Internal Audit (IA) Methodology

ICAI Bhawan, Bandra-Kurla Complex
26th August 2016

Introduction

Introduction to Standards on Internal Audit

The Council of the Institute of Chartered Accountants of India (ICAI) at its 240th meeting held on 5th February, 2004 had constituted the Committee on Internal Audit (a non standing Committee of the Institute). The main function of the Committee on Internal Audit, among other things, was to review the existing internal audit practices in India and to develop Standards on Internal Audit (SIAs).

Till date 18 SIAs have been issued under the authority of the Council.

At present all the standards are recommendatory.

protiviti
Risk & Business Consulting.
Internal Audit.

Why are SIAs introduced?

- To provide a benchmark for quality of services during an internal audit.

- With the introduction of SIAs the ICAI aims to codify the best practices in internal audit services.

Strategic Importance of SIAs

As internal audit may be conducted by professionals other than CAs, our Institute has indeed made a strategic move by initiating the codification of Standards on Internal Auditing, and thereby gain the advantage of being the first professional body to give a disciplined structure to the Internal Audit function. This would indeed give the first mover's advantage to ICAI and its members.

protiviti
Risk & Business Consulting.
Internal Audit.

What is Internal Audit?

Paragraph 3.1 of the Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India defines internal audit as follows:

"Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's risk management and internal control system"
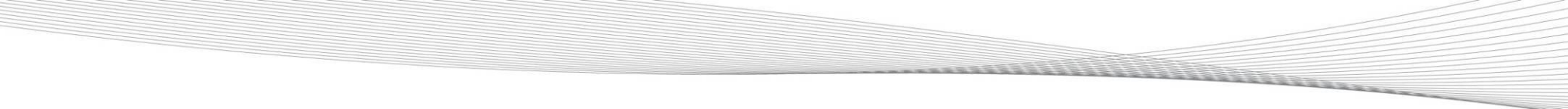

Why Internal Audit is important?

- Prevents Fraud
- Tests Internal Control
- Monitors Compliance with Company Policy
- Government Regulation

protiviti
Risk & Business Consulting.
Internal Audit.

Objectives of Internal Audit

- To evaluate the *internal control* systems and integrity of financial and operational information produced by these systems.

- To determine whether *compliance* exists in accordance with policies, procedures, laws and regulations.

- To determine whether *assets are safeguarded* and verifying the existence of these assets.

- To appraise the economy and *efficiency* of resource utilization.

- To review the operations and programs for *consistency* with established *management goals and objectives.*

protiviti
Risk & Business Consulting
Internal Audit.

Now you all know Auditing standards play an important role in performing Internal Audit

protiviti
Risk & Business Consulting.
Internal Audit.

But, How well do you know the standards?

protiviti
Risk & Business Consulting
Internal Audit

SIA issued by ICAI

|	
SIA 1 - Planning on Internal Audit	SIA 10 - Internal Audit Evidence
SIA 2 - Basic principles Governing Internal Audit	SIA 11 - Consideration of Fraud in an Internal Audit
SIA 3 - Documentation	SIA 12 - Internal Control Evaluation
SIA 4 - Reporting	SIA 13 - Enterprise Risk Management
SIA 5 - Sampling	SIA 14 - Internal Audit in an Information Technology Environment
SIA 6 - Analytical Procedures	SIA 15 - Knowledge of the Entity and it's Environment
SIA 7 - Quality Assurance in Internal Audit	SIA 16 - Using the Work of an Expert
SIA 8 - Terms of Internal Audit Engagement	SIA 17 - Consideration of Laws and Regulations in an Internal Audit
SIA 9 - Communication with Management	SIA 18 - Related Parties

protiviti
Risk & Business Consulting
Internal Audit.

International Standards for the Professional Practice of Internal Auditing

1000 – Purpose, Authority and Responsibility	2070 – External Service Provider and Organizational Responsibility for Internal Auditing
1010 - Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter	2100 – Nature of Work
1100 - Independence and Objectivity	2110 – Governance
1110 – Organizational Independence	2120 – Risk Management
1111 – Direct Interaction with the Board	2130 – Control
1120 – Individual Objectivity	2201 – Planning Considerations
1130 – Impairment to Independence or Objectivity	2210 – Engagement Objectives
1200 – Proficiency	2220 – Engagement Scope
1210 – Proficiency and Due Professional Care	2230 – Engagement Resource Allocation
1220 – Due Professional Care	2240 – Engagement Work Program
1230 – Continuing Professional Development	2300 – Performing the Engagement
1300 – Quality Assurance and Improvement Program	2310 – Identifying Information
1310 – Requirements of the Quality Assurance and Improvement Program	2320 – Analysis and Evaluation
1311 – Internal Assessments	2330 – Documenting Information
1312 - External Assessments	2340 – Engagement Supervision
1320 – Reporting on the Quality Assurance and Improvement Program	2400 – Communicating Results
1321 – Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"	2410 – Criteria for Communicating
1322 – Disclosure of Nonconformance	2420 – Quality of Communications
2000 – Managing the Internal Audit Activity	2421 – Errors and Omissions
2010 – Planning	2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"
2020 – Communication and Approval	2431 – Engagement Disclosure of Nonconformance
2030 – Resource Management	2440 – Disseminating Results
2040 – Policies and Procedures	2450 – Overall Opinions
2050 – Coordination	2500 – Monitoring Progress
2060 – Reporting to Senior Management and the Board	2600 – Communicating the Acceptance of Risks

protiviti
Risk & Business Consulting
Internal Audit

COSO 2013

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) 2013 Framework should be utilized to design and review an IFC Framework
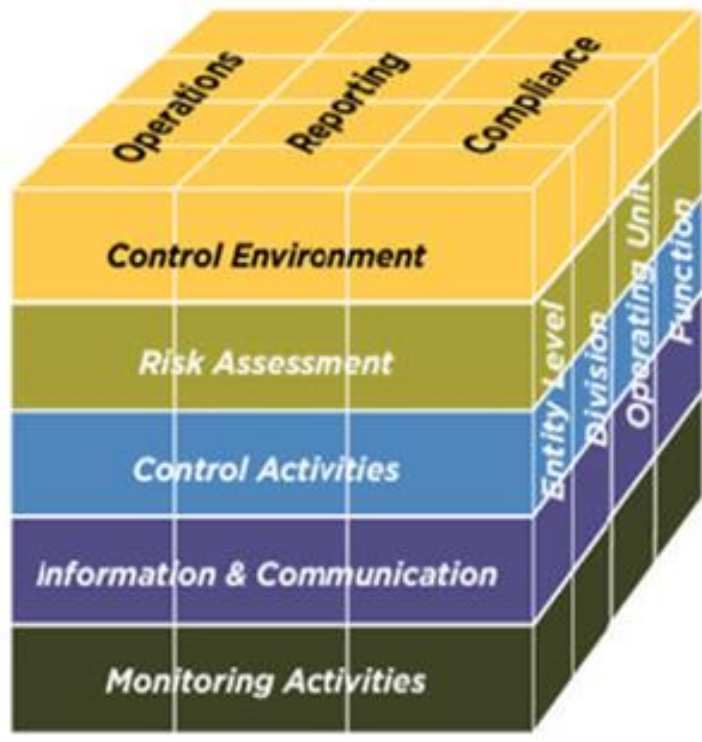
The COSO 2013 Internal Control: Integrated Framework **consists of 5 components.**

The Components have to be effective across the Entities, Divisions, Operating Units and Functions.

The new framework includes **17 COSO Principles** to be addressed and also includes **77 Points of Focus** to provide helpful guidance to assist management in designing, implementing and operating an effective internal control environment, as well as, in assessing whether relevant principles are present and functioning.

protiviti
Risk & Business Consulting.
Internal Audit.

COSO 2013 – Control Environment

Control Environment			
Principles		**Points of Focus**	
1	The organization demonstrates a commitment to integrity and ethical values	1	Sets the tone at the top
		2	Establishes standards of conduct
		3	Evaluates adherence to standards of conduct
		4	Addresses deviations in a timely manner
2	The board of directors demonstrates independence from management and exercises oversight of the develop-ment and performance of internal control	5	Establishes oversight responsibilities
		6	Applies relevant expertise
		7	Operates independently
		8	Provides oversight on Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities
3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives	9	Considers all structures of the entity
		10	Establishes reporting lines
		11	Defines, assigns, and limits authorities and responsibilities

protiviti
Risk & Business Consulting.
Internal Audit.

COSO 2013 – Control Environment (Contd.)

Control Environment (continued)			
Principles		**Points of Focus**	
4	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives	12	Establishes policies and practices
		13	Evaluates competence and addresses shortcomings
		14	Attracts, develops and retains individuals
		15	Plans and prepares for succession
5	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives	16	Enforces accountability through structures, authorities and responsibilities
		17	Establishes performance measures, incentives and rewards
		18	Evaluates performance measures, incentives and rewards for ongoing relevance
		19	Considers excessive pressures
		20	Evaluates performance and rewards or disciplines individuals

protiviti
Risk & Business Consulting.
Internal Audit.

COSO 2013 – Risk Assessment

Risk Assessment		
Principles	**Points of Focus**	
6 The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives:		
– Operations Objectives	21a	Reflects management's choices
	22a	Considers tolerances for risk
	23	Includes operations and financial performance goals
	24	Forms a basis for committing of resources
– External Financial Reporting Objectives	21b	Complies with applicable accounting standards
	22b	Considers materiality
	25	Reflects entity activities
– External Non-Financial Reporting Objectives	21c	Complies with externally established standards and frameworks
	22c	Considers the required level of precision

protiviti
Risk & Business Consulting.
Internal Audit.

COSO 2013 – Risk Assessment (Contd.)

Risk Assessment			
Principles		**Points of Focus**	
– Internal Reporting Objectives		21a	Reflects management's choices
		22c	Considers the required level of precision
		25	Reflects entity activities
– Compliance Objectives		21d	Reflects external laws and regulations
		22a	Considers tolerances for risk
7	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed	26	Includes entity, subsidiary, division, operating unit, and functional levels
		27	Analyzes internal and external factors
		28	Involves appropriate levels of management
		29	Estimates significance of risks identified
		30	Determines how to respond to risks
8	The organization considers the potential for fraud in assessing risks to the achievement of objectives	31	Considers various types of fraud
		32	Assesses incentives and pressures
		33	Assesses opportunities
		34	Assesses attitudes and rationalizations

protiviti
Risk & Business Consulting
Internal Audit.

COSO 2013 – Risk Assessment (Contd.)

Risk Assessment		
Principles	**Points of Focus**	
9 The organization identifies and assesses changes that could significantly impact the system of internal control	35	Assesses changes in the external environment
	36	Assesses changes in the business model
	37	Assesses changes in leadership

protiviti®
Risk & Business Consulting.
Internal Audit.

