SMARTER risk management

ERM Roles & Responsibilities In Community Banks:

Who is Responsible for What?

By:

John Hurlock, President

JohnHurlock@smarterriskmanagement.com

Kelly Lutinski, National Director

KellyLutinski@smarterriskmanagement.com

www.smarterriskmanagement.com

Managing risk in banks and credit unions belongs to the entire organization – from the teller, to the lender, to the executive officer. The management of risk occurs through the implementation of policies and procedures, adhering to those policies and procedures, and proactively monitoring and reacting to changes in the organization's internal and external environments. Now regulators strongly recommend implementing Enterprise Risk Management (ERM). When educating ourselves about ERM, a whole host of questions come to mind:

How does ERM fit into our organization?

How does ERM affect our current risk management processes?

Can Internal Audit be responsible for ERM or should a separate individual or group be responsible?

How does the communication process work?

Ultimately, it comes down to "who is responsible for what?" in a successful ERM program.

This question is important because there are many assumptions and misunderstandings about roles and responsibilities in an ERM program. This leads to gaps in a program that leave the financial institution vulnerable to credit, financial, and operational risks, that in the event of a proverbial "bad day" – and as consultants we have seen numerous "bad day" scenarios – become realities. The organization can become subject to situations that threaten its very survival.

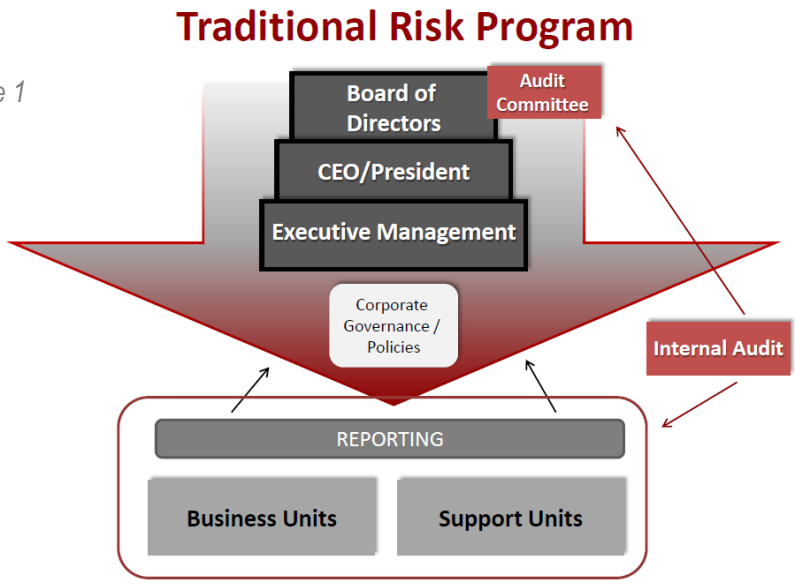
The fact that these questions continue to be asked is a key indicator there is confusion about job roles and responsibilities and this confusion needs to be addressed. Before we explore the answers to these questions, let's take a quick look at how risk is currently managed in a financial institution.

Traditional Risk Program

Figure 1 shows a typical risk program in a pre-ERM financial institution. The board, CEO / President, and executive management provide the risk governance and policies that should be followed throughout the organization. The governance and policies provide all business lines and support units the 'rules' to be followed in order to manage to the organization's risk tolerance.

Those responsible for managing risks in a traditional financial institution framework are the managers and line personnel who ensure compliance with industry regulations and the rules provided by management. The executive management and board receive feedback on the adherence to the rules and regulations through the regular reporting that comes from the business and support units. They also receive feedback from the Internal Audit department through audit reports.

Figure 1



This is a simplistic rendition of the risk framework in many organizations, which performed fairly well over the years – and, to be frank, we have not seen significant changes in this approach despite the fact that the whole environment has changed. For example, one of the primary challenges we continue to see with a framework of this type is that there is limited communication occurring from the business units to management. The majority of the communication coming from the line is information requested by management. There is little opportunity, and little benefit, for line personnel to communicate information to management without it first being requested. In many of the financial crises that have occurred in the last thirty years, the front line was where it was first noted that things weren't going as planned, but the troops refused to speak up – primarily out of belief that someone else must be dealing with the problem.

