Assessing Risks and Internal Controls

A training presentation for process owners

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Your Role as Process Owner

✓ General Expectations

- Acknowledge your responsibility for the design, implementation and maintenance of the control structure within your business processes
- Contribute direction to identify, prioritize and review risks and controls
- Remove obstacles for compliance; remedy control deficiencies
- Continue or begin a program of self-assessment and testing to monitor the controls within your processes
- Quarterly,
  - confirm key controls are implemented and effective
  - maintain documentation to support this assessment
  - sign backup certifications supporting overall Section 302 and 404 assertions

✓ Immediate Action Items

- Educate your personnel about these requirements and this effort
- Reinforce internal focus on controls within your area
- Surface any risks, concerns or issues promptly to allow adequate attention for correction (don’t wait for an audit!)
- Fix control gaps as soon as possible

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

What are Risks?

For all businesses there are risks that exist and that need to be identified and addressed in order to prevent or minimize losses.

Risk is the threat that an event, action, or non-action will adversely affect an organization's ability to achieve its business objectives and execute its strategies successfully. Risk is measured in terms of consequences and likelihood.

The following process is used for assessing risks: identifying risks, sourcing risks and measuring risks. Overall, you should focus on the high risks affecting your operations.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Risk Considerations

Considerations

- Evaluate the nature and types of errors and omissions that could occur, i.e., “what can go wrong”
- Consider significant risks (errors and omissions) that are common in the industry or have been experienced in prior years
- Information Technology risks (i.e. - access, backups, security, data integrity)
- Volume, size, complexity and homogeneity of the individual transactions processed through a given account or group of accounts (revenue, receivables)
- Susceptibility to error or omission as well as manipulation or loss
- Robustness versus subjectiveness of the processes for determining significant estimates
- Extent of change in the business and its expected effect
- Other risks extending beyond potential material errors or omissions in the financial statements

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Assertions

For all significant processes identify points within the flow of transactions or process stream where there can be failures to achieve the following assertions:

Assertion	Description
Authorization	Management has defined and communicated criteria for recognizing economic events and authorizing transactions.
Completeness and Accuracy	All transactions and other events and circumstances that occurred during a specific period and should have been recognized in that period, have, in fact, been recorded or considered. Therefore, there are no unrecorded assets, liabilities or transactions and no omitted disclosures. All, and only economic events meeting management's criteria are converted to transactions accurately and accepted for processing on a timely basis. All accepted transactions are processed accurately in accordance with management's policies and on a timely basis. Events affecting more than one system result in transactions that are reflected by each system in the same accounting period. Recorded transactions represented economic events that actually occurred during a stated period of time.
Evaluation of Balances	Assets, liabilities, revenues and expenses are recorded at appropriate amounts in accordance with relevant accounting principles. Report and database contents are periodically evaluated. Evaluation involves judgmental determinations of value. Provide reasonable assurance that reported information can be reconciled with reality.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Assertions (Continued)

Assertion	Description
Presentation, Classification and Disclosure	The captions, disclosures and other items in the financial statements are properly described and classified as well as fairly presented in conformity with generally accepted accounting principles.
Access to Assets	Physical safeguards should permit access to assets only in accordance with management's authorization.
Substantiation of Balances	Report and database contents should be periodically substantiated. Substantiation is an independent check of processing results, and is most effective if completed in an environment in which there is segregation of incompatible duties. There is reasonable assurance that reported information can be reconciled with reality.
Rights and Obligations	Assets and liabilities reported on the balance sheet are bona fide rights and obligations of the entity as of that point in time. Management should clearly identify the personnel who have primary custodial responsibility for each category of assets, critical forms and records, processing areas and processing procedures. To the extent possible, responsibility for the physical custody of an asset should be vested in employees who have no responsibility for, and are denied access to, accounting for the asset and vice versa.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

What are Internal Controls?