COSO 2013 – Control Activities

Control Activities		
Principles	**Points of Focus**	
10 The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	38	Integrates with risk assessment
	39	Considers entity-specific factors
	40	Determines relevant business processes
	41	Evaluates a mix of control activity types
	42	Considers at what level activities are applied
	43	Addresses segregation of duties
11 The organization selects and develops general control activities over technology to support the achievement of objectives	44	Determines dependency between the use of technology in business processes and technology general controls
	45	Establishes relevant technology infrastructure control activities
	46	Establishes relevant security management process control activities
	47	Establishes relevant technology acquisition, development, and maintenance process control activities

COSO 2013 – Control Activities (Contd.)

Control Activities		
Principles	**Points of Focus**	
12 The organization deploys control activities through policies that establish what is expected and procedures that put policies into action	48	Establishes policies and procedures to support deployment of management's directives
	49	Establishes responsibility and accountability for executing policies and procedures
	50	Performs in a timely manner
	51	Takes corrective action
	52	Performs using competent personnel
	53	Reassesses policies and procedures

protiviti
Risk & Business Consulting
Internal Audit

COSO 2013 – Information and Communication

Information and Communication			
Principles		**Points of Focus**	
13	The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control	54	Identifies information requirements
		55	Captures internal and external sources of data
		56	Processes relevant data into information
		57	Maintains quality throughout processing
		58	Considers costs and benefits
14	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control	59	Communicates internal control information
		60	Communicates with the board of directors
		61	Provides separate communication lines
		62	Selects relevant method of communication
15	The organization communicates with external parties regarding matters affecting the functioning of other components of internal control	63	Communicates to external parties
		64	Enables inbound communications
		65	Communicates with the board of directors
		66	Provides separate communication lines
		67	Selects relevant method of communication

protiviti
Risk & Business Consulting
Internal Audit

COSO 2013 – Monitoring Activities

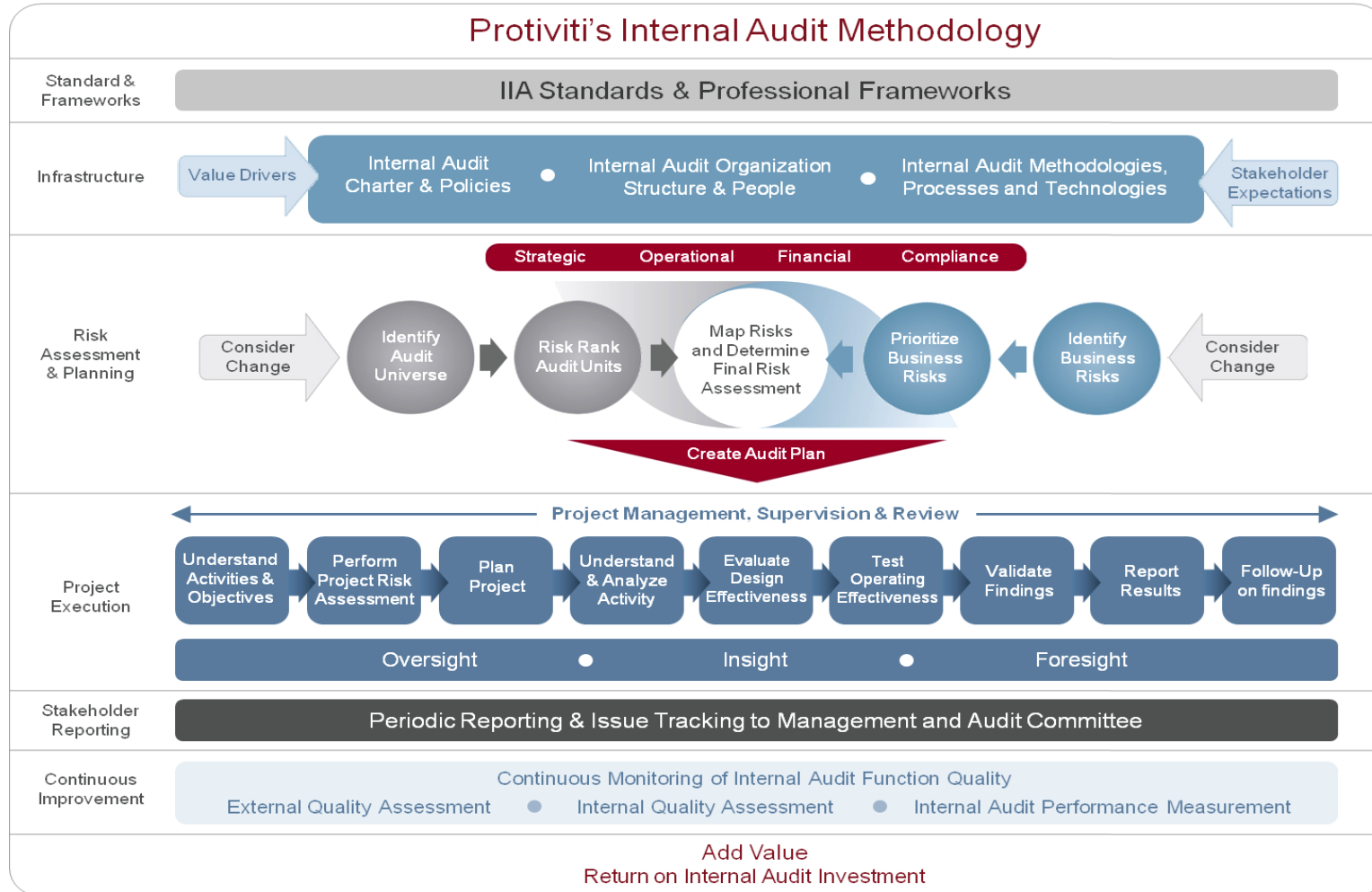| Monitoring Activities			
Principles		**Points of Focus**	
16	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning	68	Considers a mix of ongoing and separate evaluations
		69	Considers rate of change
		70	Establishes baseline understanding
		71	Uses knowledgeable personnel
		72	Integrates with business processes
		73	Adjusts scope and frequency
		74	Objectively evaluates
17	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate	75	Assesses results
		76	Communicates deficiencies to parties responsible for corrective action and to senior management and the board of directors
		77	Monitors corrective actions

protiviti
Risk & Business Consulting.
Internal Audit.

Control Environment & Risk Assessment

Principles relating to the Control Environment component include:

- The organization demonstrates a commitment to integrity and ethical values

- The board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control

- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives

- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with the objectives

- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives

Principles relating to the Risk Assessment component include:

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives

- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed

- The organization considers the potential for fraud in assessing risks to the achievement of objectives

- The organization identifies and assesses changes that could significantly impact the system of internal control

protiviti
Risk & Business Consulting.
Internal Audit.

Control Activities, Information Communication & Monitoring

Principles relating to the Control Activities component include:

- The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels

- The organization selects and develops general control activities over technology to support the achievement of objectives

- The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action

Principles relating to the Information & Communication component include:

- The organization obtains or generates and uses relevant, quality information to support the functioning of internal control

- The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

- The organization communicates with external parties regarding matters affecting the functioning of internal control

Principles relating to the Monitoring Activities component include:

- The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning

- The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors as appropriate

IA Methodology

Our Internal Audit Methodology

We will use Protiviti's Internal Audit Methodology. The methodology is standardized yet flexible, allowing for creativity and customized approaches to meet any organization's needs.

Protiviti's Internal Audit Methodology

Standard & Frameworks

IIA Standards & Professional Frameworks

Infrastructure

Value Drivers → Internal Audit Charter & Policies · Internal Audit Organization Structure & People · Internal Audit Methodologies, Processes and Technologies ← Stakeholder Expectations

Risk Assessment & Planning

Strategic   Operational   Financial   Compliance

Consider Change → Identify Audit Universe → Risk Rank Audit Units → Map Risks and Determine Final Risk Assessment ← Prioritize Business Risks ← Identify Business Risks ← Consider Change

Create Audit Plan

Project Execution

Project Management, Supervision & Review

Understand Activities & Objectives → Perform Project Risk Assessment → Plan Project → Understand & Analyze Activity → Evaluate Design Effectiveness → Test Operating Effectiveness → Validate Findings → Report Results → Follow-Up on findings

Oversight ● Insight ● Foresight

Stakeholder Reporting

Periodic Reporting & Issue Tracking to Management and Audit Committee

Continuous Improvement

Continuous Monitoring of Internal Audit Function Quality

External Quality Assessment ● Internal Quality Assessment ● Internal Audit Performance Measurement

Add Value
Return on Internal Audit Investment

protiviti
Risk & Business Consulting
Internal Audit

Key Differentiators of Our Internal Audit Methodology

Our Internal Audit methodology:

- Is built in line with the IIA's International Professional Practices Framework of Internal Auditing

- Is COSO and COBIT based, which facilitates the assessment of IT risks, from the Entity-Level Risk Assessment to the creation of solutions for identified control issues

- Provides a standard approach which drives the quality, efficiency and focus of our people

- Provides a framework to a risk-based internal audit plan

- Uses widely accepted control frameworks and internal audit methods and is designed to add value

- Ensures consistent results world-wide

- Provides standard approaches along with supporting training and technology that enables us to use our Subject Matter Experts more effectively