Enterprise Risk Management Program

Over the last several years, risk management has become co-mingled with Enterprise Risk Management. While the two are closely related, Risk Management primarily focuses on managing specific risk activities within the organization – similar to what was described in traditional risk programs. Enterprise Risk Management focuses on identifying and managing risks across and external to the entire organization.

There are many different, though similar, definitions of Enterprise Risk Management. COSO defines Enterprise Risk Management as:

> "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, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[1]

The Institute of Internal Audit defines Enterprise Risk Management as follows:

> "Structured, consistent, and continuous process across the whole organization, for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the achievement of its objectives."[2]

Regardless of the definition used, this new approach requires financial institutions to view risk more holistically (and comprehensively) than they have before in a way that:

> "Crosses silos, builds internal alliances, exhibits flexibility, expands to include emerging risks and enhances the strategic decision-making capability of the individual organization. Critical to that end are building alliances with internal risk-related functions that also have the unique responsibility of understanding all that makes up the enterprise. Key among those is the internal audit function." [3]

The ERM Program is different from traditional risk programs in two fundamental ways:

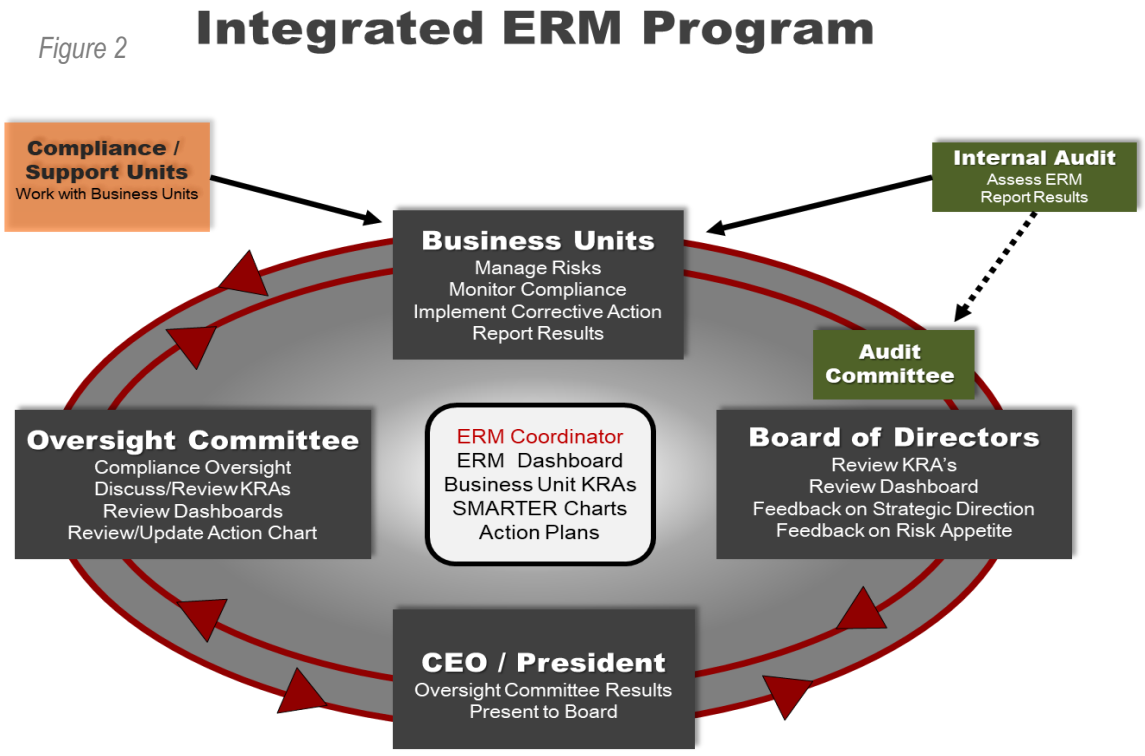
- Continuous Communication
- Formalization of Risk Management Processes

