Internal Audit Risk Assessment and Audit Planning

Supplemental Handouts

CCIA Spring 2011

May 6, 2011
Interactive IPPF

Updated as of March 15, 2011

Standards - Performance Standard

2010 – Planning

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:
The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board.

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.

2010.A2 – The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization’s operations. Accepted engagements must be included in the plan.

Related IPPF Guidance

The Institute of Internal Auditors
247 Maitland Avenue, Altamonte Springs, Florida, 32701
Tel. 1+407-937-1100, Fax. 1+407-937-1101
Web: http://www.theiia.org, Email: online@theiia.org
Interactive IPPF

Updated as of March 15, 2011
Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures

Primary Related Standard

2010 – Planning
The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Interpretation:
The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization’s risk management framework, including using risk tolerance levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board.

1. In developing the internal audit activity’s audit plan, many chief audit executives (CAEs) find it useful to first develop or update the audit universe. The audit universe is a list of all the possible audits that could be performed. The CAE may obtain input on the audit universe from senior management and the board.

2. The audit universe can include components from the organization’s strategic plan. By incorporating components of the organization’s strategic plan, the audit universe will consider and reflect the overall business’ objectives. Strategic plans also likely reflect the organization’s attitude toward risk and the degree of difficulty to achieving planned objectives. The audit universe will normally be influenced by the results of the risk management process. The organization’s strategic plan considers the environment in which the organization operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

3. The CAE prepares the internal audit activity’s audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization. Key audit objectives are usually to provide senior management and the board with assurance and information to help them accomplish the organization’s objectives, including an assessment of the effectiveness of management’s risk management activities.

4. The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the organization. In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the organization’s business, operations, programs, systems, and controls.
5. Audit work schedules are based on, among other factors, an assessment of risk and exposures. Prioritizing is needed to make decisions for applying resources. A variety of risk models exist to assist the CAE. Most risk models use risk factors such as impact, likelihood, materiality, asset liquidity, management competence, quality of and adherence to internal controls, degree of change or stability, timing and results of last audit engagement, complexity, and employee and government relations.

***
Primary Related Standard
2010 – Planning
The chief audit executive must establish risk–based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.

1. Risk management is a critical part of providing sound governance that touches all the organization’s activities. Many organizations are moving to adopt consistent and holistic risk management approaches that should, ideally, be fully integrated into the management of the organization. It applies at all levels — enterprise, function, and business unit — of the organization. Management typically uses a risk management framework to conduct the assessment and document the assessment results.

2. An effective risk management process can assist in identifying key controls related to significant inherent risks. Enterprise risk management (ERM) is a term in common use. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission defines ERM 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.” Implementation of controls is one common method management can use to manage risk within its risk appetite. Internal auditors audit the key controls and provide assurance on the management of significant risks.

3. The IIA’s International Standards for the Professional Practice of Internal Auditing (Standards) defines control as “any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.”

4. Two fundamental risk concepts are inherent risk and residual risk (also known as current risk). Financial/external auditors have long had a concept of inherent risk that can be summarized as the susceptibility of information or data to a material misstatement, assuming that there are no related mitigating controls. The Standards define residual risk as “the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.” Current risk is often defined as the risk managed within existing controls or control systems.

5. Key controls can be defined as controls or groups of controls that help to reduce an otherwise unacceptable risk to a tolerable level. Controls can be most readily conceived as organizational processes that exist to address risks. In an effective risk management process (with adequate documentation), the key controls can be readily identified from the difference between inherent and residual risk across all affected systems that are relied upon to reduce the rating of significant risks. If a rating has not been given to inherent risk, the internal auditor estimates the inherent risk rating. When identifying key controls (and
assuming the internal auditor has concluded that the risk management process is mature and reliable), the internal auditor would look for:

- Individual risk factors where there is a significant reduction from inherent to residual risk (particularly if the inherent risk was very high). This highlights controls that are important to the organization.
- Controls that serve to mitigate a large number of risks.

6. Internal audit planning needs to make use of the organizational risk management process, where one has been developed. In planning an engagement, the internal auditor considers the significant risks of the activity and the means by which management mitigates the risk to an acceptable level. The internal auditor uses risk assessment techniques in developing the internal audit activity’s plan and in determining priorities for allocating internal audit resources. Risk assessment is used to examine auditable units and select areas for review to include in the internal audit activity’s plan that have the greatest risk exposure.

7. Internal auditors may not be qualified to review every risk category and the ERM process in the organization (e.g., internal audits of workplace health and safety, environmental auditing, or complex financial instruments). The chief audit executive (CAE) ensures that internal auditors with specialized expertise or external service providers are used appropriately.