Protiviti's Internal Audit Methodology

protiviti
Risk & Business Consulting
Internal Audit
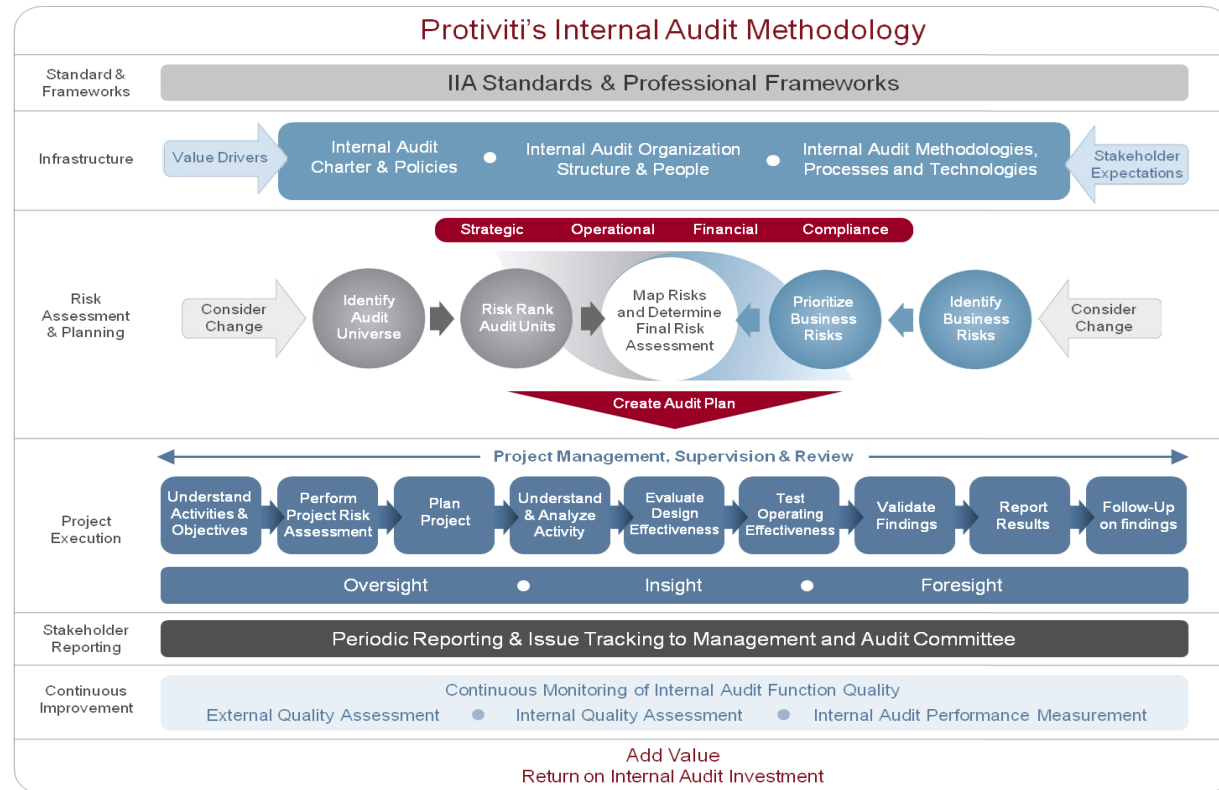
Our Approach – Standards & Frameworks

Standards & Frameworks	IIA Standards & Professional Frameworks

The IIA Standards and Professional Frameworks

We follow the IIA Standards and the IIA Code of Ethics. We utilize a variety of internationally recognized professional frameworks in our internal audit work, the primary ones being COSO and COBIT.

Protiviti's Internal Audit Methodology
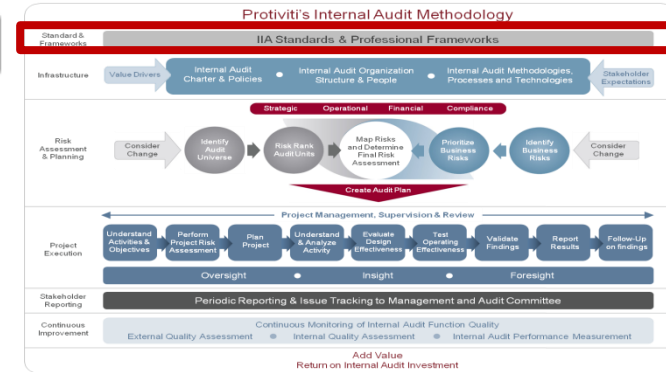
International Professional Practices Framework issued by the Institute of Internal Auditors

Three Dimensions of COSO Integrated Framework
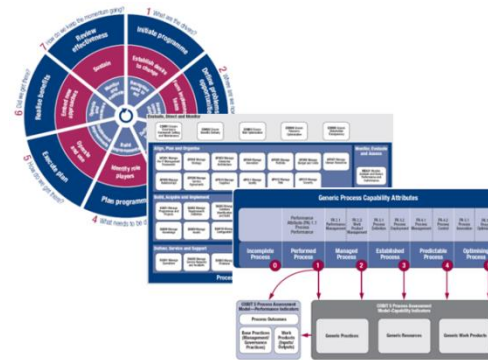
COBIT Framework

ISO 27001 standards

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance

ISO 27001 standards

protiviti
Risk & Business Consulting.
Internal Audit.

Our Approach – Infrastructure

Value Drivers & Stakeholder Expectations

We will strive to understand stakeholder expectations and their value drivers so that Internal Audit is focused on a value-added plan that is responsive to the needs of BMMI.

Internal Audit Charter & Policies

Our Internal Audit engagements start with an Internal Audit Charter that articulates:

- Function's mandate
- Authority
- Organization
- Responsibility
- Code of ethics.

We build policies and procedures to guide overall internal audit activity. We also have our own Protiviti Internal Audit Policy, The Protiviti Way, which guides how we execute Internal Audit engagements. It is in alignment with the IIA Standards and outlines our client service and delivery protocols. Our Quality and Risk Management policies outline how we manage our risk as a firm and require that certain protocols be followed.

Internal Audit Organization Structure & People

The appropriate structure needs to be determined for each Internal Audit function: either central at corporate, geographically dispersed, or some combination of both. We work with organizations to set up a structure that meets their needs and identify resources with the necessary skills to perform the work. This includes involving specialists with industry, process, regulatory and technology knowledge.

protiviti
Risk & Business Consulting.
Internal Audit.
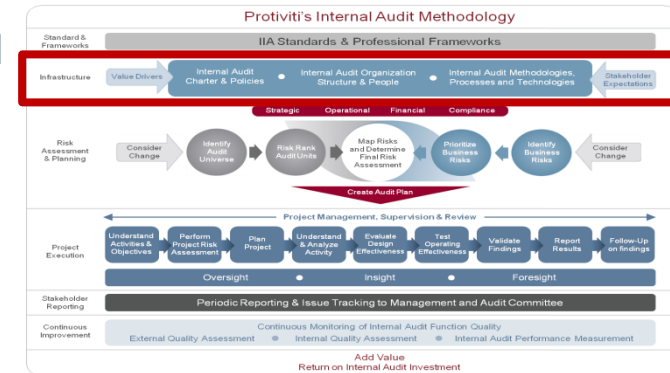
Our Approach – Infrastructure (Contd.)

Internal Audit Methodologies, Processes and Technologies

Our Internal Audit Methodology provides a common framework for our people to perform internal audit work. We will determine up front what type of reporting and project administration would be necessary for each engagement. Our Protiviti Way policy outlines required tasks on our projects in order to comply with the IIA Standards, realize efficiencies, create high-quality work, add value and facilitate consistent practices.
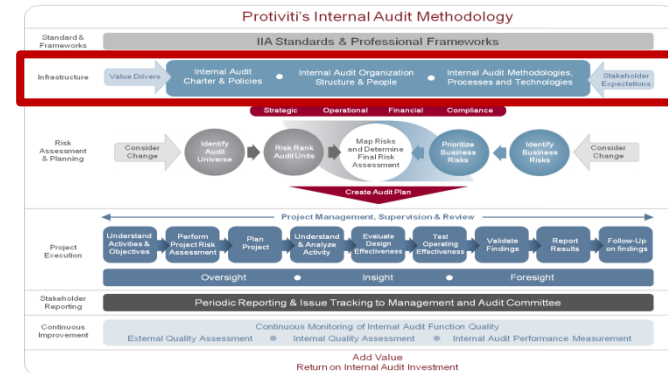
In addition to Protiviti's Internal Audit Methodology, we will use the following Protiviti Frameworks to execute our internal audit work:

- Protiviti Risk Model^{SM}
- Technology Risk Model
- Process Classification Scheme
- Six Elements of Infrastructure and Capability Maturity Model

We utilize the following technologies to perform internal audits:

- Protiviti's Governance Model
- Data Analysis – ACL^{TM}, Excel®, Protiviti's Spend Risk Assessor^{SM}
- Process Mapping – Visio®
- Audit Work Papers – Protiviti's Internal Audit Portal
- Knowledge Sharing – Protiviti's KnowledgeLeader^{SM}, iShare, Discoveri^{TM}

We can tailor our technologies and methodologies to organizations' requirements, but we generally follow the IIA Standards at a minimum.

protiviti
Risk & Business Consulting
Internal Audit.

Extract from SIA 3- Documentation

Purpose, Authority and Responsibility must be formally given in the Internal Audit Charter and CAE should review the Internal Audit Charter periodically

What is the Internal Audit Charter?

Internal Audit Charter

- Governing document for Internal Audit in a company
- Approved by audit committee
- Defines Scope of Internal Audit Department
- Authorises Internal Audit Department to carry out activities on behalf of audit committee
- Details Roles and Responsibilities of Internal Audit Director, Manager and Staff

The Internal Audit Charter also includes:
- Chief Audit Executives relationship with the Board.
- Access to records, personnel and physical properties relevant to the performance of engagement.
- Nature of Assurance services that can be undertaken.
- Nature of Consulting services that can be undertaken.

Extract from SIA 2 – Basic Principles Governing Internal Audit

- Due professional care signifies that the internal auditor exercises *reasonable care* in carrying out the work entrusted to him *in terms of deciding on aspects* such as the *extent of work* required to achieve the objectives of the engagement, relative *complexity* and *materiality* of the matters subjected to internal audit, assessment of *risk management, control* and *governance* processes and *cost benefit analysis.*

- Due professional care, however, *neither implies nor guarantees infallibility, nor does it require the internal auditor to travel beyond the scope of his engagement.*

- The internal auditor should either *have or obtain such skills and competence,* acquired through *general education, technical knowledge* obtained through study and *formal courses,* as are necessary for the purpose of discharging his responsibilities.

- The internal auditor also has a *continuing responsibility* to *maintain professional knowledge and skills* at a level required *to ensure* that the *client or the employer receives the advantage of competent professional service* based on the *latest developments* in the *profession,* the *economy,* the *relevant industry* and *legislation.*

protiviti
Risk & Business Consulting.
Internal Audit.

Governance Portal

Protiviti's Governance Portal offers clients a flexible technology solution to balance sound governance with business performance.
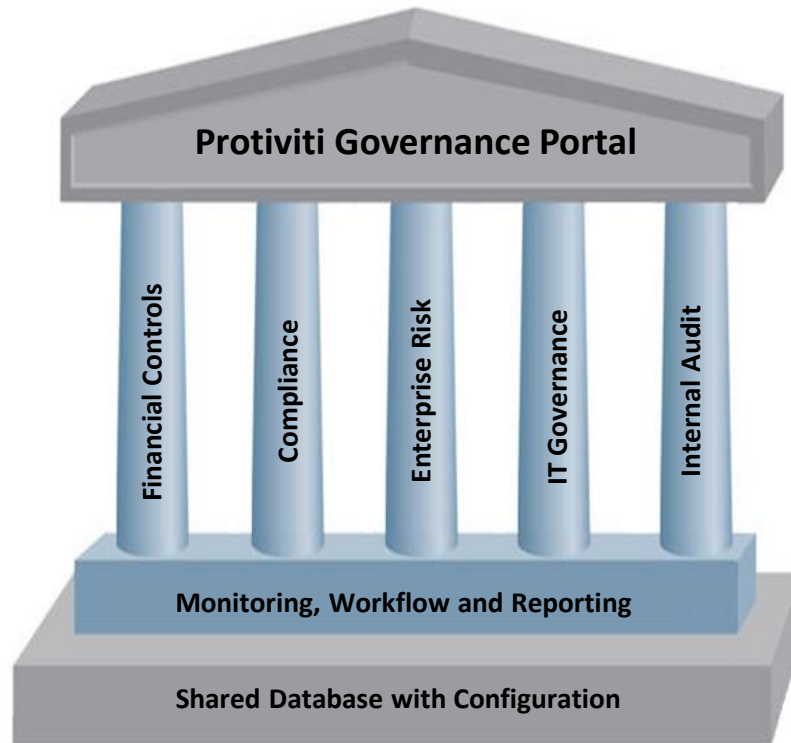
GRC Module

A GRC system that supports governance, risk and compliance, control management, and incident management. The GRC system can be used for implementing the ERM.

