Crowe Horwath

Risk Assessment:

The Critical First Step to an Effective IT Audit Plan

A White Paper by Raj Chaudhary and Steven C. Hunt

In today's economic and regulatory environment, boards, audit committees, and executives must understand the logic, value proposition, and cost behind their companies' IT audit plans. An IT risk assessment is a crucial first step to creating a methodical risk management process that quantifies the likelihood of technology-, process-, and people-related threats that could hinder the organization from attaining its objectives in an efficient, effective, and controlled manner.

Virtually all organizations of any significant size – especially publicly held companies or those in regulated industries – generally are required to conduct annual risk assessments and information technology (IT) audits to identify and confront risks from a variety of sources, both internal and external. As risks have become more apparent and regulatory requirements more complex, boards and audit committees are demanding a better understanding of the logic – and the cost – behind the IT audit plan.

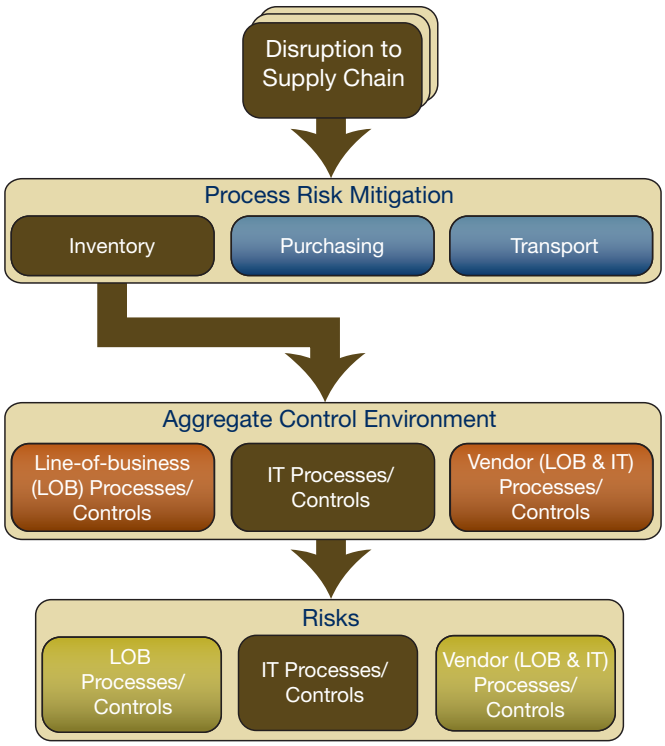
Purely subjective opinions, historical audit coverage, and gut feeling are no longer adequate for ensuring the timely recognition of potential risk exposures associated with technology. Questions arise about whether audit is looking in the right places for the right reasons, and how the audit plan meshes with the organization's overall strategic, regulatory, and governance objectives. As technology becomes more comprehensive and sophisticated, boards place greater emphasis on the internal audit group's ability to plan and act strategically, be nimble, address changes in the risk environment, and present risk-based audit plans that demonstrate an understanding of tactical architecture and controls that tie into the enterprise risk management (ERM) model.

A growing number of organizations are executing objective risk assessments, which then drive the audit coverage, scope, and frequency. This process often involves multiple assessments conducted by internal auditors and owners of different processes throughout the organization:

- At the board or audit committee level, an ERM process is performed to identify key enterprise risks (for example, as in Exhibit 1, disruption to the supply chain) and to define the organization's overall appetite for risk.
- The organization's process owners and chief audit executive perform assessments to evaluate the risks associated with the processes that support the identified enterprise risks (inventory, purchasing, and transport, for example). Often fairly subjective, these assessments are performed using risk models, professional knowledge, and, more often than not, guidance provided by skilled professionals.

The internal audit teams facilitate a risk assessment of the aggregate control environment. The result is a detailed, objective evaluation of the risks associated with the process as well as with IT and third-party vendor functions that support the specific organization processes.

Exhibit 1: The ERM Process



The IT risk assessment process begins with understanding the linkage to the key risks of the organization and ends with the development of a logical and quantifiable assessment of critical factors related to risk. Thus the process not only helps to ensure that the IT audit plan concentrates on high-risk IT components, processes, and locations; it also helps to reduce ineffective audit plans that could lead to misallocation of limited audit resources, misdiagnosed systemic risks, or failure to identify foreseeable organizational effects.

