

# Steady, Steady

Use these three steps to lay the foundation for effective enterprise risk management.

By Alan White

**M**ost credit unions that have been successful implementing an enterprise risk management program have broken the initiative into smaller tasks or phases. This helps to define clear milestones, set timelines, and track progress. This also helps to keep the momentum of the project and thus the commitment of senior management and the board.

Many successful CUs will often break the tasks down further. It is often easiest to concentrate efforts on one area of the business first (such as accounting or IT), and then deploy the program to the CU as a whole.

This helps to train the team, identify any methodology changes before rolling the program out to the entire organization, and create a success story in a lower risk project. In other words, it allows a CU to make small mistakes instead of big mistakes.

A successful ERM methodology includes three primary phases, each with associated subtasks and activities. These are setting the foundation; documenting, analyzing and remediating processes and controls; and monitoring and auditing the performance of controls. This process is shown in the diagram, p. 39.

This article will focus on the more analytical tasks in the program.

## Phase 1: Set the Foundation.

This phase is the most critical. Decisions here will affect all other phases and activities. This is also the phase unsuccessful organizations often overlook or skip completely, much to their peril later on. Urton Anderson, accounting department chair at the University

of Texas at Austin and chairman of the Professional Standards Board of the Institute of Internal Auditors, confirmed this concept:

“Organizations need to get beyond the reactive and ‘check the box’ risk management programs that are all too prevalent today. Before completing audit checklists or blindly testing controls, companies need to understand how their organizations work, who does what, how often, and why. In an environment where changes or acquisitions occur, this understanding is even more important. Armed with this information, risk managers can focus on applying good judgment, project management, and implementing sound business practices.”

Accordingly, this phase entails developing a solid understanding of the requirements of the program; establishing organizational objectives and risk appetite; inventorying all relevant compliance requirements, control objectives, and organizational policies; and conducting a preliminary risk assessment or prioritization exercise.

### *Establishing objectives and risk appetite.*

When starting an ERM program, it is critical to ensure the establishment, and proper understanding, of the CU’s business and strategic objectives, which are influenced and approved by both the executives and board. To effectively manage risks throughout the enterprise, it is critical to review specific impacts to achieving these objectives. Whether they are short-term or long-term objectives, they are important to the success of the business and need to be regularly monitored and managed.

All organizations are unique in what type of and how much risk they are willing to accept. At a management level, each CU needs to work to establish this threshold, often referred

## PHASE 1: Set the Foundation

### ACTIVITIES:

- Initial planning and analysis
- Define the organization
- Determine and assess risk indicators
- Enterprise-wide risk assessment



## PHASE 2: Document, Analyze, and Remediate Processes and Controls

### ACTIVITIES:

- Build basic process documentation
- Identify risk events
- Identify controls that mitigate process risks
- Identify process and control deficiencies
- Remediate deficiencies and update documentation



## PHASE 3: Monitor, Audit, and Assure

### ACTIVITIES:

- Identify key controls subject to monitoring
- Identify and assign monitoring resources
- Train resources to perform and monitor controls
- Develop test plans and execute tests
- Document and report results

to as the “risk appetite” or “risk tolerance.” By understanding the risk appetite, the CU is in a position to make informed decisions on when and how to address specific risk events and activities throughout its operating environment. CUs will also do well to clearly understand the difference between “rewarded risk”—such as more aggressive product development—and “unrewarded risk”—such as regulatory compliance or transaction risk.

**Inventorying compliance requirements, control objectives and organizational policies.** One of the key activities in this phase is collecting all the specific requirements under which the CU needs to operate. These requirements may come in the form of specific regulatory requirements put out by the National Credit Union Administration, or internal CU policies.

When identifying and gathering this information, it is important to develop a method for storing and accessing it. A centralized repository will help save both time and money. Having the ability to integrate these requirements with your credit union’s risk profile and your internal controls data will serve as an added benefit and will help ensure that requirements and objectives are followed.

**Doing a preliminary risk assessment.** The goal of this exercise is to identify the riskiest parts of the organization so the work can be prioritized for the rest of the program. It is critical to delineate between risk assessment and risk management. Risk assessment is about understanding objectives and identifying and ranking the threats to them. In contrast, risk management requires knowing how you are addressing your risks and ensuring these actions are performed.

A preliminary risk assessment can be performed in a variety of ways. The most common approach is management surveys and interviews. Using a set of standard questions about areas of risk in the organization will allow key management personnel to independently voice their areas of concern and, at the same time, provide a consolidated view across the full management team. Analyzing the results of the survey and/or interview process will put the CU in a position to prioritize key risk areas throughout the

organization and will serve as a priority list for upcoming program phases.