Internal Audit Module

GRC can also be extended to an integrated audit management system that facilitates risk assessment, planning, electronic work papers, issue management and reporting.

protiviti®
Risk & Business Consulting.
Internal Audit.

Our Approach – Risk Assessment & Planning
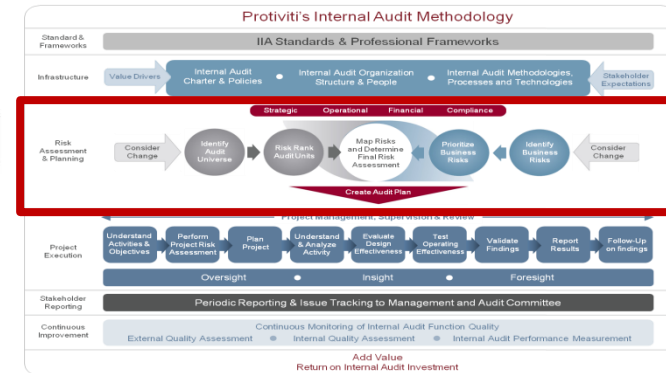
Identify Audit Universe

- We will identify the audit universe at the beginning of our relationship with BMMI.

- Identifying an audit universe entails the following considerations:
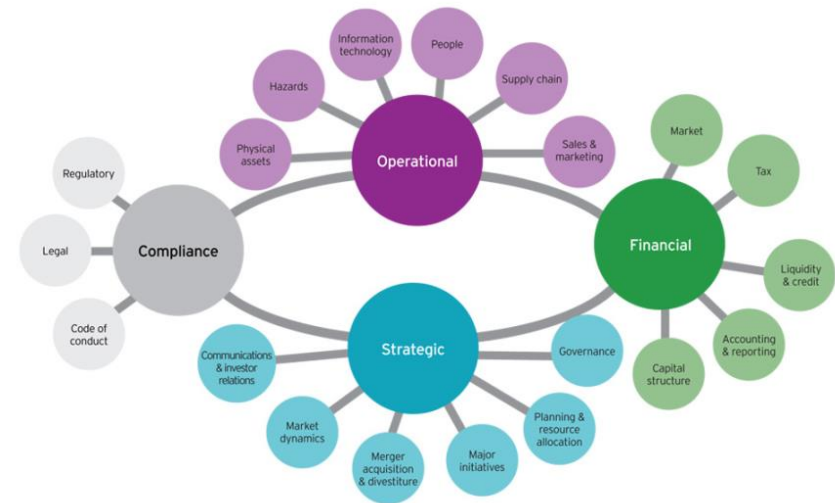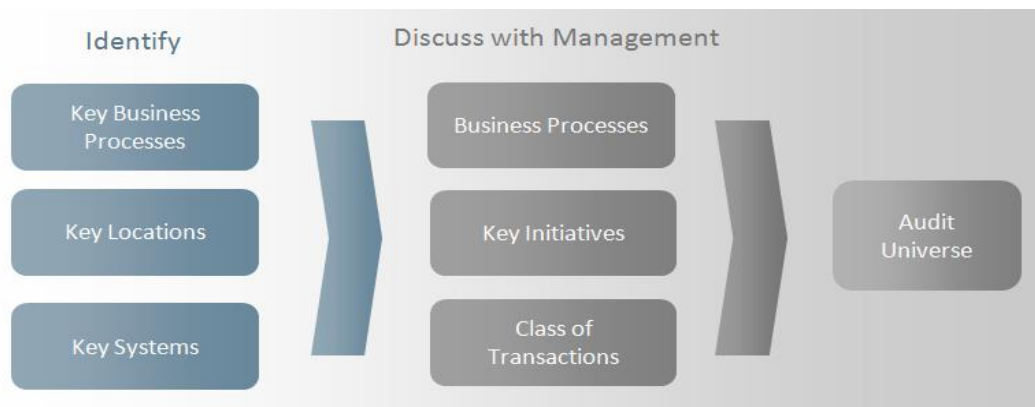
Our Approach – Risk Assessment & Planning (Contd.)
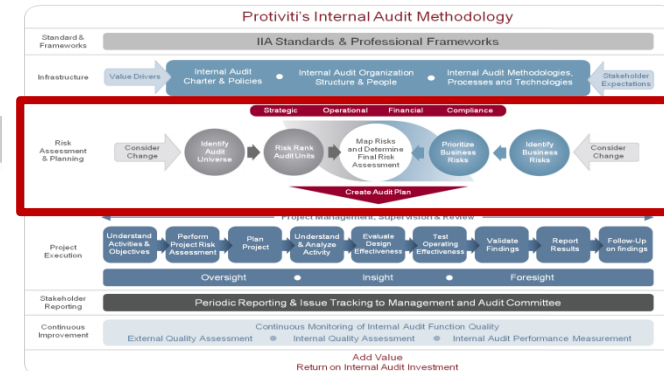
Identify Business Risks

- We shall work with the management to gain an understanding of the business strategy, unique goals and objectives vis-à-vis potential obstacles to meeting them.

- We shall utilize our understanding of BMMI's industry, business and environment by utilizing Protiviti Business Risk Models, i.e. tailored for Retail, Distribution, Services and Government sectors, as a reference point to identify key risks.

- We shall focus on three sources of uncertainties to identify business risks i.e.
    - Environment risk – uncertainties affecting the viability of the business mode
    - Process risk – uncertainties affecting the execution of the business model
    - Information for decision making risk – uncertainties over the relevance and reliability of information

- We shall consolidate this information to develop an initial business risk universe.

protiviti
Risk & Business Consulting
Internal Audit.
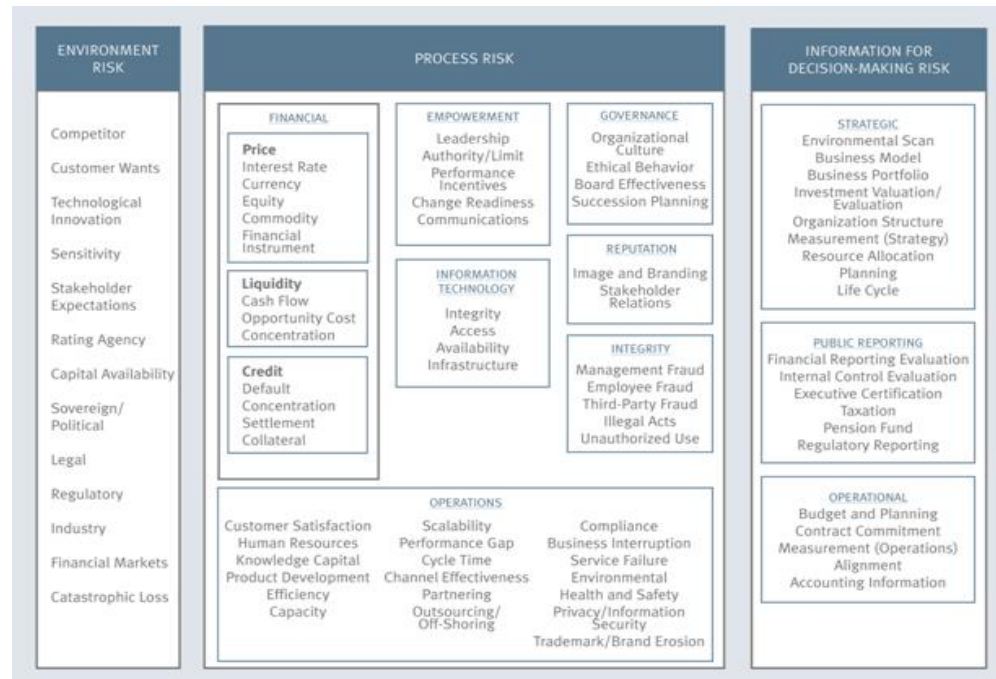
Our Approach – Risk Assessment & Planning (Contd.)
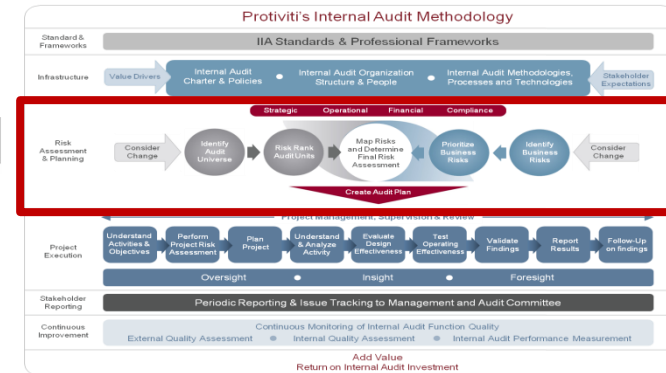
Prioritize Business Risks

- During identification of business risks, we shall gain an understanding of the overall "tone at the top" of BMMI and its entity-level control environment around the COSO framework's five components. This shall enable us to assess whether entity-level processes should become part of the audit plan and/or entity-level control gaps should be incorporated into the work programs of individual audits.

- After obtaining a solid understanding of the industry, business, objectives and entity-level control environment, we will conduct a top-down, BMMI wide assessment of all types of risk affecting BMMI at both the inherent and residual risk level. This shall include considering:

  - past history and experience;

  - known, planned and future initiatives;

  - any other risk management activities occurring in BMMI.

- Prior to risk assessment, identified business risks shall be categorised into Strategic, Operational, Financial and Compliance risks. This will facilitate effective prioritization of risks.