An equally critical advantage of this process is that it leads to an objective IT audit plan that is scalable, flexible, and linked to the organization's overall governance and ERM models.

Growing IT Audit Demands

Since emerging in the late 1960s, the practice of IT auditing has grown explosively as technology's role in every type of organization has become pervasive. Organizations' steadily growing reliance on computer-based systems and applications has led to the exponential growth of IT risks and associated IT audits of increasing complexity.

While the financial services industry has been subject to extensive audit requirements for decades, it is joined these days by insurance, healthcare, government agencies, manufacturing, and others – indeed, virtually every industry. Today federally regulated organizations require annual risk assessments to comply with a host of requirements, including the *Gramm-Leach-Bliley Act* (GLBA) and those of the Federal Financial Institutions Examination Council for financial organizations; the *Health Insurance Portability and Accountability Act* (HIPAA) for healthcare; the Annual Financial Reporting Model Regulation (commonly known as Model Audit Rule or MAR) for insurance companies with $500 million or more in written premiums; as well as the *Sarbanes-Oxley Act* (SOX) and other acts that touch virtually all types of organizations.

In addition to regulatory agencies, guidance-setting bodies such as the Institute of Internal Auditors (IIA), the Information Systems Audit and Control Association (ISACA), the National Institute of Standards and Technology (NIST), and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) have each published standards related to IT audit requirements and best practices. The IIA's International Professional Practices Framework perhaps is the most direct, as noted within the following standards:[1]

- Standard 2010 – "The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals."
- Standard 2010.A1 – "The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process."
- Standard 2110.A2 – "The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives."

[1] The Institute of Internal Auditors, www.theiia.org.

Faced with audit standards, so much guidance, and so many critical issues, how can internal auditors determine what to audit, and how often, while also managing their limited audit resources effectively? More critically, how can executive management and board members – given their potential personal liability in the event risk is not properly assessed and mitigated – verify that the IT audit function is performing adequately and in compliance with audit standards while also being consistent with the organization's ERM strategy?

Greater Complexity, Limited Resources

In many ways, widespread recognition of the critical role of IT audit, coupled with the wide variety of organizations providing guidance, can complicate the process of planning and executing an effective audit. Regulatory and guidance-setting bodies have often expounded on the "why" but have been less definitive on the "what" and "how" of conducting objective and quantifiable IT risk assessments.

Too often internal auditors feel ill-equipped to meet their boards' expectations as they wrestle with too many areas to audit and too few resources. The audit – and thus the audit plan – does not exist in isolation. Rather, it must ultimately function as part of the overall enterprise and must support and integrate with the organization's strategic issues.

Therefore the process must overcome several challenges, including:

- **Language.** Not only do organizational units and the IT group often communicate poorly with each other, but technicians and IT auditors often interpret terms differently among themselves as well. The absence of uniform definitions of terms and assessment criteria leads to confusion – and wasted effort – as the various parties must take time to reach agreement on basic terms such as "likelihood" versus "impact" and "inherent risk" versus "residual risk."
- **Relevance.** Underlying the language and miscommunication issues, there might also be a fundamental difference in belief about what should be audited. All too often, many valuable audit hours are spent on issues that IT auditors find professionally interesting but have little or no relevance to the success or failure of the organization – and thus are of little concern or interest to the board members overseeing the audit.
- **Ability to be defended.** Too frequently, the audit assessment processes are not repeatable, quantifiable, or objective-based – thus greatly reducing the audit group's ability to defend the scope, frequency, and ultimately the relevance of observations.
- **Cost.** Even in a moderately complex organization, the cost of software and implementation for assessing, planning, and executing an IT audit can quickly reach a quarter-million dollars or more. In today's economy, audit committees and boards give careful scrutiny to audit budgets and are increasingly likely to question both the audit plan and the tools requested to carry it out. Regardless of cost, audit committees and boards still expect the audit plan to address all high-risk IT segments of the organization.