## Phase 2: Document, Analyze and Remediate Processes and Controls.

This phase is about identifying risk events, determining the appropriate risk response, analyzing residual risk, and identifying any unmanaged risks not within your risk tolerance. *This is the time key decisions are made about how risks will be managed.*

Many organizations have already documented processes for audit or compliance reasons. If so, that documentation can be used as a starting place for identifying risks. However, the documentation for ERM does not need to be so detailed as documentation for an audit. The goal is to focus on risks. In many cases, process improvement opportunities can also be identified as credit unions identify duplicative or unnecessary controls.

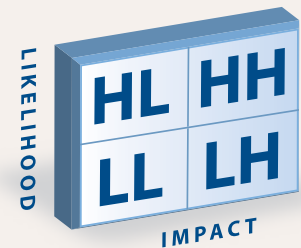
**Identifying risks.** The COSO framework ([www.coso.org](http://www.coso.org)) makes an important distinction between “inherent risk” and “residual risk.” Inherent risk refers to risk that exists simply by being involved in a certain activity or business, in a certain place, at a certain time. It is often defined as the “risk of doing business” and is driven by such things as the product mix, the membership base, and the geographical profile of the organization.

All organizations will have some high inherent risks. For example, most credit unions handle cash and there is a risk that someone will steal it. This risk is inherent to the CU business. Many CUs mitigate this risk to near zero through control measures that include locked drawers, safes, teller training, security cameras and alarm systems. The remaining risk is often insured or transferred so this risk is rarely unmanaged—but it still exists. “Residual risk” refers to the risk that remains after risk mitigation or control measures have been put in place.

Many risk and control frameworks do not include this concept. This idea is an important part of the COSO framework because it points out the most important control measures that must be monitored later.

Identified risks should be rated for likelihood and impact. Simple rankings are best because

they are usually the easiest to implement and track. High vs. low or high/medium/low are almost always sufficient to determine risk responses, which is usually the objective. Some rating combinations are included below:



- **High risk**—(HH) High impact and high likelihood of inherent risk. Resources should be allocated to mitigate or transfer these risks.
- **Medium risk**—(HL) or “death by a thousand cuts,” and (LH) or “tsunami event” type risks are medium risks that require management judgment to either transfer, accept or mitigate.
- **Low Risk**—(LL) Low inherent risk issues are typically accepted by the risk owners and do not justify allocation of valuable resources to manage.

For reporting purposes, it is usually helpful to plot these risks on a map like the one above.

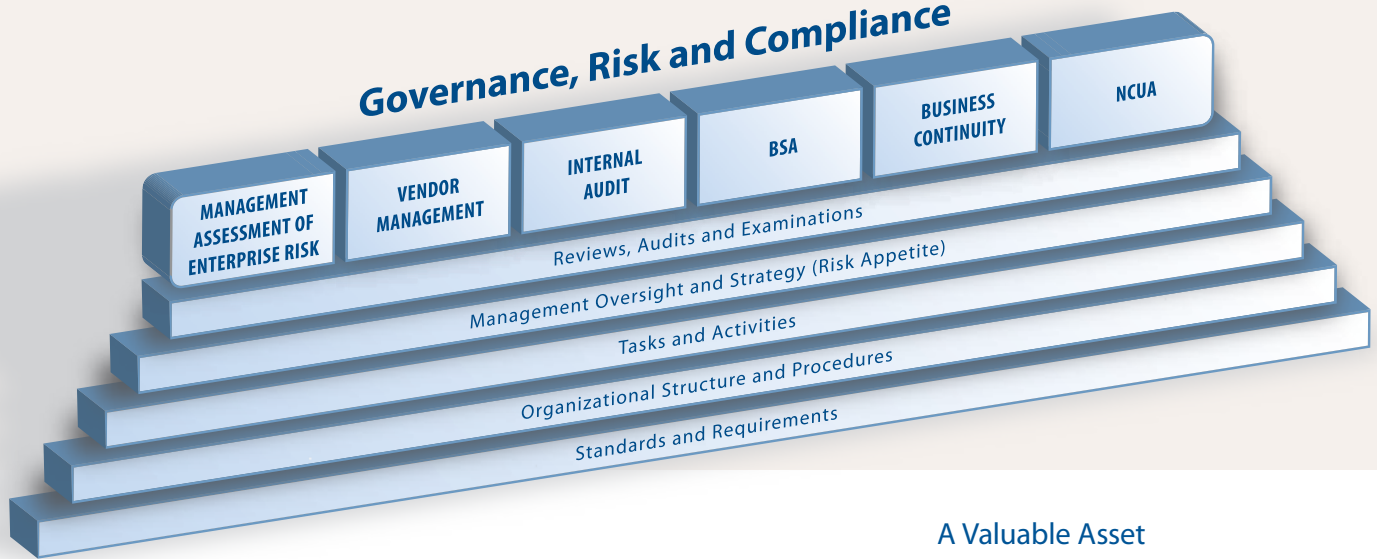
This gives management, the board, and the supervisory committee a good sense of the risks they face. In addition, analyzing the distribution helps to determine if process owners are over- or under-rating risks (if nearly all risks are rated as HH, the organization is probably over-rating risks). These maps should be created at various levels in the organization to provide insight into different departments and business units, as well as to the CU as a whole.