8. Risk management processes and systems are set up differently throughout the world. The maturity level of the organization related to risk management varies among organizations. Where organizations have a centralized risk management activity, the role of this activity includes coordinating with management regarding its continuous review of the internal control structure and updating the structure according to evolving risk appetites. The risk management processes in use in different parts of the world might have different logic, structures, and terminology. Internal auditors therefore make an assessment of the organization’s risk management process and determine what parts can be used in developing the internal audit activity’s plan and what parts can be used for planning individual internal audit assignments.

9. Factors the internal auditor considers when developing the internal audit plan include:

- Inherent risks — Are they identified and assessed?
- Residual risks — Are they identified and assessed?
- Mitigating controls, contingency plans, and monitoring activities — Are they linked to the individual events and/or risks?
- Risk registers — Are they systematic, completed, and accurate?
- Documentation — Are the risks and activities documented?

In addition, the internal auditor coordinates with other assurance providers and considers planned reliance on their work. Refer to The IIA’s Practice Advisory 2050-2: Assurance Maps.

10. The internal audit charter normally requires the internal audit activity to focus on areas of high risk, including both inherent and residual risk. The internal audit activity needs to identify areas of high inherent risk, high residual risks, and the key control systems upon which the organization is most reliant. If the internal audit activity identifies areas of unacceptable residual risk, management needs to be notified so that the risk can be
addressed. The internal auditor will, as a result of conducting a strategic audit planning process, be able to identify different kinds of activities to include in the internal audit activity’s plan, including:

- Control reviews/assurance activities — where the internal auditor reviews the adequacy and efficiency of the control systems and provides assurance that the controls are working and the risks are effectively managed.
- Inquiry activities — where organizational management has an unacceptable level of uncertainty about the controls related to a business activity or identified risk area and the internal auditor performs procedures to gain a better understanding of the residual risk.
- Consulting activities — where the internal auditor advises organizational management in the development of the control systems to mitigate unacceptable current risks.

Internal auditors also try to identify unnecessary, redundant, excessive, or complex controls that inefficiently reduce risk. In these cases, the cost of the control may be greater than the benefit realized and therefore there is an opportunity for efficiency gains in the design of the control.

11. To ensure relevant risks are identified, the approach to risk identification is systematic and clearly documented. Documentation can range from the use of a spreadsheet in small organizations to vendor supplied software in more sophisticated organizations. The crucial element is that the risk management framework is documented in its entirety.

12. The documentation of risk management in an organization can be at various levels below the strategic level of the risk management process. Many organizations have developed risk registers that document risks below the strategic level, providing documentation of significant risks in an area and related inherent and residual risk ratings, key controls, and mitigating factors. An alignment exercise can then be undertaken to identify more direct links between risk “categories” and “aspects” described in the risk registers and, where applicable, the items already included in the audit universe documented by the internal audit activity.

13. Some organizations may identify several high (or higher) inherent risk areas. While these risks may warrant the internal audit activity’s attention, it is not always possible to review all of them. Where the risk register shows a high, or above, ranking for inherent risk in a particular area, and the residual risk remains largely unchanged and no action by management or the internal audit activity is planned, the CAE reports those areas separately to the board with details of the risk analysis and reasons for the lack of, or ineffectiveness of, internal controls.

14. A selection of lower risk level business unit or branch type audits need to periodically be included in the internal audit activity’s plan to give them coverage and confirm that their risks have not changed. Also, the internal audit activity establishes a method for prioritizing outstanding risks not yet subject to an internal audit.

15. An internal audit activity’s plan will normally focus on:

- Unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately.
• Control systems on which the organization is most reliant.
• Areas where the differential is great between inherent risk and residual risk.
• Areas where the inherent risk is very high.

16. When planning individual internal audits, the internal auditor identifies and assesses risks relevant to the area under review

***
Primary Related Standard

2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement’s objectives, scope, timing, and resource allocations.

1. The internal auditor plans and conducts the engagement, with supervisory review and approval. Prior to the engagement’s commencement, the internal auditor prepares an engagement program that:
   - States the objectives of the engagement.
   - Identifies technical requirements, objectives, risks, processes, and transactions that are to be examined.
   - States the nature and extent of testing required.
   - Documents the internal auditor’s procedures for collecting, analyzing, interpreting, and documenting information during the engagement.
   - Is modified, as appropriate, during the engagement with the approval of the chief audit executive (CAE), or his or her designee.