Developing a Focused IT Audit Plan

A comprehensive IT risk assessment can address the challenges noted in the preceding paragraphs (language, relevance, ability to be defended, and cost) by producing the critical information needed to formulate an effective and efficient IT audit plan. The ultimate goal of the assessment is to enable a company to build a multiyear internal IT audit plan that is focused on organizational risk, objective, scalable, flexible, and defendable. The IT risk assessment also:

- Identifies high-risk IT components, processes, and locations that support key organizational processes;
- Coordinates with larger global strategic enterprise projects, such as IT governance and ERM;
- Helps the organization comply with regulatory requirements as well as applicable standards, such as those issued by the IIA, ISACA, NIST, COSO, and other bodies; and
- Provides identification and support for potential strategic and tactical follow-on projects, such as disaster recovery and business continuity, privacy, change management, and network penetration and vulnerability assessments.

Although many audit-planning software products provide useful tools and insight into trends, patterns, and long-term challenges, often the IT risk assessment can be performed using only basic spreadsheet software. It is imperative to recognize that the true added value is not necessarily derived from the technology or tool that creates the audit plan but rather from the journey itself – that is, the risk factors, criteria, understanding, and analysis.

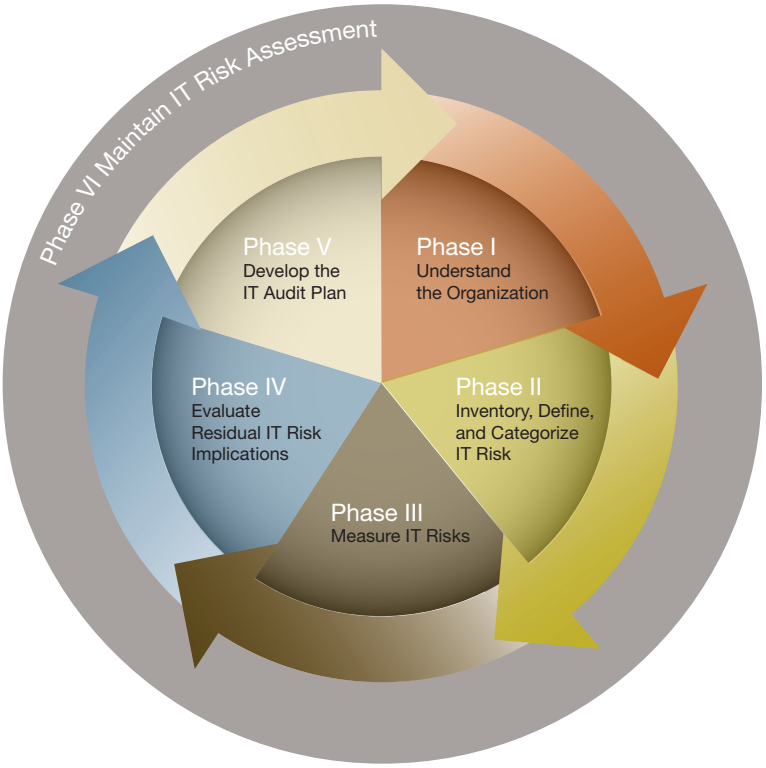
A Six-Phase IT Risk Assessment Framework

The six-phase process that follows provides the framework for performing an IT risk assessment. The actual breadth and depth of the execution of each phase will vary depending on the specific industry, the complexity of the IT environment of the organization, and the overall objective of the assessment (see Exhibit 2).

Phase I: Understand the Organization

The first phase of the IT risk assessment involves gaining an understanding of the organization's objectives and its related appetite for and tolerance of risk. This understanding must not only be specific to assessment of risks but also provide a broader perspective of the organization's approach toward risk management. This phase begins with developing an understanding of the organization's environment

Exhibit 2: Phases of the IT Risk Assessment Framework



and concludes with identifying the relevant organizational processes and related technology. More specifically, the risk assessment team needs to develop a clear understanding of:

- The objectives of the organization;
- The risk appetite and tolerance of the organization; and
- The processes, including IT application and supporting infrastructure, of the organization.

Before team members can gain a solid understanding of an organization's objectives, the team must identify all of the stakeholders within the scope of the IT risk assessment. Interviewing the key IT risk assessment stakeholders will yield much of the information necessary for compiling the risk assessment.

Once organizational objectives are understood, the risk assessment team should take time to understand risk appetite (that is, the broad-based amount of risk an organization is willing to accept) as well as risk tolerance (the acceptable amount of variation between risk appetite and actual results). Risk appetite and tolerance must be understood and documented at the entity level and at the level of the processes relevant to the IT risk assessment. It is also important to note that neither risk appetite nor risk tolerance should be defined by IT or the IT audit function. Rather, they must be defined by those who are responsible for running the organization – the board of directors, the audit committee, and senior management.