[1] Enterprise Risk Management – Integrated Framework, Issued by COSO September 2004
[2] IIA Position Paper: The Role of Internal Auditing in Enterprise Risk Management, Issued January 2009
[3] Risk Management and Internal Audit: Forging a Collaborative Alliance, Issued 2012

As Figure 2 shows, the primary difference is the continuous communication that occurs not just from the board to the business and support units but then from the business and support units back to management and the board. This open communication creates more transparency within the organization on what risks are occurring within the organization because information is not just being passed down but is being communicated multi-directionally.

The second primary difference is the formalization of the risk management process. By getting all different areas of the organization involved in risk management and making decisions based on the organization's risk appetite, there is a requirement to assign an individual to coordinate and lead this effort. The program shown in Figure 2 cannot be successful in financial institutions without a defined risk function that is responsible for formalizing and managing the risks across the organization, and this function must be different from the Internal Audit function.

Figure 2



The Role of the Risk and Internal Audit

Since the establishment of the Internal Audit function in the 1940's, the role in financial institutions has always been defined as an independent, value-added, assurance activity and critical to the risk and control functions in the organization. Executive management and the board have relied heavily on Internal Audit's assessment of the internal control environment and the integrity of financial statements.

Internal Audit used to be viewed solely for the purpose of opining on internal controls and financial statements, in 1999, the Institute of Internal Auditors (IIA) expanded the definition of internal audit to be a more value added function. The IIA defined the role of Internal Audit to be:

> "An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."[4]

However, most financial institutions continue to view the Internal Audit function, whether it's in-house, co-sourced or outsourced, as an independent assurance function with a focus on internal controls and financial statements. This assurance is really targeted at the board of directors in order to provide shareholders with a reasonable certainty that things are working as expected. Some organizations have expanded the Internal Audit role to include some consultative activities but few financial institutions have been successful using Internal Audit in that role. Because of this, the Internal Audit and Risk functions need to be further clarified in order to eliminate any ambiguity about these roles.

[4] www.iia.org

CASE STUDY

In 2007, a $1.2 billion mid-western bank implemented an ERM program. The Compliance Officer (who also had Internal Audit reporting to her administratively) was assigned the role of Risk Manager and was responsible for implementing and maintaining the program. The ERM program had the same look and feel as the organization's Compliance Program and was very detailed in scope. While the Compliance Officer (as the Risk Manager) tried to instill an understanding of risk and risk appetite across the organization, the program was never fully established or embraced.

In 2010, we were asked to assist the Bank in redefining their ERM program. In order to understand the current risk program and where it broke down, we had discussions with key management. The main factor that caused the rejection of the program was a lack of understanding of 'who was responsible for what.' There was not a clear understanding of the roles and responsibilities assigned which created a level of ambiguity across the organization. The key managers also indicated the program approach felt more like an Audit rather than a way to proactively identify risk.

In redefining the program, the first thing we did was formally define 'who was responsible for what' and communicate this across the organization. By clearly defining the roles of the board, executive management, risk management, compliance, internal audit, and the line managers, everyone understood where their responsibilities were and how to complete them. Additionally, we took a more holistic approach to the program incorporating work already being done in the organization so as to not duplicate efforts. Identified risks were also assigned to specific individuals to support ownership and responsibility. The program was successfully up and running in less than six months.