- Risk assessments are performed through a discussion based approach from that risk maps are produced which map the impact of each risk against the likelihood of their occurrence.

protiviti
Risk & Business Consulting
Internal Audit
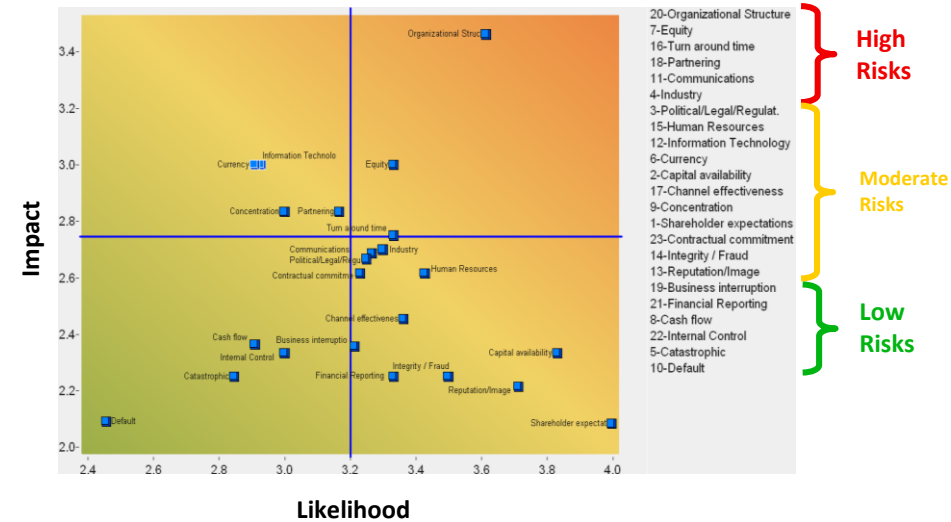
Our Approach – Risk Assessment & Planning (Contd.)
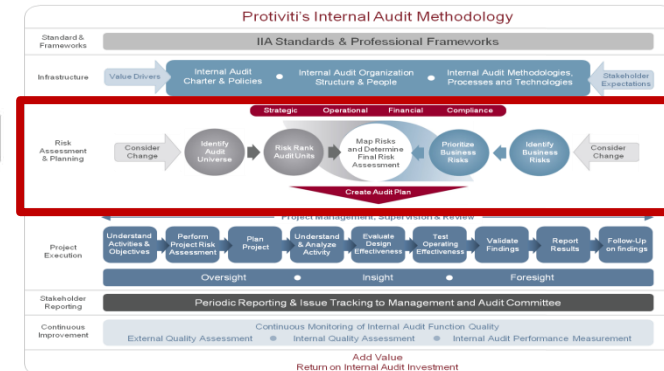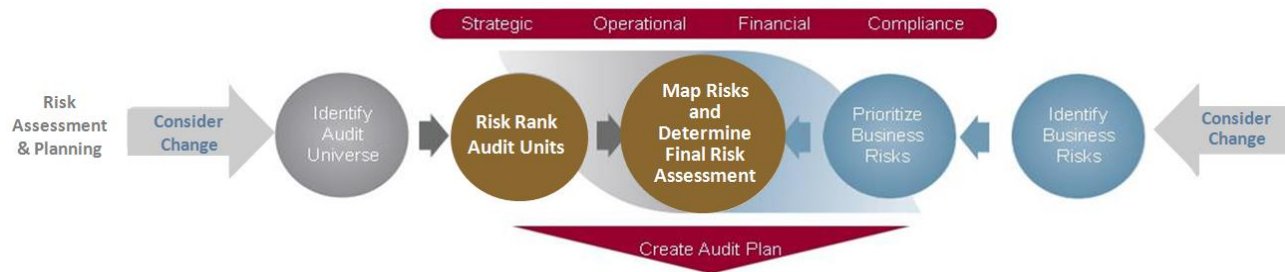
Risk Rank Audit Units

- Protiviti's approach not only takes into consideration our extensive experience and proven methodologies but also places an emphasis on pressing or emerging trends in the industry.

- We shall identify internal audit focus areas. Based upon our discussions with the management, with respect to their individual importance to business performance along with the likelihood of existing control / process issues, we shall rank audit units as high, moderate and low risk areas. These rankings will reflect exposure to risks attached to controls / processes in such audit units.

Map Risks and Determine Final Risk Assessment

- Based on the prioritization of risks and risk ranking audit units, we shall identify the relationship between auditable units and prioritized risks to bring forth an integrated risk assessment.

- Throughout this stage, we will involve appropriate stakeholders to come up with final risk assessment.

- This shall lead to either confirmation of the risk ranks assigned earlier or revision in such rankings.

protiviti
Risk & Business Consulting.
Internal Audit.
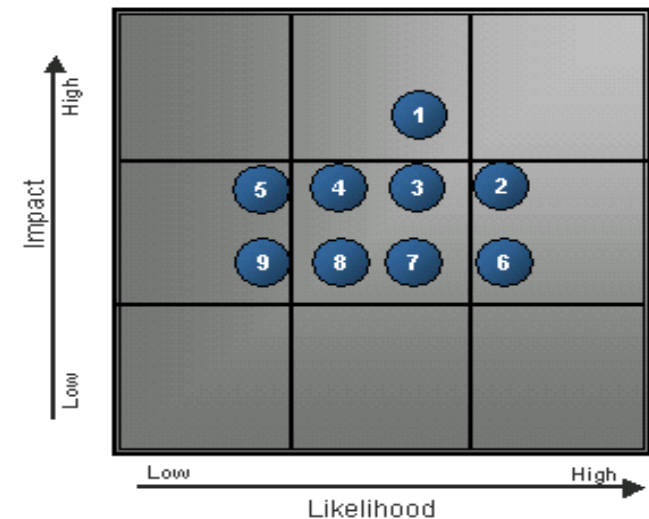
Our Approach – Risk Assessment & Planning (Contd.)
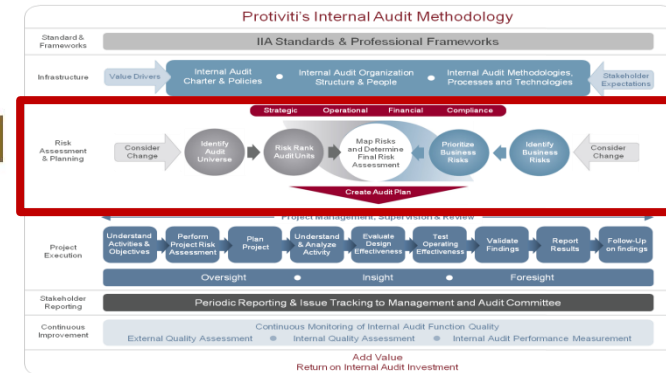
Consider Change

- Our risk based methodology is responsive to stakeholder needs and emerging risks / opportunities in a changing environment. As a part of our ability to respond to change, we consider any new management initiatives and the company's change management process.

- For the portions of the audit universe that generally remain steady, it can be relatively straightforward to identify, understand and evaluate risks. New initiatives, products, processes and technology are typically areas of high risk and may require additional internal audit focus.

protiviti
Risk & Business Consulting.
Internal Audit.
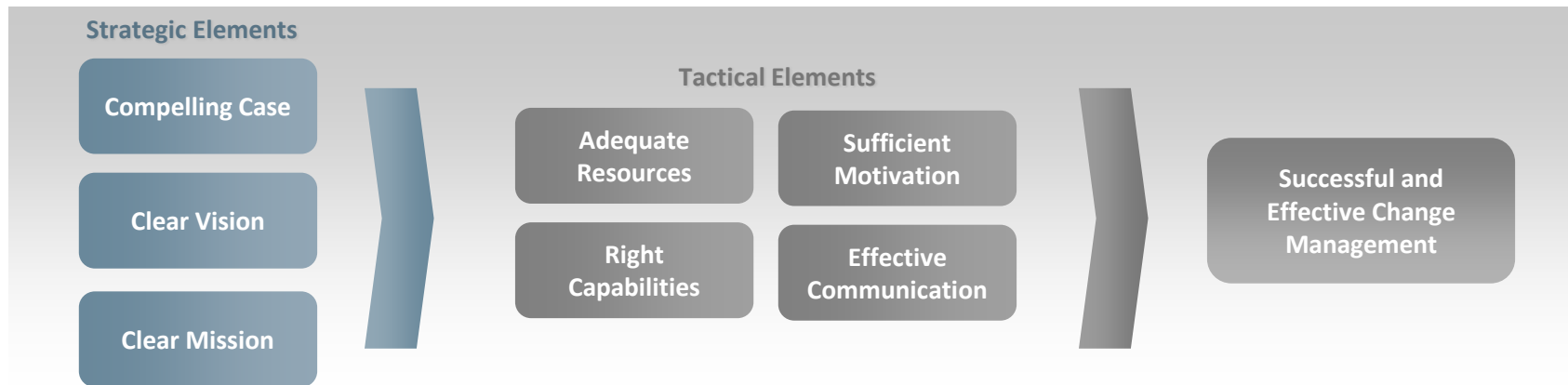
Our Approach – Risk Assessment & Planning (Contd.)

Internal Audit Risk Rating Criteria

Risk Factors	Impact		
	High	**Medium**	**Low**
Materiality / Financial Impact	▪ Adverse impact on assets, annual revenues, costs or profit: 1% or more of total revenue. ▪ Rise in expenses or operational cost: by 20%. ▪ External frauds of significant magnitude. ▪ Significant internal frauds, which may lead to complete change in management / bankruptcy.	▪ Adverse impact on assets, annual revenues, costs or profit: 0.5% to 1% of total revenue. ▪ Rise in expenses or operational cost: by 10% to 20%. ▪ External frauds of moderate magnitude. ▪ Internal frauds of significant magnitude.	▪ Adverse impact on assets, annual revenues, costs or profit: Less than 0.5% of total revenue. ▪ Rise in expenses or operational cost: by 10 % or less. ▪ External Fraud of less magnitude. ▪ Internal Fraud of less magnitude.
Operational	▪ Operational errors affecting the system or resulting in huge losses. ▪ Policies and procedures are non existent or not implemented or completely outdated. ▪ Process not designed to comply with internal Investment policy, Code of conduct and other essential policies. ▪ Systems failures producing loss of records or large inaccuracies in records. ▪ Project delays/cancellations leading to large penalties or losses.	▪ Operational errors in transactions affecting a Department. ▪ Policies and procedures exist but are weak or partially implemented or not updated for a long time. ▪ Process not designed to comply with internal personal dealing policy. ▪ SLAs exist but needs some amendments. ▪ Minor project delays leading to loss. ▪ Project expenses escalating affecting profitability.	▪ Operational errors in transactions affecting a single customer or resulting in duplication of work. ▪ Informal policies and procedures (viz, through emails) exist and updated through informal communication channels. ▪ Process not designed to comply with internal IT policy, Procurement policy etc.
Regulatory	▪ Violations, which may lead to financial penalties from regulatory / statutory bodies.	▪ Violations, which may lead to warnings being issued by regulators / statutory bodies.	▪ Violations of negligible impact.
Reputation	▪ Bad publicity or damage to reputation from a country / regional / global perspective. ▪ Major loss of trustees confidence. ▪ Major loss in confidence of financial institutions.	▪ Bad publicity or damage to reputation from some segments of customers / parties. ▪ Minor loss in confidence of trustees or financial institutions.	▪ Bad publicity or damage to reputation from few customers / parties.

protiviti
Risk & Business Consulting
Internal Audit

Our Approach – Risk Assessment & Planning (Contd.)

