Auditing ERM – Making ERM Part of your Audit Program



June 21, 2018

WIPFLi LLP
CPAs and Consultants

Presenter

Sara Mikuta
Partner
Wipfli LLP
630.368.7013
smikuta@wipfli.com

WIPFLI LLP
CPAs and Consultants

ERM – the Basics

WIPFLi LLP
CPAs and Consultants

Enterprise Risk Management (ERM)

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

Enterprise Risk Management

- Whose responsibility?
- Can’t hire out ERM
- It’s never done
- It’s a mindset
- It’s a continuing activity to evolves over time
- No silver bullet solution

WIPFLi LLP
CPAs and Consultants

ERM Components

- Established “Risk Culture” – tone at the top
- Clear Objectives – marrying strategy with risk management
- Event Identification – and how management responds
- Risk Assessment – continuous assessing risk
- Risk Response – Avoid, Accept, Reduce, Share

ERM Components

- Control Activities – Independent from risk-taking and operational functions
- Information and Communication – relevant information is critical
- Monitoring - are we operating with parameters set.

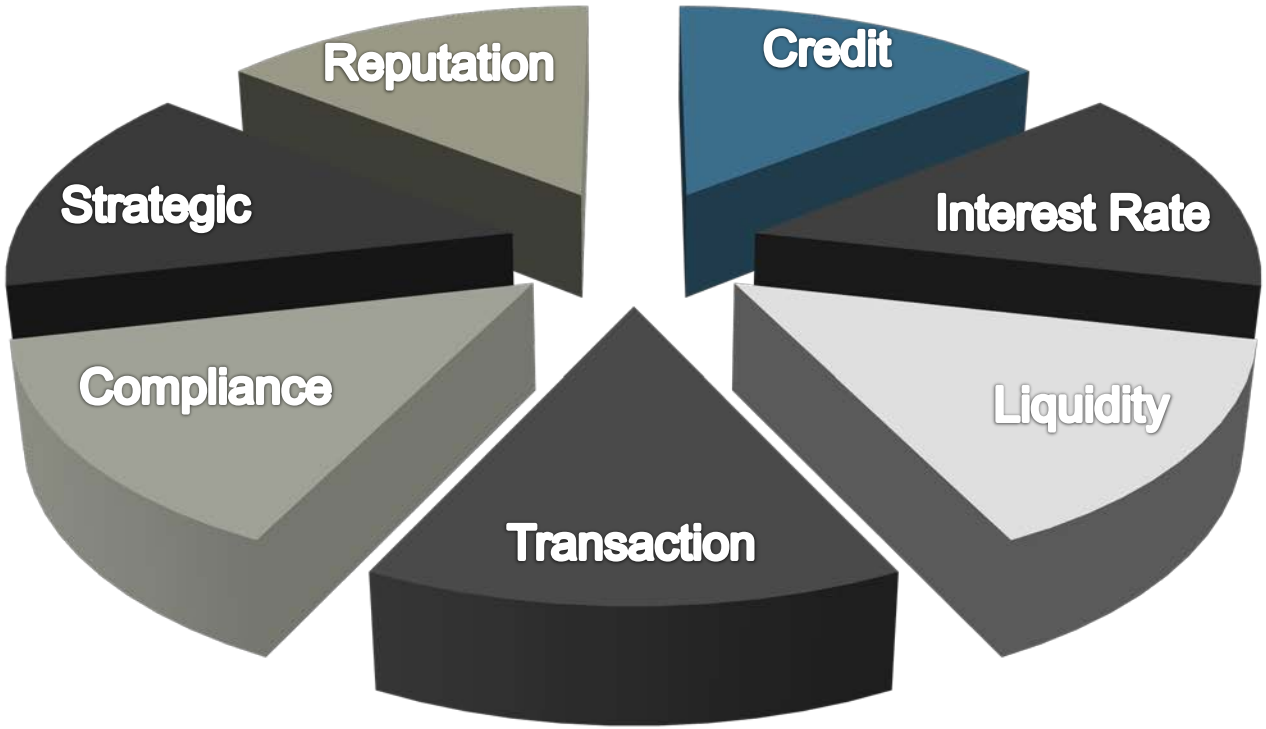
Regulator Expectations

- "Natural person credit unions are not required to implement a formal ERM framework. ***However, credit unions are expected to have sound processes sufficient to manage the risk associated with their business model and strategies."***
- "There is no 'off-the-shelf" solution for organizations seeking to launch an effective enterprise-wide approach to risk management. Rather, organizations can meet their specific needs with various tailored approaches that take into account the complexity, resources, and expertise. Credit Unions that incorporate ERM into their risk management infrastructure may resource the program internally, **through paid consultants (emphasis added ☺)**, or through a combination of outsourced and internal resources. NCUA does not view any approach as preferable…."

  - NCUA Letter to Credit Unions No. 13-CU-12

WIPFLi LLP
CPAs and Consultants

What Risks are we managing?



WIPFLi LLP
CPAs and Consultants

How Does the Board and Management get their arms around all those risks?

WIPFLi LLP
CPAs and Consultants

What Are Your Silos?

WIPFLi LLP
CPAs and Consultants

Examination Expectations

- Will be evaluated on the management of risks as noted above and in coordination with CAMEL ratings.
- Absence of solid risk management frameworks/processes may result in regulatory action.

ERM – An Internal Audit Approach

WIPFLi LLP
CPAs and Consultants

Internal Auditor Responsibilities

- Play an important role in ERM, but do NOT have primary responsibility from implementation or its maintenance.
- Can assist management and the Board by