Management must control identified risks to help the Company:

- achieve its performance and profitability targets,
- prevent loss of resources,
- ensure reliable financial reporting, and
- ensure compliance with laws and regulations, avoiding damage to its reputation and other consequences.

In summary, internal controls can help our company get where it wants to go, and avoid pitfalls and surprises along the way.

DEFINITION OF INTERNAL CONTROL

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- ***Effectiveness and efficiency of operations***
- ***Reliability of financial reporting***
- ***Compliance with applicable laws and regulations***

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Internal Control Myths and Facts

MYTHS:	FACTS:
Internal control starts with a strong set of policies and procedures.	**Internal control starts with a strong control environment.**
Internal control: That's why we have internal auditors!	*While internal auditors play a key role in the system of control, management is the primary owner of internal control.*
Internal control is a finance thing.	**Internal control is integral to every aspect of business.**
Internal controls are essentially negative, like a list of "thou-shalt-nots."	*Internal control makes the right things happen the first time.*
Internal controls take time away from our core activities of making products, selling, and serving customers.	**Internal controls should be built "into," not "onto" business processes.**

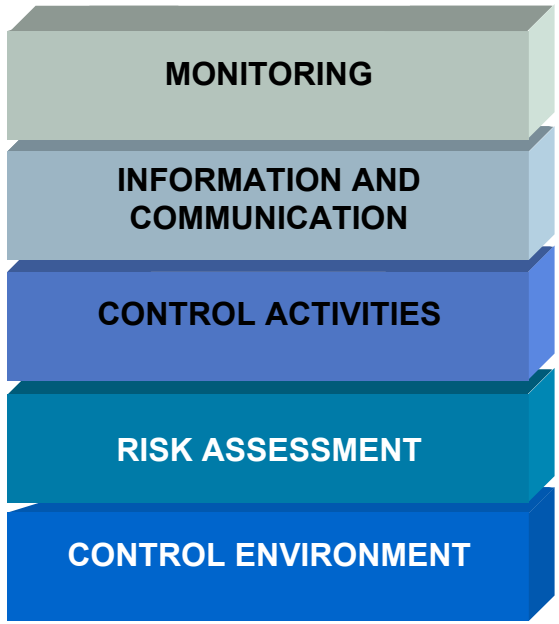
Source: Institute of Internal Auditors, 2003

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Internal Control Structure

In many cases, you perform controls and interact with the control structure every day, perhaps without even realizing it.

Monitoring:
- Monthly reviews of performance reports
- Internal audit function



Information & Communication:
- Vision and values survey
- Issue resolution calls
- Reporting
- Corporate communications (e-mail, meetings)

Control Activities:
- Purchasing limits
- Approvals
- Security
- Reconciliations
- Specific policies

Risk Assessment:
- Monthly Risk Control meetings
- Internal audit risk assessment

Control Environment:
- Tone from the top
- Corporate Policies
- Organizational authority

An internal control structure is simply a different way of viewing the business – a perspective that focuses on doing the right things in the right way.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Concepts and Objectives

Control definition reflects certain fundamental concepts:

- Internal control is **a process**. It's a means to an end, not an end in itself.
- Internal control is effected by **people**. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide **only reasonable assurance**, not absolute assurance, to an entity's management and board.

Objectives of Internal Control

Internal controls are established to further strengthen:

- The reliability and integrity of information.
- Compliance with policies, plans, procedures, laws and regulations.
- The safeguarding of assets.
- The economical and efficient use of resources.
- The accomplishment of established objectives and goals for operations or programs.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Control Focus

Redefining the control focus

The new approach to controlling business risks may be characterized by the "new rules" of "prevent and monitor" and "build in quality" as opposed to the "old rules" of "detect and correct" and "inspect in quality." This means a paradigm shift in the traditional viewpoint of control as illustrated in the following table:

Old Paradigm	New Paradigm
• Only AUDITORS and TREASURY are concerned about risks and controls	• EVERYONE, including operations, is concerned about managing business risks
• FRAGMENTATION – Every function and department does its own thing ("SILO MANAGEMENT")	• Business risk assessment and control are FOCUSED and COORDINATED with senior level OVERSIGHT
• NO BUSINESS RISK CONTROL POLICY	• FORMAL BUSINESS RISK CONTROL POLICY approved by management and the board
• INSPECT for and DETECT business risk and REACT to it	• ANTICIPATE and PREVENT business risk at the source and MONITOR business risk controls continuously
• Ineffective PEOPLE are the primary source of business risk	• Ineffective PROCESSES are the primary source of business risk

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

CONTROL TECHNIQUES

Prevention techniques are designed to provide reasonable assurance that only valid transactions are recognized, approved and submitted for processing. Therefore, many of the preventive techniques are applied before the processing activity occurs. In most situations, preventive techniques are likely to be more effective in a strong control environment, when management authorization criteria are well-defined and properly communicated.

Control type definitions:
Preventive - Manual
Preventive - System

Examples of preventive controls include:

- Segregation of duties **(Preventive-Manual)**
- Business systems integrity and continuity controls, e.g., application design standards, change controls, security controls, systems backup and recovery **(Preventive – System)**
- Physical safeguard and access restriction controls (human, financial, physical and information assets) **(Preventive-Manual)**
- Effective planning/budgeting process **(Preventive-Manual)**
- Effective "whistle blowing" processes **(Preventive-Manual)**

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

CONTROL TYPES

Detection techniques are designed to provide reasonable assurance that errors and irregularities are discovered and corrected on a timely basis. Detection techniques normally are performed after processing has been completed. They are particularly important in an environment that has relatively weak preventive techniques. That is, when front-end approval and processing techniques do not provide reasonable assurance that unacceptable transactions are prevented from being processed or do not assure that all approved transactions are processed accurately. In this case, after-the-fact techniques become more important in detecting and correcting processing errors.

Control type definitions:
Detective - Manual
Detective - System

Examples of detection techniques include:

- Reconciliation of batch balance reports to control logs maintained by originating departments. **(Detective – Manual)**
- Reconciliation of cycle inventory counts with perpetual records. **(Detective – Manual)**
- Review and approval of reference file maintenance ("was-is") reports. **(Detective – Manual)**
- Comparison of reported results with plans and budgets. **(Detective – Manual)**
- Reconciliation of subsidiary ledger balances with the general ledger. **(Detective – Manual)**
- Reconciliation of interface amounts exiting one system and entering another. **(Detective – System)**
- Review of on-line access and transaction logs. **(Detective – System)**

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Conclusion

✓ Why all this trouble?

- Compliance with a very visible law
- Puts teeth into the value statement, “Do it right the first time”
- Additional comfort and “tightness” that the company is doing the right things and communicating the right information internally, to the auditors and to the public
- Over time, the metrics that evolve to monitor the control areas can provide insight for key business decisions
- Documentation will provide communication tool with management and improve ability to train and share information

✓ What happens if we don’t do this?

- Less formal control structures leave room for risks to become real issues
- External Auditor may not sign their attestation of our control structure
- Potential SEC investigation
- Investor, lender and customer confidence will be further weakened, affecting stock price and available financing

✓ What are the next steps?

- Continue communication
- Validation of process documentation
- Identification and sourcing of risks and controls

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Appendix - COSO Components Defined

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), was formed in 1985 to improve the quality of financial reporting through business ethics, effective internal controls and corporate governance. Based on these principles, they developed and published the COSO framework in 1992 as a foundation for establishing internal control systems and determining their effectiveness.

Control Environment

- The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors.

Risk Assessment

- Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Control Activities

- Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)

Appendix - COSO Components Defined (cont.)

Information and Communication

- Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Monitoring

- Internal control systems need to be monitored -- a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

Source: Protiviti KnowledgeLeader (www.knowledgeleader.com)