Internal Audit Risk Rating Criteria

Impact			
Risk Factors	**High**	**Medium**	**Low**
Customer impact	▪ Dissatisfaction of a large segment of customers or high value customers	▪ Dissatisfaction of few key customers	▪ Dissatisfaction of few low segment customers
Legal	▪ Legal action leading to significant reputation / financial damage	▪ Legal action leading to moderate reputation / financial damage	▪ Legal action leading to minor reputation / financial damage
Information Technology	▪ Confidential information / data loss from server ▪ Breakdown of mission critical IT applications (for example – Great Plains) and/or significant data loss. ▪ System Downtime for 8 hours.	▪ Less confidential information / data loss from server ▪ Breakdown of key IT applications ▪ System Downtime for 4 hours	▪ Information / data loss from server, which are of least importance. ▪ Breakdown of minor IT application (say email system) ▪ System Downtime for 2 hrs.
People	▪ Employee has recently been transferred, no experience or training on current profile. ▪ Earlier track record of disciplinary cases against the Employee.	▪ Employee has recently been transferred, no experience but has undergone training on current profile.	▪ Non- performing employee due to other factors.
Likelihood rating			
Parameters	**Very Likely**	**Likely**	**Less Likely**
The Likelihood of the risk occurring within a 1 year period	10% or more	5% - 10%	Less than 5%

protiviti
Risk & Business Consulting
Internal Audit.

Our Approach – Risk Assessment & Planning (Contd.)

Create Audit Plan

- We shall develop a risk-based internal audit plan based on use the results of risk assessment and changes, if any, occurred since the date of completion of risk assessment. The risk-based internal audit plan will be responsive to the needs of BMMI. This will include a preliminary scope of the audit. The audit plan shall be discussed with and approved by the executive management.

- Work steps carried out in creating an Audit Plan are illustrated below:

protiviti
Risk & Business Consulting
Internal Audit

Our Approach – Project Execution

Understand Activities & Objectives

We will start out scoping audits by understanding the activities of the process (inputs, outputs and systems) and identifying the audit objectives in collaboration with process owners and senior management. This will include agreeing with process owners and senior management about the scope of work and the audit tests to be performed. Once the scope is agreed, we will commence by reviewing policies & organizational structure.

Aligning audit objectives with client objectives ensures that Internal Audit adds value to the client as illustrated below.

Key Audit Objectives

Safeguarding of Assets	Reliability & Integrity of financial and operating information	Effectiveness & Efficiency of operations	Compliance with laws and regulations

Audit objectives are aligned to BMMI's objectives to ensure 'Value Addition'

World Class Internal Audit Service

protiviti
Risk & Business Consulting
Internal Audit

Our Approach – Project Execution (Contd.)
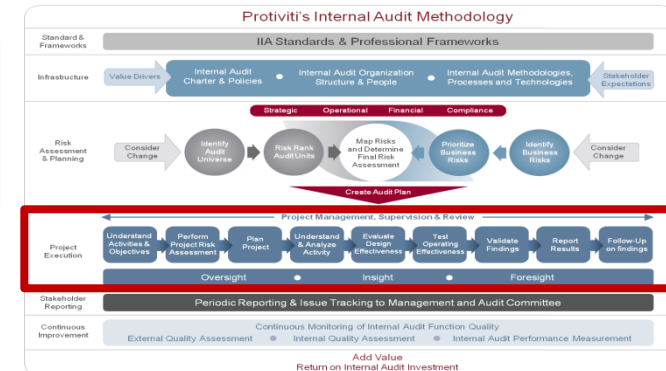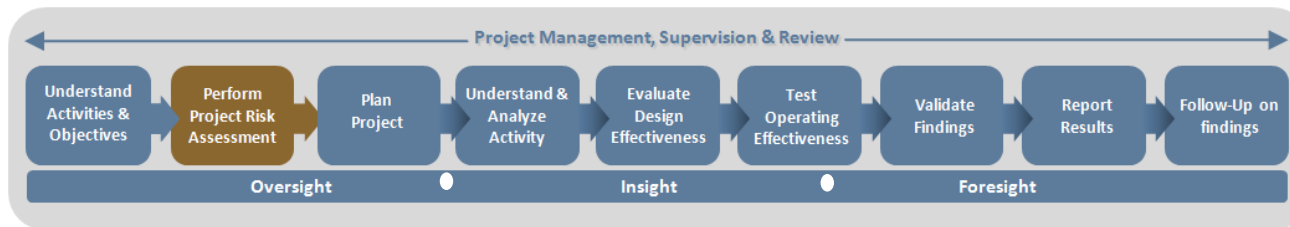
Perform Project Risk Assessment

We will leverage information gathered in the final risk assessment to perform a risk assessment at the project level by understanding the business strategy, objectives and key processes of the area under review and identifying what risks may stand in the way of achieving those business strategies and objectives. In performing the project level risk assessment, we will utilize an RCM (Risk and Control Matrix) which is a table that documents risks, risk assessment, controls, and the type and nature of controls as illustrated below. It helps us to identify control gaps and unmitigated risks.

What can go wrong?

What can prevent it from going wrong or detect it in time?

Risk	Impact	Likelihood	Assessment	Control	Type	Nature	Design Evaluation	Control Recommendation
Unauthorized adjustments are made to the books of accounts.	High	Moderate	High	Reconciliations & Signoffs	Manual	Detective	Adequate	All Adjustment entries should be reviewed before posting in the Finance system by the Head of Accounts.

Type and nature of control

protiviti
Risk & Business Consulting
Internal Audit

Our Approach – Project Execution (Contd.)
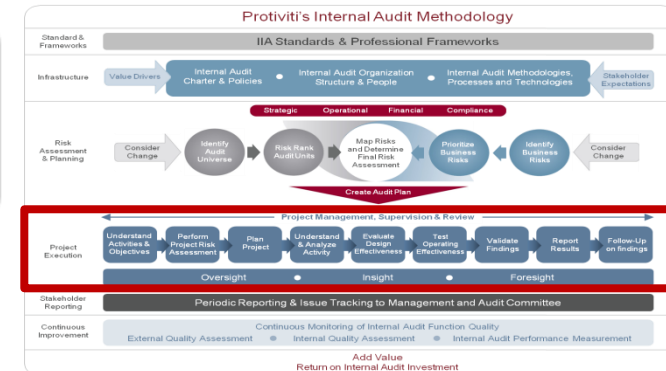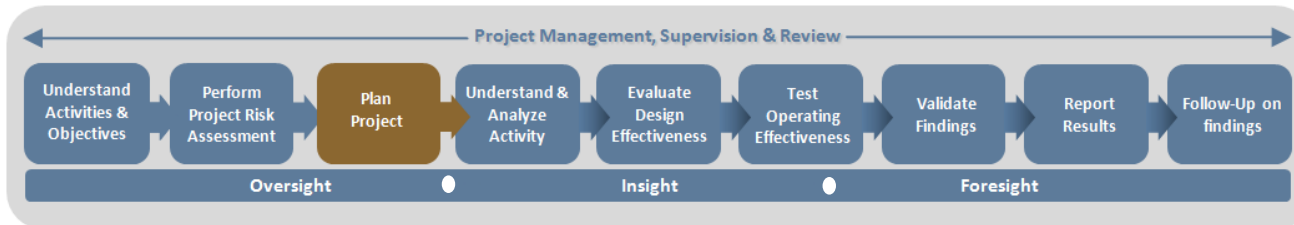
Plan Project

Our planning and scoping documents contain pertinent information on individual department and function. The scope of our audit approach is approved before fieldwork commences. It delineates 'what is in' and 'what is out.' It narrows the audit focus to specific areas of significance (processes, transactions, locations, activities or systems) for the project objectives. We draft the administrative work program at this time and determine the appropriate resources to perform the work.

Key considerations when prioritizing Audit Focus

- Materiality
- Inherit Risk
- Adjusted Risk Level
- Past Audit Results
- Control Effectiveness
- Audit Frequency

Audit Focuses on Specific Areas of Significance

- Business Processes
- Systems
- Transactions
- Activities
- Locations

protiviti
Risk & Business Consulting
Internal Audit
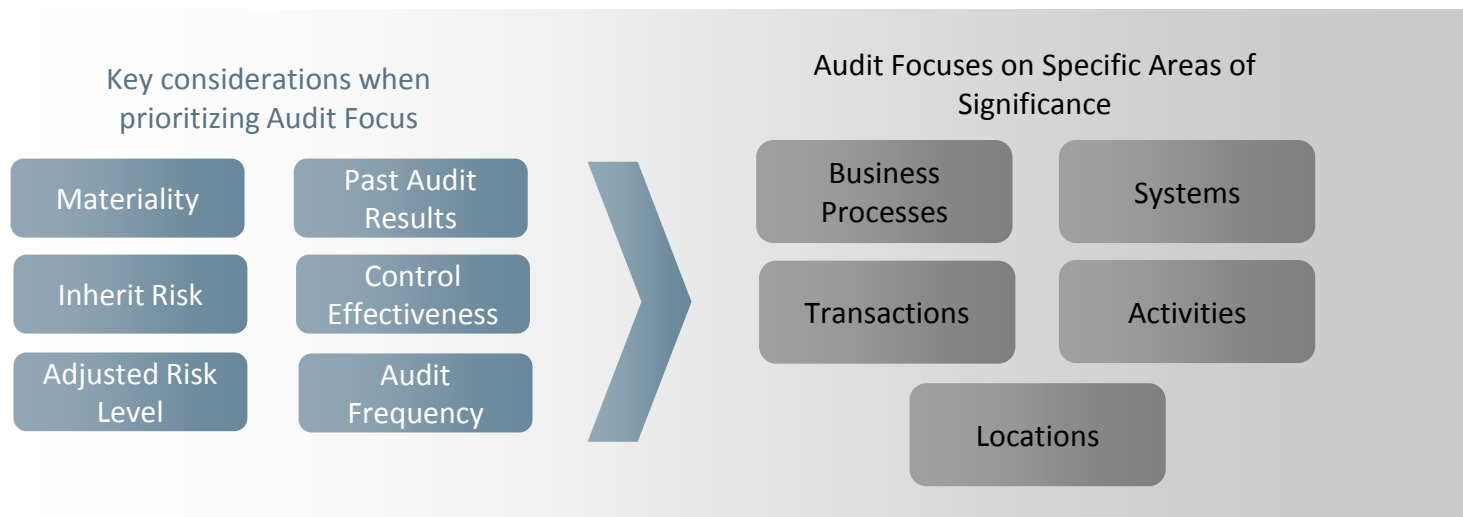
Our Approach – Project Execution (Contd.)
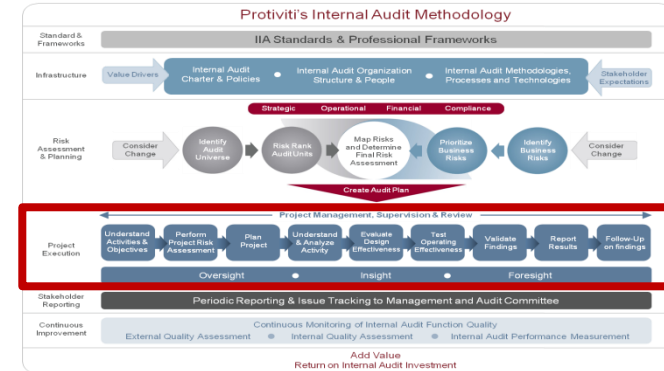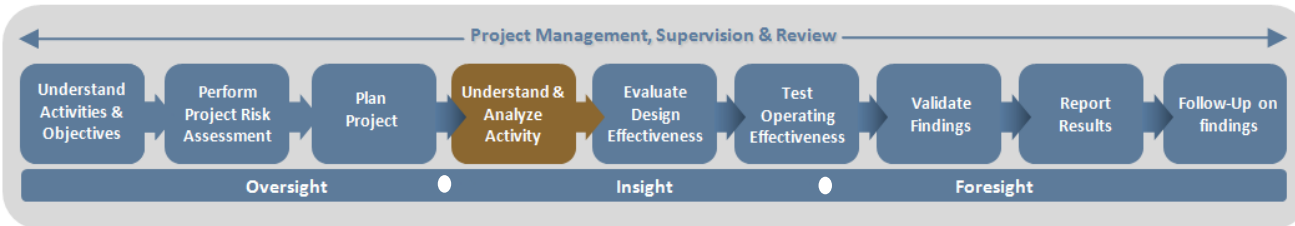
Understand & Analyze Activity

