowe.com