The IT risk assessment team then works with the process owners and the IT function to map the organizational objectives to processes as well as to the IT applications and supporting infrastructure, thus creating the critical foundation that will guide the remaining phases of the IT risk assessment process (see Exhibit 3).

This mapping is captured in a relational matrix that links the IT components to the organizational processes. This process inventory is used to create the universe of auditable areas.

The relational matrix identifies components of the organization such as:

- **Key organizational processes supporting ERM.** Help to link the audit plan to the overall ERM process.
- **Regulatory effects in each area.** Help to identify technology that may affect regulatory assessments.
- **Recovery times in the event of catastrophic failure.** Help to identify the organizational significance of the various processes.
- **IT infrastructure.** Includes applications, databases, platforms, networks, and physical infrastructure.
- **IT processes.** Include change management, security administration, and the help desk.
- **Key vendors that support the organization.** Include outsourced data centers and organizational processes such as payroll and check processing.

With a skilled IT risk assessment team leading a collaborative effort, the mapping process within a moderately complex environment can be accomplished in a matter of days. In addition to supporting the risk assessment process, this mapping provides secondary value by helping to change activities and business continuity processes, which require similar correlation.

Phase II: Inventory, Define, and Categorize IT Risks

The overall objective of Phase II is to establish the relevant risk universe – that is, risks that are included within, or are relevant to, the IT risk assessment. During this phase, the following are created:

- A risk universe; and
- Mapped risks within the universe to specific organizational processes and the supporting IT applications, infrastructure, and operations.

Creating the risk universe requires a definition of risk. Risk is defined as the possible occurrence of an event that could have a negative impact on the achievement of an objective or series of objectives. The types of risk within the IT environment of an organization must also be defined.

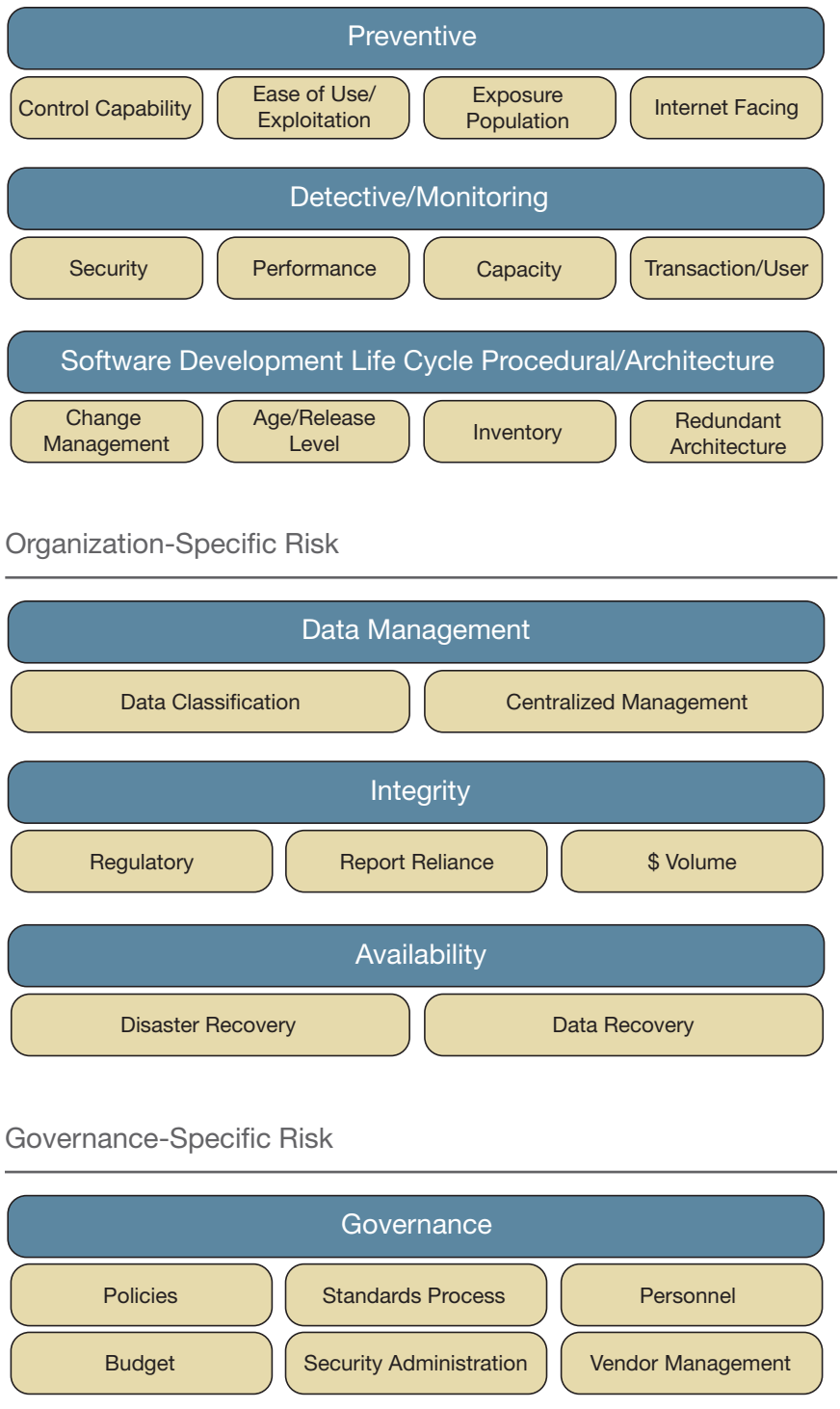
Risk Types. Risk types are specific criteria that are used to classify or categorize different kinds of risk. From an IT perspective, they are generally common across all types of technology, relevant, quantifiable, and, most important, measurable. Typically risk types fall into three general groups (see Exhibit 4):