  - Can "champion" the implementation of the process
  - Monitoring and providing assurance on risk management processes
  - Provide advice on controls and risk management tools and practices

WIPFLi LLP
CPAs and Consultants

Internal Audit Coverage

- Coverage dependent on size/breadth of ERM program. Maturity of the program should also be considered in your risk ratings.

- Internal control adequacy can be part of your risk based program and plan each year.

Internal Audit Coverage

- Coverage should include the following:
  - Board and Management Oversight
  - Procedures, Policies and Limits
  - Risk Monitoring and Management Information Systems
  - Internal Controls

WIPFLi LLP
CPAs and Consultants

Some simple ERM Internal Audit Steps

- Obtain copies and read/evaluate the following:
  - Risk Management Organization Chart
  - ERM policy and procedures
  - ERM most recent company wide risk assessments
  - Risk Appetite Statement
  - Internal ERM training materials
  - Last ERM risk profile
  - Interim ERM updates to last annual risk profile
  - Director and senior management ERM reporting package(s), including minutes of ERM committees and Board noting discussion of ERM

Some simple ERM Internal Audit Steps

- Perform an assessment to ascertain:
  - Current ERM governance framework coverage and strengths. Determine work performed related to the updated COSO Enterprise Risk Management framework, if applicable.
  - Scope of the risk governance framework
  - Roles and Responsibilities of ERM constituents
  - Strategic Plan and incorporations into ERM Elements
  - Risk Appetite Statement, including process to set levels of risk
  - Concentration and front-line risk
  - Risk Appetite monitoring and communication
  - Risk Limit breaches

WIPFLi LLP
CPAs and Consultants

Some simple ERM Internal Audit Steps

- Perform an assessment to ascertain:
  - Concentration risk management
  - Risk data aggregation and reporting
  - Relationship of risk appetite statement, concentration risk limits and front-line unit risk limits to other processes
  - Talent management processes
  - Compensation and performance management programs

Some simple ERM Internal Audit Steps

- Interview key ERM board and management team members to determine their understanding and active role in ERM function.

WIPFLi LLP
CPAs and Consultants



Resources

- COSO – Enterprise Risk Management – Integrating with Strategy and Performance www.coso.org
- The Institute of Internal Auditors www.na.theiia.org
- NCUA – Supervisory Letter 13-12
- Federal Reserve Bank Supervisory Guidance 16-11

WIPFLi LLP
CPAs and Consultants

Questions?

WIPFLi LLP
CPAs and Consultants



www.wipfli.com/fi