2. The CAE should require a level of formality and documentation (e.g., of the results of planning meetings, risk assessment procedures, level of detail in the work program, etc.) that is appropriate to the organization. Factors to consider would include:
   - Whether the work performed and/or the results of the engagement will be relied upon by others (e.g., external auditors, regulators, or management).
   - Whether the work relates to matters that may be involved in potential or current litigation.
   - The experience level of the internal audit staff and the level of direct supervision required.
   - Whether the project is staffed internally, by guest auditors, or by external service providers.
   - The project’s complexity and scope.
   - The size of the internal audit activity.
   - The value of documentation (e.g., whether it will be used in subsequent years).

3. The internal auditor determines the other engagement requirements, such as the period covered and estimated completion dates. The internal auditor also considers the final engagement communication format. Planning at this stage facilitates the communication process at the engagement’s completion.

4. The internal auditor informs those in management who need to know about the engagement, conducts meetings with management responsible for the activity under review, summarizes and distributes the discussions and any conclusions reached from the meetings, and retains the documentation in the engagement working papers. Topics of discussion may include:
• Planned engagement objectives and scope of work.
• The resources and timing of engagement work.
• Key factors affecting business conditions and operations of the areas being reviewed, including recent changes in internal and external environment.
• Concerns or requests from management.

5. The CAE determines how, when, and to whom engagement results will be communicated. The internal auditor documents this and communicates it to management, to the extent deemed appropriate, during the planning phase of the engagement. The internal auditor communicates to management subsequent changes that affect the timing or reporting of engagement results.

***
Practice Advisory 2200-2:  
Using a Top-down, Risk-based Approach to Identify the Controls to be Assessed in an Internal Audit Engagement  

Primary Related Standard  
2200 – Engagement Planning  
Internal auditors must develop and document a plan for each engagement, including the engagement’s objectives, scope, timing, and resource allocations.


2. This practice advisory assumes that the objectives for the internal audit engagement have been determined and the risks to be addressed have been identified in the internal audit planning process. It provides guidance on the use of a top-down, risk-based approach to identify and include in the internal audit scope (per Standard 2220) the key controls relied upon to manage the risks.

3. “Top-down” refers to basing the scope definition on the more significant risks to the organization. This is in contrast to developing the scope based on the risks at a specific location, which may not be significant to the organization as a whole. A top-down approach ensures that internal auditing is focused, as noted in Practice Advisory 2010-2, on “providing assurance on the management of significant risks.”

4. A system of internal control typically includes both manual and automated controls. (Note that this applies to controls at every level — entity, business process, and information technology (IT) general controls — and in every layer of the control framework; for example, activities in the control environment, monitoring, or risk assessment layers may also be automated.) Both types of controls need to be assessed to determine whether business risks are effectively managed. In particular, the internal auditor needs to assess whether there is an appropriate combination of controls, including those related to IT, to mitigate business risks within organizational tolerances. The internal auditor needs to consider including procedures to assess and confirm that risk tolerances are current and appropriate.

5. The internal audit scope needs to include all the controls required to provide reasonable assurance that the risks are effectively managed (subject to the comments in paragraph 9, below). These controls are referred to as key controls — those necessary to manage risk associated with a critical business objective. Only the key controls need to be assessed, although the internal auditor can choose to include an assessment of non-key controls (e.g., redundant, duplicative controls) if there is value to the business in providing such assurance. The internal auditor may also discuss with management whether the non-key controls are required.

6. Note that where the organization has a mature and effective risk management program, the key controls relied upon to manage each risk will have been identified. In these cases, the internal auditor needs to assess whether management’s identification and assessment of the key controls is adequate.

7. The key controls can be in the form of:
• Entity-level controls (e.g., employees are trained and take a test to confirm their understanding of the code of conduct). The entity-level controls may be manual, fully automated, or partly automated.
• Manual controls within a business process (e.g., the performance of a physical inventory).
• Fully automated controls within a business process (e.g., matching or updating accounts in the general ledger).
• Partly automated controls within a business process (also called “hybrid” or IT-dependent controls), where an otherwise manual control relies on application functionality such as an exception report. If an error in that functionality would not be detected, the entire control could be ineffective. For example, a key control to detect duplicate payments might include the review of a system generated report. The manual part of the control would not ensure the report is complete. Therefore, the application functionality that generated the report should be in scope.

The internal auditor may use other methods or frameworks, as long as all the key controls relied upon to manage the risks are identified and assessed, including manual controls, automated controls, and controls within IT general control processes.

8. Fully and partly automated controls — whether at the entity level or within a business process — generally rely on the proper design and effective operation of IT general controls. GAIT-R discusses the recommended process for identifying key IT general controls.

9. The assessment of key controls may be performed in a single, integrated internal audit engagement or in a combination of internal audit engagements. For example, one internal audit engagement may address the key controls performed by business process users, while another covers the key IT general controls, and a third assesses related controls that operate at the entity level. This is common where the same controls (especially those at the entity level or within IT general controls) are relied upon for more than one risk area.