1. Technology – system and application attributes that are preventive, detective, or change-related in nature;

Exhibit 3: Business Process-to-Technology Layer Mapping

Technology Layer	Affected Regulations			Application	Database	Platform	Mobility	Network Infrastructure	Process	Risk Mgmt.	Vendor Mgmt.
Business Process	HIPAA	GLBA	SOX	FMS	SQL	Windows®	Mobile Data	Firewall	Security Administration	Change Mgmt.	SAS-70
Insurance Underwriting	X		X		X	X	X		X	X	
Insurance Premium Calculation	X		X	X	X	X			X	X	
Insurance Premium Collection	X		X	X	X	X			X	X	
Payroll		X	X			X	X		X	X	X
Fixed Assets			X			X			X	X	
Connectivity/ Communication						X		X	X	X	
Annual Capitalization Deposit			X	X	X	X			X	X	
Benefit Management (401(k), 457)		X	X			X		X	X		X
Health Insurance Management	X					X			X	X	

Exhibit 4: Three Types of Risk



2. Organization – information-based attributes such as data management, integrity, and availability; and
3. Governance – attributes providing management guidance and oversight.

Criteria. The criteria for assessing each type of risk must be defined clearly and agreed upon to help ensure consistent evaluation. This component is typically the most critical for building consensus since it provides the assessment criteria for risk measurement (see Exhibit 5). It is also very important for the stakeholders to provide consistent answers if asked the following questions:

- What events could or would cause the risk to occur, and what is the likelihood of each?
- What is the potential impact to the organization if the risk were to occur?

Phase III: Measure IT Risks

In Phase III, the IT risk assessment team applies a scale (or measurement) to the risks that have been identified by this point in the assessment. Risk should be considered at its inherent state (that is, before controls are considered) and its residual state (after controls are considered). Consequently, management's strategies (or responses) must be considered and understood.

In Phase III, no attempt is made to assess whether a given risk or its measurement level is good or bad, advisable or not. Nor does the phase include making plans for the future. This phase yields a current view of inherent risk and a consideration of the strategies in place to manage those risks, and then results in a residual risk.

The following steps and activities are expected to be part of measuring the risks:

- **Determining the method for gathering information for the ratings.** Common examples include surveys, inquiries, interviews, workshops, and review of corporate information (likely received during Phase I).