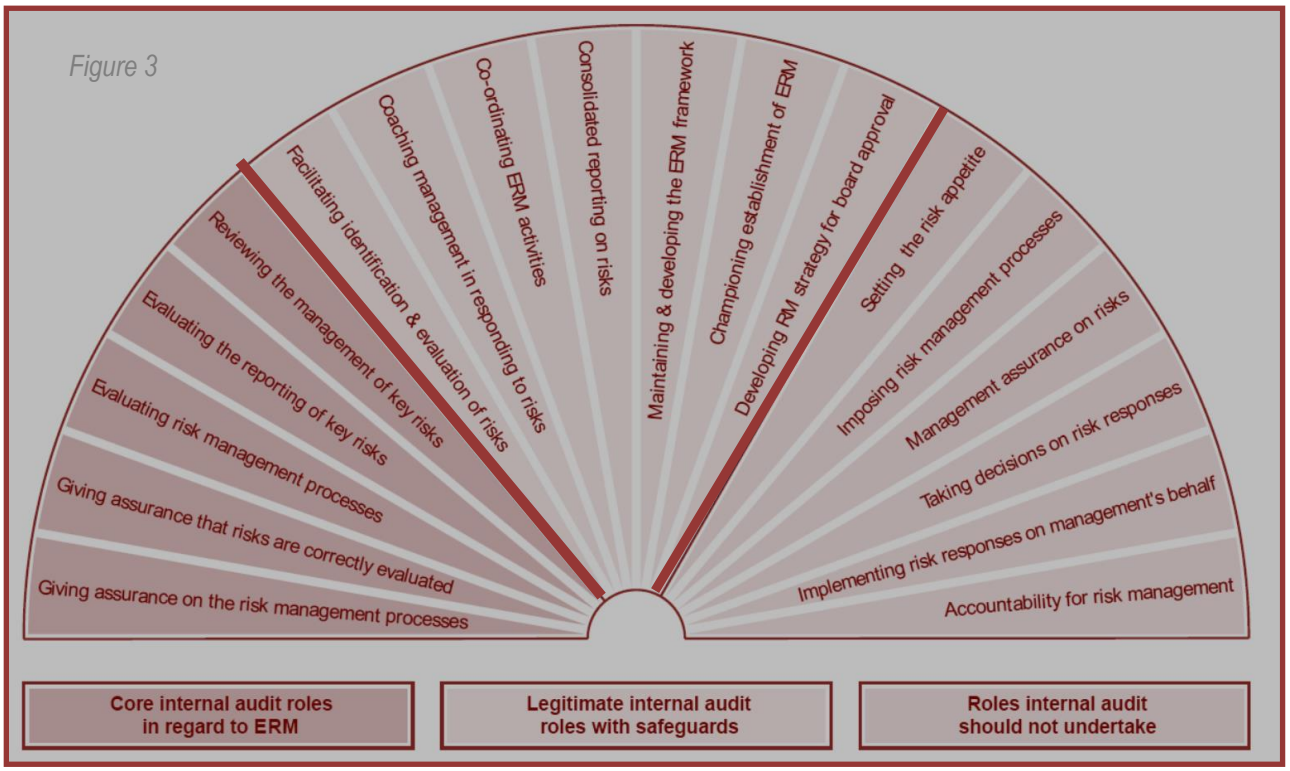
Today, the organization continues to have a solid ERM program that is supported by the Board, Executive Management and the rest of the organization.

In 2009, The Institute of Internal Audit (IIA) identified 18 different ERM activities and indicated whether or not Internal Audit should perform those activities (see Figure 35). Of these 18 activities, the IIA indicated:

- Five of the activities are core Internal Audit roles that relate to the Internal Audit's independent assurance function,
- Seven activities can be performed by Internal Audit with safeguards, and
- Six are off-limits to Internal Audit.

[5] IIA Position Paper: The Role of Internal Auditing in Enterprise Risk Management, Issued January 2009

As a result of our extensive work with banks and credit unions implementing ERM programs, we agree with the IIA that the Internal Audit function should be responsible for the five "core internal audit roles." However, we believe that in banks and credit unions – in addition to the six "roles internal audit should not undertake" – the seven 'safeguard' activities should also not be undertaken by financial institutions' Internal Auditors. These (combined) 13 activities should be handled by a Risk Function and not Internal Audit, as we have observed that Internal Audit has a difficult time performing these roles in financial institutions.