10. As noted in paragraph 5, before providing an opinion on the effective management of the risks covered by the internal audit scope, it is necessary to assess the combination of all key controls. Even if multiple internal audit engagements are performed, each addressing some key controls, the internal auditor needs to include in the scope of at least one internal audit engagement an assessment of the design of the key controls as a whole (i.e., across all the related internal audit engagements) and whether it is sufficient to manage risks within organizational tolerances.

11. If the internal audit scope (considering other internal audit engagements as discussed in paragraph 9) includes some, but not all, key controls required to manage the targeted risks, a scope limitation should be considered and clearly communicated in the internal audit notification and final report.

***
Practice Advisory 2210-1: Engagement Objectives

Primary Related Standard

2210 – Engagement Objectives
Objectives must be established for each engagement.

1. Internal auditors establish engagement objectives to address the risks associated with the activity under review. For planned engagements, the objectives proceed and align to those initially identified during the risk assessment process from which the internal audit plan is derived. For unplanned engagements, the objectives are established prior to the start of the engagement and are designed to address the specific issue that prompted the engagement.

2. The risk assessment during the engagement’s planning phase is used to further define the initial objectives and identify other significant areas of concern.

3. After identifying the risks, the auditor determines the procedures to be performed and the scope (nature, timing, and extent) of those procedures. Engagement procedures performed in appropriate scope are the means to derive conclusions related to the engagement objectives.

***
Practice Advisory 2210.A1-1: Risk Assessment in Engagement Planning

Primary Related Standard
2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

1. Internal auditors consider management’s assessment of risks relevant to the activity under review. The internal auditor also considers:
   - The reliability of management’s assessment of risk.
   - Management’s process for monitoring, reporting, and resolving risk and control issues.
   - Management’s reporting of events that exceeded the limits of the organization’s risk appetite and management’s response to those reports.
   - Risks in related activities relevant to the activity under review.

2. Internal auditors obtain or update background information about the activities to be reviewed to determine the impact on the engagement objectives and scope.

3. If appropriate, internal auditors conduct a survey to become familiar with the activities, risks, and controls to identify areas for engagement emphasis, and to invite comments and suggestions from engagement clients.

4. Internal auditors summarize the results from the reviews of management’s assessment of risk, the background information, and any survey work. The summary includes:
   - Significant engagement issues and reasons for pursuing them in more depth.
   - Engagement objectives and procedures.
   - Methodologies to be used, such as technology-based audit and sampling techniques.
   - Potential critical control points, control deficiencies, and/or excess controls.
   - When applicable, reasons for not continuing the engagement or for significantly modifying engagement objectives.

***
Institute of Internal Auditors Standards

- Dollar materiality
- Asset liquidity
- Management competence
- Quality of internal controls
- Degree of change or stability
- Time of last audit engagement
- Complexity
- Employee and government relations

Patton, Evans, and Lewis¹ (in order of importance)

- Quality of Internal Control
- Competence of Management
- Integrity of Management
- Size of Unit ($)
- Recent Change in Accounting System
- Complexity of Operations
- Liquidity of Assets
- Recent Change in Key Personnel
- Economic Condition of Unit
- Rapid Growth
- Extent of Computerized Systems
- Time Since Last Audit
- Pressure on Management to Meet Objectives
- Extent of Government Relations
- Level of Employee Morals
- Audit Plans of External Auditors
- Political Exposure
- Need to Maintain an Appearance of Independence by Internal Auditor
- Distance from Main Office

McNamee and McNamee²

- Short-Term/Financial Threats


Community College Internal Auditors
Spring Conference 2011
Common Risk Factors

- Errors (may be multiplied into various major error types/categories)
- Omissions
- Delays (may be internal, external, or both)
- Fraud (may be employee, supplier, customer, or internal/external categories)

- Mid-Term Threats/Opportunities
  - Cost Avoidance
  - Cost Savings
  - Cost Recoveries
  - Revenue Enhancement (program enhancement for government/not-for-profits)
  - Asset Utilization (may be multiplied into various major asset types/categories)
  - Employee Satisfaction/Utilization (a form of asset utilization)

- Long-Term Opportunities
  - Customer Satisfaction
  - Supplier Satisfaction
  - System Improvement
  - Product Quality
  - Market Share
  - Other long-term goal issues from the organization’s mission/vision/purpose statements
EXTERNAL RISK

External risk arises when there are external forces that can affect an organization’s performance, or make its choices regarding its strategies, operations, customer and supplier relationships, organizational structure or financing obsolete or ineffective. These forces are outside management’s ability to control.