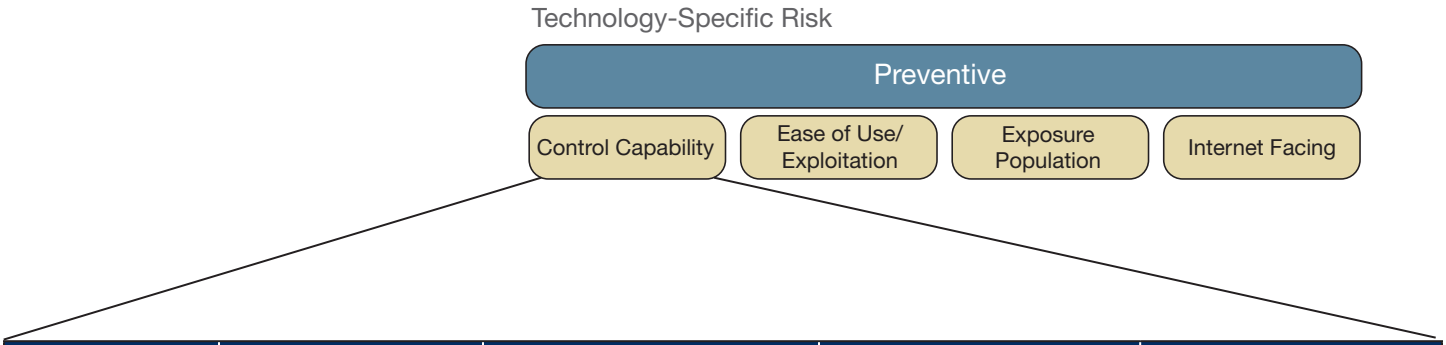
- **Measuring inherent risk.** Apply appropriate scoring to the risk that exists in the absence of internal controls. As mentioned earlier, understanding the scale as well as the criteria used for assessing risk will provide consistency in the measurement phase.
- **Evaluating risk response.** Management has made a decision about its response to a risk in the organization's risk universe. For risks that are reduced through the use of internal controls or risk transference, the level of mitigation (and the effectiveness of that risk management) must be considered. Perceived controls should be documented. Note that the validation of the design or operating effectiveness of these perceived controls are not in the scope of Phase III.

For shared risks, the practitioner should document the key third parties or service providers with whom the risk has been shared or to whom it has been transferred.

The IT risk assessment team should consider the level and form of documentation needed to support risk response and its perceived effectiveness. In addition, conditions might exist in which multiple response strategies have been employed. The IT risk assessment team must consider the full array of strategies when determining the response.

With the development of and agreement on IT risk types and assessment criteria, the collection and correlation process can be performed with surprising efficiency. In a moderately complex environment, a skilled IT risk assessment team can collect the necessary data in a matter of days. After stakeholders or owners are briefed on the criteria, the assessment of high, medium, and low risks becomes a straightforward process.

Exhibit 5: Risk-Driver Description and Criteria for Assessing Risk Ranking



Control Driver	Description	Value = 1 (Strong)	Value = 2 (Marginal)	Value = 3 (Weak)
Control Capabilites	What are the inherent control capabilities of this resource to manage logon, password management, and access?	System has inherent ability to manage strong passwords and access controls. Operating-system-level controls are integrated to support logon, password management (minimum length, complexity, change interval, guesses), and access to files and directory.	System has limited ability to manage strong passwords (for example, passwords are required but cannot force minimum length and complexity), but it can force size. Access can be limited. User initial logon is integrated with operating-system-level security but is less sophisticated.	Secondary passwords are used but do not rely on operating-system level (for example, not integrated with RACF/AD/AS400), no password syntax ability exists, and access is "all or none."

Phase IV: Evaluate Residual IT Risk Implications

The primary objective of Phase IV is to communicate residual IT risk to key stakeholders and to reconcile it to the organization's risk appetite and tolerance levels.

The first step in this phase is a detailed review of the organization's residual IT risk profile. The review's purpose is to articulate to management the risk that remains after the perceived level of control and other risk mitigation strategies have been considered. This review should be conducted with the appropriate organizational stakeholders, and their acceptance should be formally documented. The review also provides the opportunity to identify and incorporate some subjective input from stakeholders (such as senior managers and audit and compliance professionals) into the IT risk assessment calculation. Also at this point, senior management has an opportunity to override the initial risk rankings. Some subjectivity, using professional judgment, at this stage is acceptable – even advisable – if only to rule out a risk that might be causing unwarranted or unnecessary concern.