Taking the seven 'Legitimate Internal Audit Roles with Safeguards' documented in Figure 3, the following details our rationale for why we believe Internal Audit should not perform these roles – and the benefits the organization gains by having a separate Risk Function perform these critical activities.

Role

Facilitating Identification and Evaluation of Risks (or Working with Business Lines to Identify Risks)

Rationale

Internal Audit reports directly to the Audit Committee which is required in order to support their independence when auditing other areas of the organization. This need for independence in an organization creates a perception among business line managers that Internal Audit is not on the same team as the line manager. Audit is perceived as looking for problems as they perform their assurance functions. No one wants to get 'written up' by Internal Audit and – given the importance placed on internal audit findings – there is fear and in some cases reverence placed on the role of Internal Audit; we are not advocating that this perception is appropriate, this is simply what we have observed.

The value of having a separate Risk Function work with the business lines to identify risk is that the Risk Function will be seen as being on the same team as the business lines, and will be able to work with the business lines without any fear of needing to be independent. This will allow management to foster more transparency between the business lines and management on the risks being faced, and the business lines will not fear being 'written up' for self-identifying a risk. This should also eliminate the perception that Risk is an Internal Audit function.

Role

Coaching Management in Responding to Risks

Rationale

In most (not all) financial institutions, the Internal Audit staff does not have the time or resources to adequately learn about a particular function they are auditing so they rely on the line managers to provide much of the education. While Audit uses their skills in understanding risks and controls to critically evaluate the department/area being reviewed, they do not always have the level of expertise necessary to coach management on how to respond to risks – especially if they are responsible for identifying the risk.

When Internal Audit identifies a risk (in an audit engagement) and brings it to the attention of management, this indicates the risk was significant to Internal Audit and they feel it needs to be responded to. We believe Internal Audit should retain their independence and continue to bring the issues to management's attention and make recommendations on how to correct the issue, but management and the Risk Function should respond to the finding and determine if they are willing to accept the risk.

For risk issues not identified by Internal Audit, Internal Audit should be asked their opinion (i.e., in a consultative role) where necessary but it is ultimately management's decision on how to respond.

Role

Consolidated Reporting on Risk

Rationale

Internal Audit is primarily focused on transactions that have occurred in the past (i.e., as of a specific date) and identifying risks the financial institution may encounter based on those transactions. They provide management with audit reports that identify what they perceive the risks to be with a recommended action plan to resolve. The ability for Internal Audit to put on a different hat, to consolidate the risks management believes are important, and disregard those risk items identified by Audit that management has accepted, does not comfortably fit in the role of a bank Internal Auditor. The risk function (or CRO) is part of the management team and should fulfill this role by using the Consolidated Risk Report as a means to discuss with management and the board the risks the organization is facing and the action taken to manage the risks.

Role

Championing Establishment of ERM
Maintaining and Developing the ERM Framework
Developing ERM Strategy for Board Approval

Rationale

As mentioned previously, the role of Internal Audit in financial institutions is primarily an independent assurance function – to give management and the board a level of confidence that the organization's internal control environment and financial statements are appropriate. Having Internal Audit establish, maintain and develop the ERM Framework and ERM strategy is in conflict with the primary role of Internal Audit in banks.