**Competitor Risk** – Major competitors or new entrants to the market take actions to establish and sustain competitive advantage over the organization or even threaten its ability to survive.

**Customer Wants Risk** – The organization is not aware that customer needs and wants change. Such needs and wants may apply to desired quality, willingness to pay and/or speed of execution.

**Technological Innovation Risk** – The organization is not leveraging advancements in technology in its business model to achieve or sustain competitive advantage or is exposed to the actions of competitors or substitutes that do leverage technology to attain superior quality, cost and/or time performance in their products, services and processes.

**Sensitivity Risk** – Sensitivity risk results when management commits the organization's resources and expected cash flows from future operations to such an extent that it reduces the organization's tolerance for (or ability to withstand) changes in environmental forces that are totally beyond its control.

**Shareholder Expectations Risk** – The risk of failing to manage shareholder expectations, resulting in a decline in investor confidence that may impair the organization's ability to efficiently raise capital and reduce stock evaluations over time.

**Capital Availability Risk** – The organization does not have efficient access to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.

**Sovereign/Political Risk** – The risk of adverse consequences through political actions in a country in which a organization has made significant investments (a major project, for example), is dependent on a significant volume of business or has entered into an agreement with a counter party subject to the laws of that country.

**Legal Risk** – The risk that a organization's transactions, contractual agreements and specific strategies and activities are not enforceable under applicable law.

**Regulatory Risk** – Changes in regulations and actions by national or local regulators can result in increased competitive pressures and significantly affect a organization's ability to efficiently conduct business.

**Industry Risk** – The risk that the industry will lose its attractiveness due to changes in the key factors for competitive success within the industry, capabilities of existing and potential competitors, and organization’s strengths and weaknesses relative to competitors.

**Financial Markets Risk** – Financial markets risk is defined as exposure to changes in the earnings capacity or economic value of the firm as a result of changes in financial market variables (e.g., currency rates). These changes affect income, expense or balance sheet values.
**Catastrophic Loss Risk** – The inability to sustain operations, provide essential products and services, or recover operating costs as a result of a major disaster.

**INTERNAL RISK**

The risk that business processes are not clearly defined, are poorly aligned with business objectives and strategies, do not satisfy customer needs, dilute shareholder wealth, or expose assets to misappropriation or misuse.

**Governance Risk** – The risk that the organization’s governance processes do not comply with legal requirements or stakeholder expectations and that the board of directors fails to provide adequate monitoring and oversight of executive management activities.

- **Organizational Culture Risk** – The organization’s culture does not encourage managers to realistically portray the potential outcomes of transactions, deals, investments and projects and understand and portray the full picture for decision makers. The organization experiences dysfunctional behavior because managers are either risk averse or incented to take risks beyond the organization’s risk appetite.

- **Ethical Behavior Risk** – The organization, through its actions or inaction, demonstrates that it is not committed to ethical and responsible business behavior.

- **Board Effectiveness Risk** – The board does not constructively engage management and provide anticipatory, proactive and interactive oversight of the organization’s activities and affairs, with integrity, vision, common sense and unquestioned independence.

- **Succession Planning Risk** – Leadership talent within the organization is not sufficiently developed to provide for orderly succession in the future.

**Reputation Risk** – The risk of loss of brand image such that the organization will be unable to operate in the marketplace.

- **Image and Branding Risk** – The risk that a organization may lose customers, key employees or its ability to compete, due to perceptions that it does not deal fairly with customers, suppliers and stakeholders, or know how to manage its business.

- **Stakeholder Relations Risk** – A decline in investor confidence may impair a organization's ability to efficiently raise capital. The organization will not have the same efficient access as competitors to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.

**Operations Risk** – The risk that operations are inefficient and ineffective in satisfying customers and achieving the organization’s quality cost and time objectives.

- **Customer Satisfaction Risk** – The organization's processes do not consistently meet or exceed customer expectations due to a lack of focus on the customer.

- **Human Resources Risk** – The personnel responsible for managing and controlling an organization or a business process do not possess the requisite knowledge, skills and
experience needed to ensure that critical business objectives are achieved and significant business risks are reduced to an acceptable level.

Knowledge Capital Risk – Processes for capturing and institutionalizing learning across the organization are either nonexistent or ineffective, resulting in slow response time, high costs, repeated mistakes, slow competence development, constraints on growth and unmotivated employees.

Product Development Risk – The productivity of the product development process is significantly less than more innovative competitors who are able to achieve higher productivity through a stronger customer focus, concentrating focused resources and faster cycle time.

Efficiency Risk – The process is inefficient in satisfying valid customer requirements resulting in higher than competitive costs.