If they are not already documented, we will gain an understanding of the activities being audited. This documentation will be created in the form of flowcharts or memoranda, and we will confirm its completeness and accuracy with process owners.
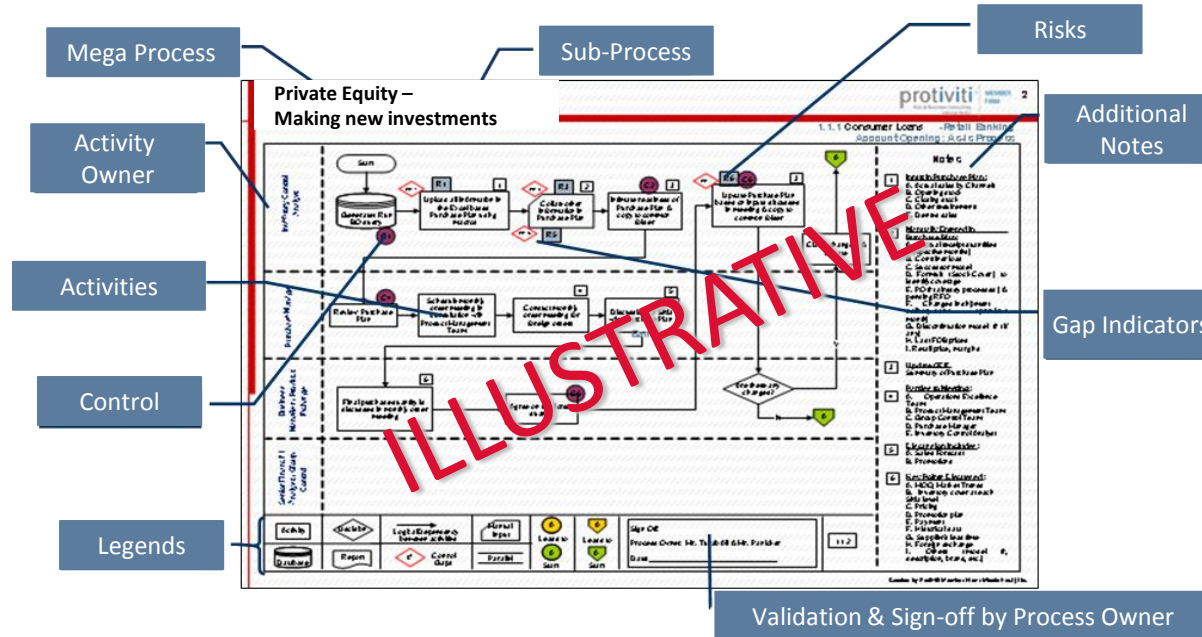
Our Approach – Project Execution (Contd.)
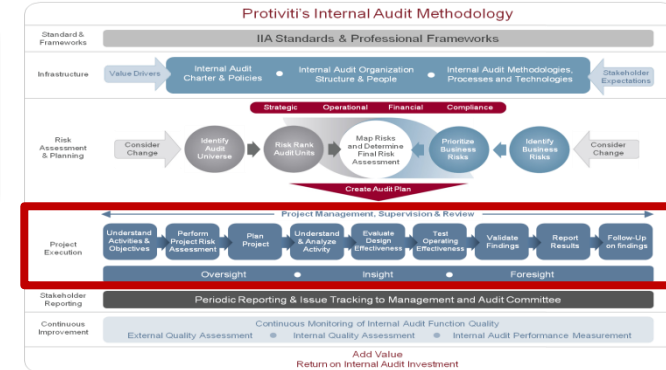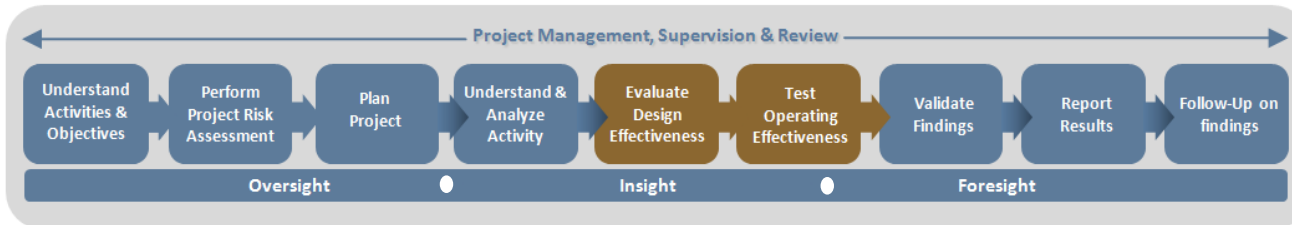
Evaluate Design Effectiveness

We will evaluate the design effectiveness of the collection of controls for each risk before proceeding to testing of controls. In many cases, multiple controls are required to mitigate a risk; in some cases, one control may adequately mitigate multiple risks.

Test Operating Effectiveness

Our work program is further built out when we develop the detailed test plan. We use standard sample sizes to test the operating effectiveness of controls and expand testing on daily controls when the error rate is non-negligible. Testing techniques may include inquiry, observation, inspection and re-performance.

protiviti
Risk & Business Consulting
Internal Audit
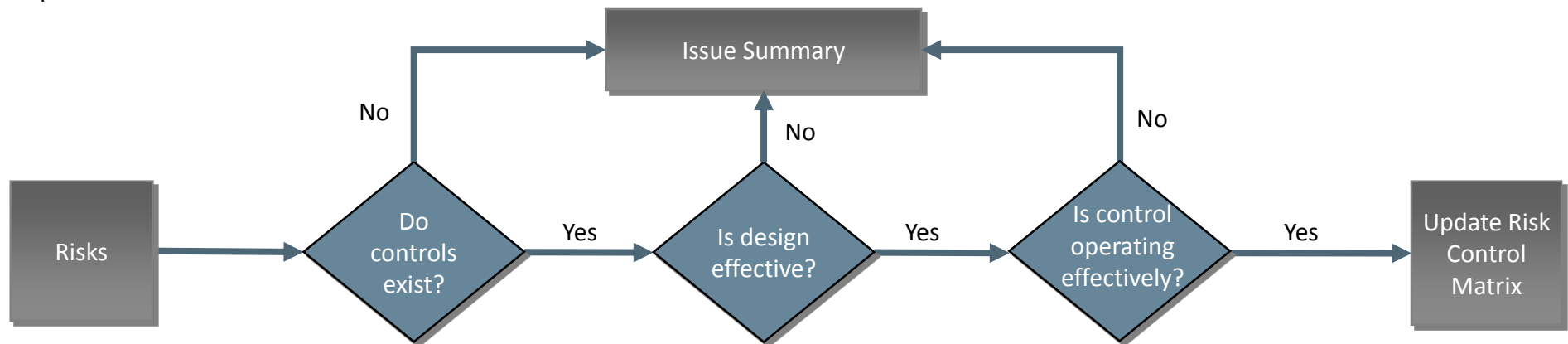
Our Approach – Project Execution (Contd.)

Tests of Controls & Substantive Tests

Once the understanding of internal controls have been obtained and assessment of planned control risks have been made, we will determine the extent of testing controls. We will design appropriate tests of controls and substantive tests of transactions to meet the transaction / function related audit objectives This includes application of requisite audit procedures, representative samples with sufficient size and timing of tests.

Test of Controls

Tests of controls are performed when the assessment of risk of material misstatement at the assertion level includes an expectation that controls are operating effectively. This means it can only be performed when (i) a system exists; and (ii) the system has adequate controls.

We will perform tests of controls to establish whether those controls in the systems are actually functioning properly and effectively so that we can determine whether or not we can rely upon such controls.

Substantive Tests

Substantive tests or substantive procedures are designed to test for error or irregularities that directly affects the correctness of financial statement balances. Substantive tests include:

- Substantive tests of transactions – emphasize the verification of transactions recorded in the journals and then posted in the general ledger.

- Analytical procedures – emphasize the overall reasonableness of transactions and the general ledger balances.