In any event, changes to the initial inherent risk ranking – either increasing or decreasing ratings – should be supported by written documentation from management that articulates the justification for overriding the initial risk ranking. After all, the initial risk ranking is the product of agreed-upon risk types, criteria, and organizational risk appetite and tolerance.

The next step in this phase is comparing residual risk to the organization's risk appetite and tolerance levels. The IT risk assessment team must identify and document where risks exceed risk appetite and tolerance thresholds and thus require one or more mitigation strategy in order to fall within an acceptable deviation.

This step is critical because there is always a possibility that at least some amount or type of residual IT risk could be found to be outside of risk tolerance. If that is the case, and depending on the amount or level of variance, it is possible that risk tolerance has been set too narrowly or tightly – that is, with very little room for deviation. If this has occurred, the IT risk assessment team will need to work with management to either refine the risk tolerance or accept the higher-than-anticipated residual risk.

Phase V: Develop the IT Audit Plan

The overall objective of Phase V is to create an internal audit plan that addresses the areas of high inherent risk (when appropriate) and high residual risk as well as other areas of concern or mandatory regulatory compliance. For example, the areas of highest inherent or residual risk might be audited annually, while areas of moderate risk are audited only every other year. Areas of low inherent risk could then be audited every third year, through control self-assessment or on an as-needed basis. Such a multiyear audit plan is likely to lead to a more manageable and efficient audit function over the long term.

In addition to establishing audit frequency, the audit plan should define responsibility for individual IT audits to determine how each area will be audited. Options might include using the internal audit team, cosourcing with a third party, performing control self-assessments, or leveraging audits performed by external regulators or auditors. The audit plan should also identify opportunities to build on the work that is already being performed as part of other internal regulatory or specialty reviews such as privacy, HIPAA, or SOX compliance audits.

Crowe Horwath

Contact Information

Raj Chaudhary, PE, CGEIT, is a principal with Crowe Horwath LLP in the Chicago office. He can be reached at 312.899.7008 or raj.chaudhary@crowehorwath.com.

Steve Hunt, CIA, CISA, CGEIT, CBM, is with Crowe Horwath LLP in the Dallas office. He can be reached at 214.574.1004 or steve.hunt@crowehorwath.com.

Phase VI: Maintain the IT Risk Assessment

The IT risk assessment process should be reviewed at least annually, according to IIA standard 2010.A1. The data captured from completed audits, monitoring processes, changes in types of risk, changes in the organization – including increases or decreases in its risk appetite or tolerance – should be reprocessed through the IT risk assessment model.

This recalculation might revalidate the current plan or identify a need to shift audit efforts and resources to emerging areas of risk. This maintenance process enables the IT audit plan to remain dynamic and focused on relevant organizational risk.

Benefits Beyond Audit Efficiency

The benefits of this comprehensive IT risk assessment framework might include a reduction in audit costs along with greater assurance that critical IT risks are being covered. Managers often find they don't need to audit some areas as frequently as they had thought previously – and sometimes discover that other areas of IT risk are being overlooked consistently.

However, the benefits to management of a comprehensive IT risk assessment go beyond an efficient audit. For example, developing a common language to define and evaluate IT risk can also help break down, on a broader scale, the silos and disconnections between processes that contribute to inefficiency and quality issues.

The organization and IT process maps, in particular, are helpful for identifying recurring patterns of IT risk that might point to enterprisewide issues such as change management, Internet security, privacy protection, and disaster recovery for business continuity. Issues such as these, which can touch all processes, might not be apparent when each process is examined individually.

In addition, the linkage of regulatory impact to organizational processes developed during the creation of the relational matrix as part of Phase I increases internal audit's ability to be more efficient and responsive when required to assess compliance functions such as privacy, HIPAA, and SOX.

Most important, at the conclusion of the IT risk assessment process the organization will have implemented an objective, structured, and repeatable organizational risk framework for creating a *quantifiable* and *defendable* multiyear IT audit plan.

www.crowehorwath.com

MOHAWK windpower

When printed by Crowe Horwath LLP, this piece is printed on Mohawk Color Copy Premium, which is manufactured entirely with Green-e® certified wind-generated electricity.

TR12901