**Responding to risks.** Once risks have been identified and analyzed, the appropriate response can be determined. Options include transfer (usually through insurance), accept or mitigate. The organization should have clear standards for when risks can be accepted. Apathy is not an acceptable reason to accept a risk; rather it must be within the credit union’s risk tolerance as determined in phase one, setting the ERM foundation.

Review and confirm process



# Governance, Risk and Compliance



documentation; identify and analyze control measures; and find and document any process design deficiencies (those where unacceptable unmanaged risks are identified). High residual risks will usually require some finding or deficiency to be reported. In general, it should be very rare that high residual risks are accepted and should require approval of at least senior management, if not the board and/or supervisory committee.

### Phase 3: Monitor, Audit and Assure.

ERM programs are only as good as the controls in place to manage the identified risks. Those controls must be performed consistently and predictably. In many cases, CU employees will need to change how they do their jobs, including conducting more reviews and approvals, documenting work, and retaining evidence that can be used by auditors and examiners later on.

COSO has addressed this issue in its newly released “COSO Guidance on Monitoring Internal Control Systems” (<http://tinyurl.com/cosoguidance>). This provides an overview of effective monitoring programs, implementation techniques, and guidance for smaller organizations where several levels of control are not the norm.

Credit unions should implement three types of monitoring controls:

- **Supervisory controls**—Typically performed by line managers or department heads, these include reviews and examinations of controls performed by individual employees. A daily or weekly review of the loans issued by a loan officer is one example. These controls provide almost immediate feedback and corrective action, but are not sufficient to provide assurance that organizational objectives are being met because those performing the reviews may not have a thorough understanding of those objectives.

- **Oversight controls**—Executives and senior

managers should monitor controls as well, but these activities are typically done less frequently and at a more macro level than supervisory controls. Budget-to-actual analysis or reviews of member satisfaction surveys serve as examples of oversight controls.

- **Internal auditing controls**—These are traditional internal audits done in accordance with auditing standards. Such internal controls provide the best level of assurance, as they include detailed reviews, investigation of unusual items, and identification and analysis of findings. However, internal audits are often performed well after a control problem has occurred and do not provide sufficient timeliness to be effective as a primary control monitoring method.

Credit unions that build effective monitoring systems can use “early warning signs” to identify and correct control issues before they are found in an audit or examination. These systems also help to establish accountability and measurement for the ERM program, which can enhance culture and commitment. Finally, organizations that effectively monitor controls as they are performed enjoy decreased disruption during audits and regulatory examinations.

Internal auditors specialize in testing controls. Reviewing policies, examining evidence, evaluating exceptions, and identifying deficiencies and weaknesses should come very naturally to any internal auditor, and organizations should make use of these skills during this phase.

However, as with the “document processes and controls” phase, the scope of these activities is likely to be significantly larger than the audit department is accustomed to. Often times, their resources will need to be supplemented with consultants or through peer reviews by process owners. In addition, auditors involved in these programs must enhance their skills with project management, quality assurance, and training capabilities to maximize their chances of success.

### A Valuable Asset

Credit unions that complete these phases will have built a valuable asset. The ERM program provides enormous value by helping management understand and mitigate risks and by helping boards and members obtain assurance that risks are appropriately addressed.

But perhaps more importantly, CUs that complete this process will have built the foundation for effective governance, risk and compliance. By leveraging the information they have built, these credit unions will be more able to adapt to new regulations or implement new risk and compliance-related initiatives much more easily.

The GRC platform above demonstrates the usefulness of data collected through the phases. Once the foundation of policy, process, risk and control data is identified and documented for the credit union, responding to new initiatives and requirements becomes a streamlined effort. At the end of the day, regardless of what regulation or requirement you are looking to address, the same business data is being used, just reported on a bit differently. 🔄

Allan White is president/CEO of Vital Insight, CUES’ partner in CUES Enterprise Risk Management, Powered by Vital Insight ([cues.org/erm](http://cues.org/erm)).

### Resources

Learn more about CUES Enterprise Risk Management Powered by Vital Insight at [cues.org/erm](http://cues.org/erm).

Sign up for the CUES School of Risk Management, slated for May in Boston and for September in Chicago, and for CUES Advanced School of Risk Management, also in Chicago in September. Save 20 percent on both. Visit [cues.org/schoolofriskmanagement](http://cues.org/schoolofriskmanagement).