Capacity Risk – The effective productive capacity of the plant is not fully utilized, resulting in spreading fixed costs over fewer units and creating higher unit costs and lower unit margins or the capacity does not fulfill customer needs resulting in a loss of business.

Scalability Risk – The inability to operate differently and more efficiently at larger volumes or amortize costs over greater sales volume, resulting in diseconomies of scale that threaten the firm's ability to generate competitive profit margins.

Performance Gap Risk – A business process does not perform at a world-class level because the practices designed into the process are inferior.

Cycle Time Risk – Elapsed time between the start and completion of a business process (or activity within a process) is too long because of redundant, unnecessary and irrelevant steps.

Sourcing Risk – The fewer the alternative sources of energy, metals and other key commodities and raw materials used in an organization's operations, the greater the risks of shortages and higher costs. These risks can significantly affect the organization's capability to provide competitively priced products and services to customers at the time they are wanted.

Channel Effectiveness Risk – Poorly performing or positioned distribution channels threaten the organization’s capacity to access current and potential customers/end users effectively and efficiently.

Partnering Risk – Inefficient or ineffective alliance, joint venture, affiliate and other external relationships affect the organization's capability to compete. These uncertainties arise due to choosing the wrong partner, poor execution, receiving more value than is given (ultimately resulting in loss of a partner) and failing to capitalize on partnering opportunities.

Compliance Risk – As a result of a flaw in design or operation or due to human error, oversight or indifference, the organization's processes do not meet customer requirements the first time or do not comply with prescribed procedures and policies. Compliance risk can also result in failure to conform with laws and regulations at the international, country, state and local level that apply to a business process.
Business Interruption Risk – The organization's capability to continue critical operations and processes may be highly dependent on availability of certain raw materials, information technologies, skilled labor and other resources.

Product/Service Failure Risk – The organization's operations create risk of customers receiving faulty or nonperforming products or services.

Environmental Risk – Environmental risks expose companies to potentially enormous liabilities. The exposure is twofold -- (1) liability to third parties for bodily injury or property damage caused by the pollution, and (2) liability to governments or third parties for the cost of removing pollutants plus severe punitive damages.

Health and Safety Risk – These risks expose an organization to potentially significant workers' compensation liabilities, financial loss, and negative publicity. Firms and their managers could find themselves criminally liable for failure to provide a safe working environment for their employees.

Trademark/Brand Erosion Risk – The risk that a trademark or brand will lose its value. A trademark is a word, symbol or device -- or any combination of these -- that identifies a product or service and distinguishes that product or service from the products or services of competitors.

Empowerment Risk – The risk that managers and employees are not properly lead, do not know what to do (or how to do it) when they need to do it, exceed the boundaries of their defined authorities, do not have the resources, training and tools necessary to make effective decisions or are given incentives to do the wrong thing.

Leadership Risk – The risk that the people responsible for the important business processes do not or cannot provide the leadership, vision, and support necessary to help employees be effective and successful in their jobs.

Authority/Limit Risk – The risk that people either make decisions or take actions that are not within their explicit responsibility or control or fail to take responsibility for those things for which they are accountable. Failure to establish or enforce limits on personnel actions may cause employees to commit unauthorized, illegal or unethical acts or assume unauthorized or unacceptable business risks.

Outsourcing Risk – Outside service providers do not act within their defined limits of authority and do not perform in a manner consistent with the values, strategies and objectives of the organization.

Performance Incentives Risk – Unrealistic, subjective or unclear performance measures may cause managers and employees to act in a manner that is inconsistent with the organization's business objectives, strategies, ethical standards and prudent business practice.

Change Readiness Risk – The people within the organization are unable to implement process and product/service improvements quickly enough to keep pace with changes in the marketplace.
Communications Risk – Communication channels (top-down and bottom-up or cross-functional) within the organization are ineffective and result in messages that are inconsistent with authorized responsibilities or established measures.

Information Technology Risk – The risk that the information technologies used in the business are not efficiently and effectively supporting the current and future needs of the business or threaten the organization’s ability to sustain the operation of critical business processes.

Integrity Risk – This risk encompasses all of the risks associated with the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by and reported on by the various application systems deployed by an organization.

Access Risk – Access risk includes the risk that access to information (data or programs) or systems will be inappropriately granted or refused. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases and risks associated with information confidentiality.

Availability Risk – The risk that information will not be available when needed. This includes risks such as loss of communications (e.g., cut cables, telephone system outage, satellite loss), loss of basic processing capability (e.g., fire, flood, electrical outage) and operational difficulties (e.g., disk drive breakdown, operator errors).