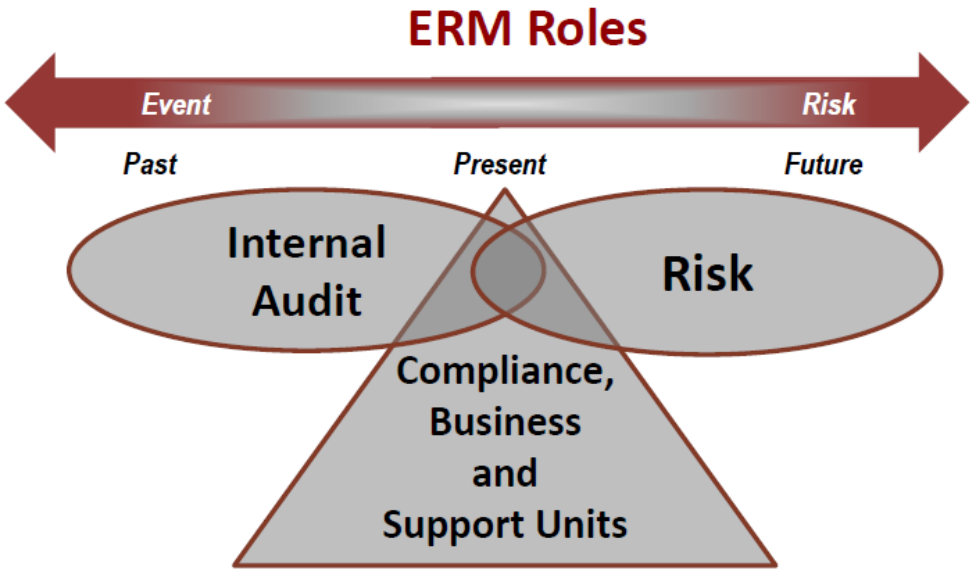
As has been noted, Internal Audit and Risk share many of the same responsibilities, however, as was also noted, the Internal Audit and Risk functions should not be combined. The value of the risk function will be significantly diminished if it is perceived within the organization as another audit function.

Defining Roles and Responsibilities

As is shown in Figure 4, managing risk is a future focused activity. We tend to think of managing risks as managing potential unexpected events that could cause a negative outcome to the organization. Managing risks can also lead to unexpected positive events – this is why we as financial institutions take risks – we are hoping for a positive event (e.g., increased earnings). Once a risk occurs, it becomes an event that we need to react to - it is no longer a risk. We will always have unexpected events – both positive and negative, the goal of Enterprise Risk Management is to manage risks within our risk tolerance so we can limit the number of unexpected events and also work on ways to be more nimble when reacting to these events.

This can only be accomplished by clearly defining the roles of the individual players in an organization and eliminating the ambiguity that can occur. The roles of Internal Audit, risk, compliance, the business and support units, management, and the board should be clearly defined and communicated. Without this formal definition and communication, employees and management create their own assumptions – right or wrong – about roles and responsibilities which can leave the organization vulnerable. The following are key (not all) responsibilities for these functions.

Figure 4



Internal Audit

- Verify the integrity of financial reporting and the effectiveness of internal controls through audits and other means (e.g., SOX or FDICIA work).
- Identify risk exposures the organization is currently involved in through audits and the Risk Assessment process.
- Give credit in the audit report, where appropriate, when a risk is self-identified.
- Perform an independent assessment of an audit finding and, using their professional judgment, report on it if they determine it to be reportable. They should not be influenced by the organization's risk appetite.
- Communicate newly identified risk areas to the lines of business and Risk.
- Perform an independent risk assessment of the organization and review with Risk to discuss discrepancies.
- Perform in a consultative role where necessary.

Risk

- Work with management, compliance, and the business and support units to develop the risk exposure for the organization – which includes risks the organization is currently involved and may be involved, both internal and external to the organization. Compare this to Internal Audit's independent Risk Assessment and discuss discrepancies.
- Work with management, compliance, and the business and support units on an on-going basis to identify new risks and monitor existing risk exposures.
- Work with Internal Audit on understanding the risk exposures they have identified and determine if the risks are within the organization's risk appetite. Where necessary, work with business lines to respond to Audit Findings.
- Communicate summary risk exposure to the board.

Compliance

- Work with the business and support units to implement programs, policies and procedures to comply with legal, regulatory, and ethical requirements. Monitor compliance with these programs, policies and procedures.
- Work with Internal Audit and Risk on risk identification and management of risk exposures in the organization. This should include the documentation of the risks, why they are risks, the actions or controls that are in place to manage the risks, and whether or not the risk is currently being managed within the organization's risk tolerance (i.e., the SMARTER approach to risk management).
- Identify key risk and performance indicators to assist in monitoring and managing risk.