Infrastructure Risk – The risk that the organization does not have an effective information technology infrastructure (e.g., hardware, networks, software, people and processes) to effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion.

Integrity Risk – The risk of management fraud, employee fraud, and illegal and unauthorized acts, any or all of which could lead to reputation degradation in the marketplace or even financial loss.

Management Fraud Risk – Management issues misleading financial statements with intent to deceive the investing public and the external auditor or engages in bribes, kickbacks, influence payments and other schemes for the benefit of the organization.

Employee Fraud and Third Party Fraud Risk – Fraudulent activities perpetrated by employees, customers, suppliers, agents, brokers or third-party administrators against the organization for personal gain expose the organization to financial loss.

Illegal Acts Risk – Managers and employees individually or in collusion commit illegal acts, placing the organization, its directors and officers at risk to the consequences of their actions.

Unauthorized Use Risk – The organization's employees (or others) use its physical and financial assets for unauthorized or unethical purposes.

Financial Risk – Financial risk can occur if the organization fails to provide adequate liquidity to meet the firm’s obligations or manages financial risks in a manner that is inconsistent with the firm’s business objectives. Its severity depends on a number of factors, which include the firm’s
size, industry, financial position (e.g. public/private, leverage, free cash flow to equity, etc.), and the direction of the market as a whole.

**Price Risk** – The exposure of earnings or net worth to changes in market factors (e.g., interest rates, currency rates), which affect income, expense or balance sheet values.

Interest Rate Risk – The risk that interest rates deviate from their expected value resulting in lower-than-expected investment yields, higher-than-expected borrowing or product costs, or deterioration of the firm’s competitive position in its industry.

Currency Risk – The exposure to fluctuations in exchange rates may arise as a result of business activity in foreign markets and investment in securities, which are issued by overseas entities or are denominated in a foreign currency.

Equity Risk – The exposure to fluctuations in the income stream and/or value of equity ownership in an incorporated entity.

Commodity Risk – This can be a financial market risk if an organization chooses an investment as part of a diversification strategy for managing investment risk. From the industrial perspective, commodity risk is the exposure to fluctuations in prices of commodity-based materials or products (e.g., gold, energy, copper, and coffee).

Financial Instrument Risk – Financial market risk can vary depending upon the particular segment of the market to which the holder of a financial instrument is exposed, or the way in which the exposure is structured.

**Liquidity Risk** – The exposure to loss as a result of the inability to meet cash flow obligations in a timely and cost-effective manner. Liquidity risk often arises as a result of an investment portfolio with a cash flow and/or maturity profile, which differs from the underlying cash flows dictated by the organization's operating requirements and other obligations.

Cash Flow Risk – Actual losses incurred as a result of the inability to fund the operational or financial obligations of the business.

Opportunity Cost Risk – The use of funds in a manner that leads to the loss of economic value, including time value losses, transaction costs due to inappropriate or inefficient management of cash flows and other causes of loss of value.

Concentration Risk – Exposure to loss as a result of the inability to access cash in a timely manner due to the inability to liquidate exposures without moving the market, unusual market conditions, use of “proprietary” financial products, or excessive reliance on a small number of funding sources.

**Credit Risk** – The exposure to actual loss or opportunity cost as a result of default (or other failure to perform) by an economic or legal entity (the debtor) with which the organization does business.

Default Risk – A counterparty will be unable to fulfill its obligations.
Concentration Risk – Inappropriate emphasis of sales volume or revenues on a single customer, industry sector, or other economic segment leads to exposure to excessive loss.

Settlement Risk – In financial terms, this risk arises when financial counterparties effect their payments to each other at different times or in different locations. In a non-financial context, settlement risk describes the risk of unexpected costs and/or administrative inconvenience associated with the failure to deliver payment in the right place at the right time.

Collateral Risk – This is the risk that the value of an asset provided as collateral for a loan, receivable, or commitment to perform may be partially or totally lost.

**INFORMATION RISK**

The risk that information used to support strategic, operational and financial decisions is not relevant or reliable. This risk relates to the usability and timeliness of information that is either created or summarized by processes and application systems or a failure to understand information needs.