Support Unit

- Work with the business units and compliance to implement programs, policies and procedures to comply with legal, regulatory and ethical requirements. Monitor compliance with high risk programs, policies and procedures.
- Work with Risk on risk identification and management of risk exposures in the organization. This should include the documentation of the risks, why they are risks, the actions or controls that are in place to manage the risks, and whether or not the risk is currently being managed within the organization's risk tolerance (i.e., the SMARTER approach to risk management).
- Identify key risk and performance indicators to assist in monitoring and managing risk.

Business Unit

- Work with Risk on risk identification and management of risk exposures in the organization. This should include the documentation of the risks, why they are risks, the actions or controls that are in place to manage the risks, and whether or not the risk is currently being managed within the organization's risk tolerance (i.e., the SMARTER approach to risk management).
- Work with compliance and the support units to implement programs, policies and procedures to comply with legal, regulatory, and ethical requirements. Monitor compliance with high risk programs, policies and procedures.

- Work with Risk, as necessary, to determine if an audit finding is or is not within the organization's risk tolerance. If the risk is within the organization's risk tolerance and the business unit does not feel remediation is necessary, the business unit, with management's support, has the authority to indicate as such in their response to the audit finding. If the risk needs remediation, management should support the plan to remediate.
- Identify key risk and performance indicators to assist in monitoring and managing risk

Management and the Board

- Develop and foster the organizations corporate governance and strategic direction.
- Determine the organization's risk appetite and risk tolerance and manage to that.
- Conclude on audit findings. An audit finding should not remain on an 'open audit findings log' for a long period of time. A finding is either a risk that needs remediation or management is accepting the risk.
- Work with Risk on risk identification and management of risk exposures in the organization. This should include the documentation of the risks, why they are risks, the actions or controls that are in place to manage the risks, and whether or not the risk is currently being managed within the organization's risk tolerance (i.e., the SMARTER approach to risk management).
- Identify key strategic risk and performance indicators to assist in monitoring and managing risk.

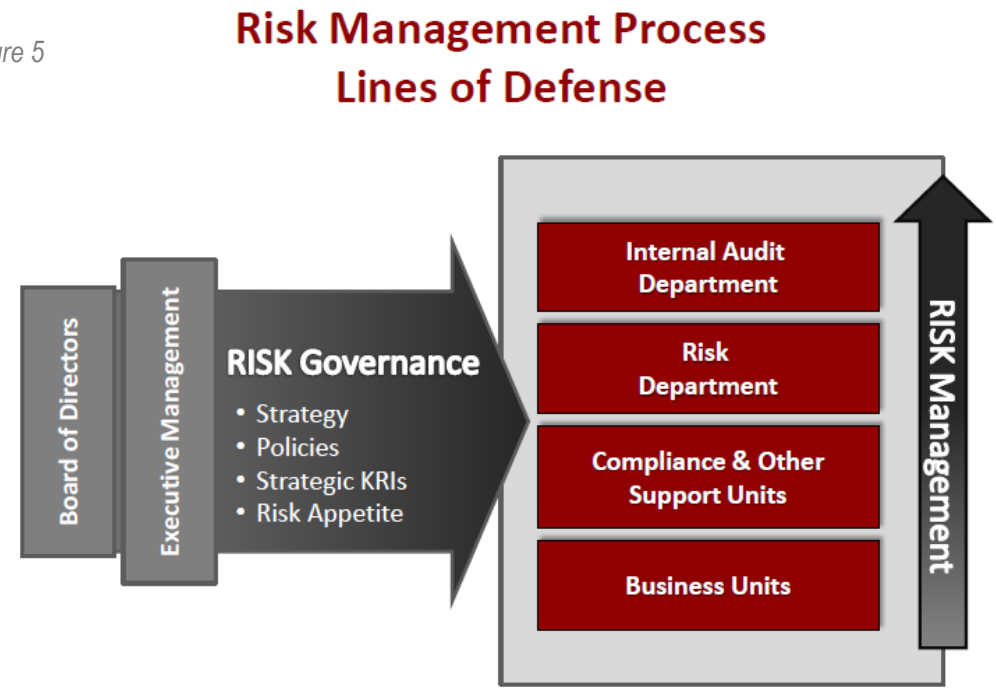
Enterprise Risk Management Committee

- Provide a cohesive umbrella for all of the risk management programs currently in place. The committee does not replace any existing risk and compliance program oversight committees that are responsible for ensuring adequate risk measurement, mitigation and management in their respective areas of authority.
- Ensure that key risks for the bank have been appropriately identified and are being appropriately managed.
- Discuss and assess key changes in the organization's business and markets to determine the impact and the actions required to manage the associated risks.
- Provide ongoing guidance and support to Risk and the risk owners.
- Provide updates to the Board on ERM activities, conclusions and recommendations.

Working in Harmony

With this process in place, there is a 'line of defense' that should assist in identifying, understanding, managing and monitoring risk in the organization. Figure 5 shows the lines of defense financial institutions will have to manage risks in the organization.

Figure 5



The primary responsibility of risk management lies with the business unit that is performing the risk activity. The second line of defense is with compliance and other support units that review, oversee and support the business lines. The third line of defense is the Risk Department and the final line of defense is the Internal Audit Department.

Each area in the organization has a responsibility to communicate risks they see and needs to feel comfortable communicating those risks. The business units, compliance and support units are actively involved in the activities occurring in their areas, and are closest to understanding what risks are increasing or decreasing, and need to communicate those risks. The Risk Department isn't as close to the risk activities but understands risk and needs to work with the business and support units and ask probing questions to uncover risks that may have been overlooked. Internal Audit (as the assurance

function) independently identifies the risks in an individual area and audits to ensure the control environment is in place to manage those risks. If they identify a risk that the three previous areas didn't identify, the question everyone should ask is 'why?'.

In order for this process to work effectively, there are a number of realities that must be understood. These are heavily influenced by an organization's culture and need to be dealt with in order to have a successful risk framework.

1) Everyone in the organization must be given the responsibility and authority to communicate risks without the threat of condemnation.
2) Risks need to be owned by one individual who understands and can monitor the risk. This does not mean they need to do all of the work to manage the risk but they need to be ultimately responsible for the risk. Typically, this is someone in the business line.
3) Internal Audit is not a control. They are performing their work as an independent function for management and the board – not for the business unit. Business units should not rely on Internal Audit to verify all risks have been identified and are controlled.
4) An ERM program is not meant to replace any existing risk management activities or the documentation in place to support those activities.

ERM and the Regulators

The implementation of an ERM program will increase the understanding of risks throughout the organization and will create greater transparency on the decisions being made in the organization to accept or manage risks. The documentation of these efforts should assist financial institutions in their discussions with regulators on the organization's approach to identifying and managing risks. As regulators identify risks – which is where you start playing offense instead of defense (see Figure 3) – there can be open, constructive discussions on your decision processes relating to the risk identified and why or why not you feel their finding is a risk given the organization's risk appetite. And, providing you identified the risk through your ERM program, you can provide any documentation on your decision-making.

Summary

Enterprise Risk Management is a change in the way organizations approach risk. For many banks and credit unions, the change should not be overwhelming, intimidating or confusing, but an opportunity to create ownership and an understanding of risks across the organization. A formal ERM program should be created with the view that it will add value to the organization.

People perform their jobs better when they have a clear understanding of their role and responsibilities. We have found this to be true throughout our many engagements and also from our experience as bankers. Clarifying the roles and responsibilities of the specific parties involved in risk management is crucial to creating a successful program. The inclination for financial institutions to use the Internal Audit role to manage the ERM process is a disservice to the entire organization and does not provide the on-going value that could be garnered out of an integrated ERM program – the ability to proactively identify and manage risks across the organization.