**Operational Risk –**

- **Budget and Planning Risk** – Budgets and business plans are not realistic, based on appropriate assumptions, based on cost drivers and performance measures, accepted by key managers, or used as a monitoring tool.
- **Product/Service Pricing Risk** – The organization's price is more than customers are willing to pay or does not cover production and distribution costs.
- **Contract Commitment Risk** – The organization does not have information that effectively tracks contractual commitments outstanding at a point in time, so that the financial implications of decisions to enter into incremental commitments can be appropriately considered by decision makers.
- **Measurement (Operations) Risk** – Process performance measures do not provide a reliable portrayal of operating performance and do not accurately reflect reality. The measures do not provide relevant information for decision making because they are not informative, understandable, believable, actionable, or indicators of change.
- **Alignment Risk** – The objectives and performance measures of the organization's business processes are not aligned with its overall business objectives and strategies. The objectives and measures do not focus people on the right things and lead to conflicting, uncoordinated activities.
- **Accounting Information Risk** – Financial accounting information used to manage business processes is not properly integrated with nonfinancial information focused on customer satisfaction, measuring quality, reducing cycle time and increasing efficiency. The result is a myopic, short-term fixation on manipulating the outputs of business processes to achieve financial targets, rather than fulfilling customer expectations by controlling and improving processes.
Public Reporting –

Financial Reporting Evaluation Risk – Financial reports issued to existing and prospective investors and lenders include material misstatements or omit material facts, making them misleading.

Internal Control Evaluation Risk – Failure to accumulate sufficient relevant and reliable information to assess the design and operating effectiveness of internal control over financial reporting, resulting in inaccurate assertions by management in the internal control report.

Executive Certification Risk – Failure to accumulate sufficient, relevant and reliable information to assess the design and operating effectiveness of disclosure controls and procedures, resulting in material information not being disclosed timely to certifying officers and in public reports.

Taxation Risk – Significant transactions of the organization have adverse tax consequences that could have been avoided had they been structured differently. Failure to comply with all tax regulations (e.g. payment and filing requirements) creates risks.

Pension Fund Risk – Pension funds are not actuarially sound, e.g., they are insufficient to satisfy benefit obligations defined by the plan.

Regulatory Reporting Risk – Reports of operating and financial information required by regulatory agencies are incomplete, inaccurate, or untimely, exposing the organization to fines, penalties and sanctions.

Strategic Risk –

Environmental Scan Risk – The failure to monitor and stay in touch with a rapidly changing environment resulting in obsolete business strategies.

Business Model Risk – The organization has an obsolete business model and doesn't recognize it and/or lacks the information needed to make an up-to-date assessment of its current model and build a compelling business case for modifying that model on a timely basis.

Business Portfolio Risk – The risk that a firm will not maximize business performance by effectively prioritizing its products or balancing its businesses in a strategic context.

Investment Valuation/Evaluation Risk – Management does not have sufficient financial information to make informed short-term and long-term investment decisions and link the risks accepted to the capital at risk. Management and key decision-makers are unable to reliably measure the value of a specific business or any of its significant segments in a strategic context.

Organization Structure Risk – The organization's organizational structure does not support change or the organization's business strategies.
**Measurement (Strategy) Risk** – Occurs when overall organizational performance measures focus primarily on near-term financial results or are not consistent with and do not support business strategies.

**Resource Allocation Risk** – The organization's resource allocation process does not establish and sustain competitive advantage or maximize returns for shareholders.

**Planning Risk** – The organization's business strategies are not driven by creative and intuitive input or based on current assumptions about the external environment resulting in strategies that are out-of-date and unfocused.

**Life Cycle Risk** – An organization's approach to managing the movement of its product lines and evolution of its industry along the life cycle (e.g., start-up, growth, maturity and decline) threatens the ultimate success of its business strategies.
Interviewee/Title/Department:

Interviewers:

I. Introduction

• Introduction of interviewers and the project
• Purpose of the project (Why this project?)
• Stress confidentiality of the interview
• What is your background?

II. Macro Level – general operations/strategy

• What are the Company’s key business objectives? (the three to five most important; Vision, Mission, Stated Objectives)
• What are the significant business risks the Company faces relative to the key objectives?
• What really worries you?
  (relative to the organization as a whole and to your specific area)

• How are these risks currently being addressed? How effective is that?

• How would you address these risks? (what solutions would you suggest?)
• What recent or planned changes are there in the business? Organization? Competitive environment? Technology? Regulations?

III. Micro Level – the business unit or areas of responsibility of the interviewee

• What are your responsibilities?

• What are your objectives for your business unit/ areas of responsibility?
• What are the significant risks of your business unit/areas of responsibility?

• How are these risks currently being addressed? How effective is that?

• How would you address these risks? (what solutions would you suggest?)
• What recent or planned changes are there in your business unit/areas of responsibility?

• What issues (in the organization or your business unit) derive from:
  – Complexity or size of the operation?
  – Hand off of information between business functions/operational units?
  – Easily transferable/marketable assets? (liquidity)
  – Regulations or other issues that may impact the Company’s reputation?
IV. Closing

- What role can Internal Audit play in the organization and in your department

- Have we missed anything? Are there any other comments you would like to add?