- Test of details of balances – consider the closing balances in the general ledger.
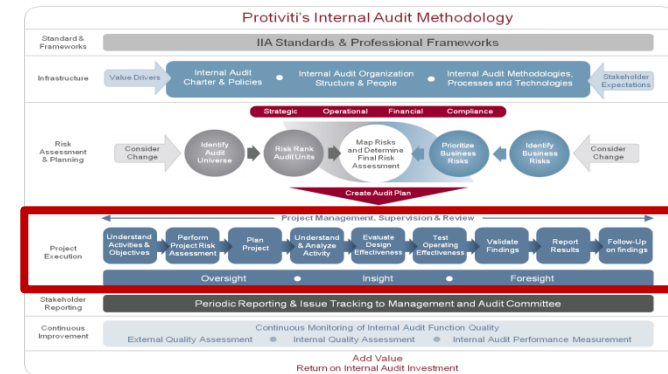
Relationship of Controls with Test of Details and Substantive Analytical Procedures

protiviti
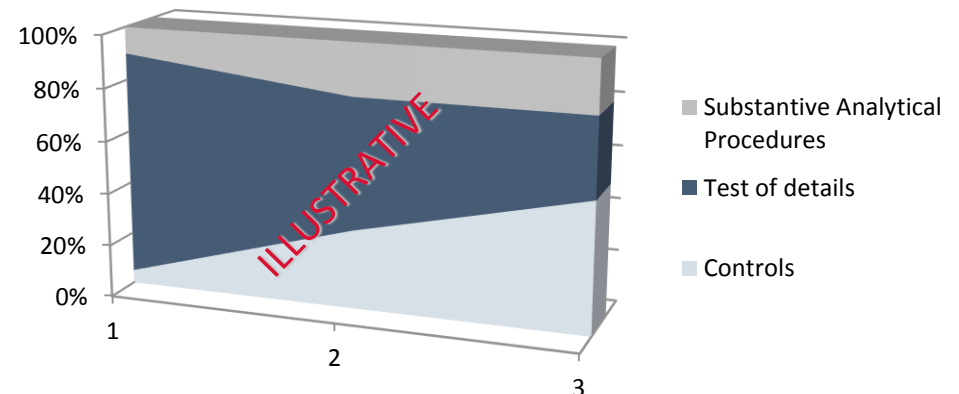
Use of Analytical Procedures

Analytical Procedures would be performed at the planning and testing phases during the engagement.

Planning Phase

Analytical procedures are required in the planning phase to assist in determining the nature, extent, and timing of audit procedures to be applied. It further helps in identifying areas requiring special consideration during internal audit execution.

Testing Phase

Analytical procedures are often performed during the testing phase. These procedures are performed in conjunction with other audit procedures (substantive test of transactions and test of details of balances).

Benchmarks for Analytical Procedures

We develop expectation on account balances, ratios, etc by considering information from:

- Industry data

- Similar prior – period data

- Client – determined expected results

- Auditor – determined expected results

- Expected results using nonfinancial information
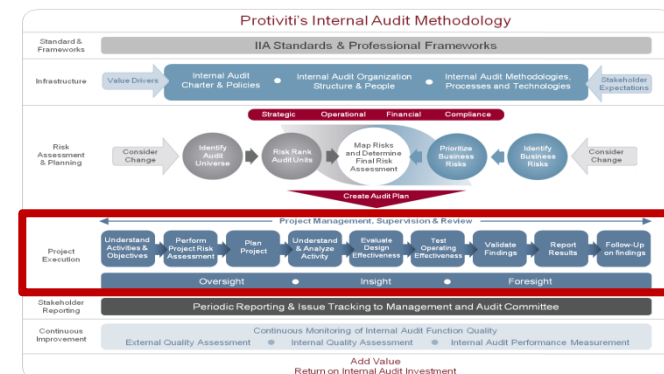
Purpose and Timing of Analytical Procedures

Purpose	Phase	
	Planning	Testing
Understand client's industry and business operations	Primary Purpose	Secondary Purpose
Indicate possible misstatements, if any	Primary Purpose	Secondary Purpose
Reduce volume and extent of detailed tests	Secondary Purpose	Primary Purpose

protiviti
Risk & Business Consulting.
Internal Audit.

Our Approach – Project Execution (Contd.)

Use of CAATs

- We will use Computer Assisted Audit Techniques (CAAT) for analyzing large and complex data.

- Usage of CAAT helps in covering the entire population, thereby providing nearly 100% assurance on high risk areas.

- Data Analytics helps in looking at and summarizing data with the intent to extract hidden predictive information and develop conclusions.

Our Approach – Project Execution (Contd.)


Validate Findings

We will confirm all preliminary audit findings with personnel directly involved in the controls or transactions that gave rise to the preliminary issues in order to obtain agreement on the facts and to determine whether all pertinent factors have been considered.

Report Results

We will communicate factual findings of the design and operational effectiveness of internal controls and provide recommendations for process improvement. Working with management, we will develop action plans and agree on owners and implementation dates.

Follow-Up on Findings

While ownership of implementation belongs to management, we will perform follow-up with management on a timely basis to confirm that the agreed-upon action plans have been implemented.

protiviti
Risk & Business Consulting
Internal Audit
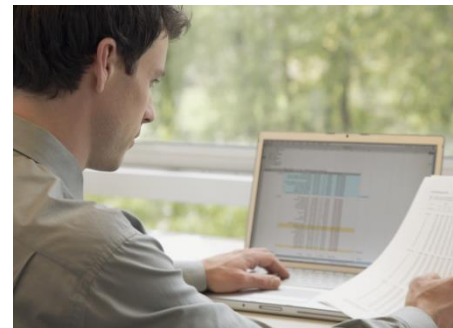
Our Approach – Project Execution (Contd.)
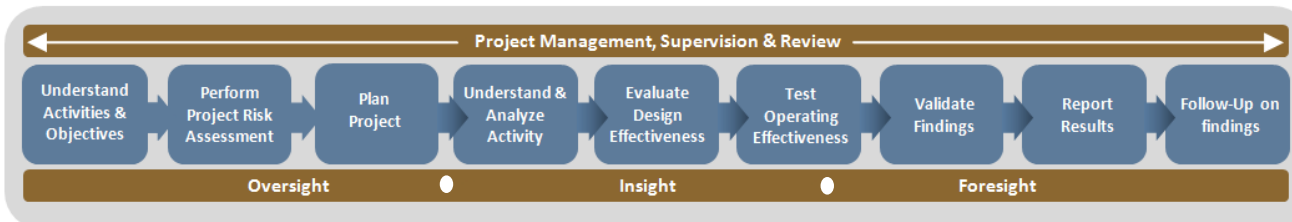


Project Management, Supervision & Review

Protiviti will utilize its proprietary Project Management framework, which is comprehensive, end-to-end, flexible, proven, repeatable, and reliable (Refer to Appendix 2 for an overview of our Project Management Framework).

Oversight, Insight & Foresight

Unique within our methodology is the continuum of "Oversight, Insight and Foresight".

While many internal audit approaches only focus on "Oversight" (i.e. the ability to comply with company policies or internal directives), we believe the value-add aspects of our execution and recommendations are derived from the emphasis to "Insight" (i.e. the ability to operate faster, smarter, or cheaper) and "Foresight" (i.e. the ability to operate in a manner that not only embraces the current time period, but also embraces the future).

In this regard, the "Insight" and "Foresight" components of our methodology differentiates us from our competitors, as our Internal Audit professionals are not only skilled at diagnosing problems and formulating solutions to these problems, but are also skilled in identifying process improvements and executing process re-engineering projects.
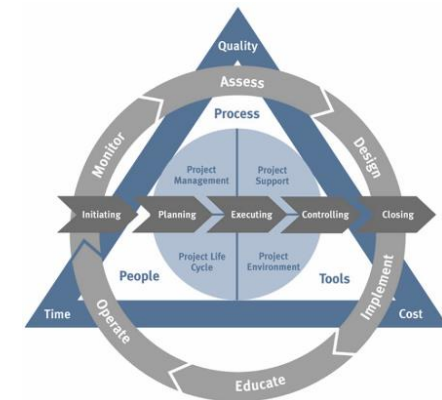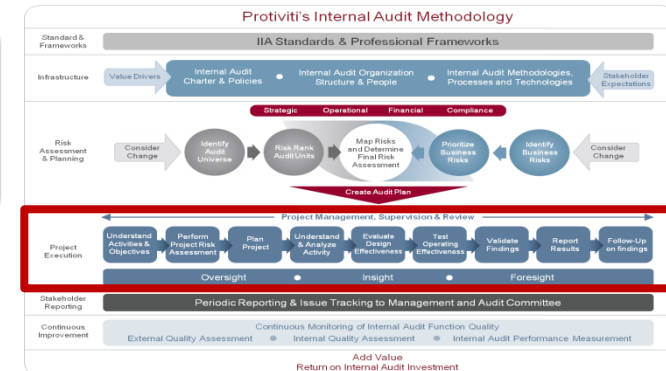

Protiviti's Project Management Framework

protiviti
Risk & Business Consulting
Internal Audit

Our Approach – Stakeholder Reporting

Stakeholder Reporting

> **Periodic Reporting & Issue Tracking to Management and Audit Committee**

Periodic Reporting & Issue Tracking to Management and Audit Committee

We will report periodically to the senior management regarding the performance of internal audit relative to its plan, and report significant risk exposures and control issues, corporate governance issues and other matters. We will work the management to create a customized reporting solution that allows users to best understand relevant information on issues related and opportunities for control / process enhancement.
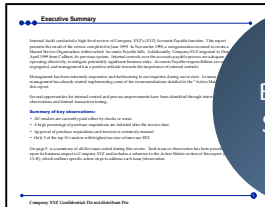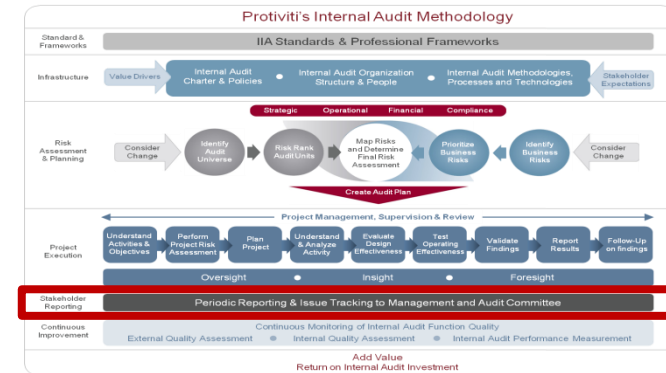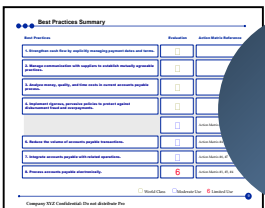

Executive Summary — A high-level overview of the engagement, including scope of the work, audit objectives, and the actual work performed.
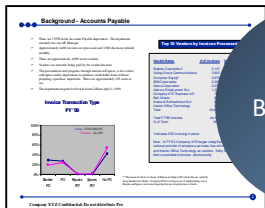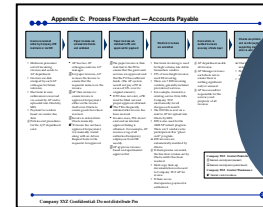
Background — Information on the process being reviewed, including process background, statistics, and graphs.
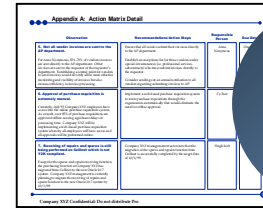
Internal Control Scorecard — An evaluation of the practices and internal controls.

Process Flowcharts — Graphical representation of the process being reviewed which identifies key internal control points, Best Practices, and internal control/ process improvement opportunities.

Action Matrix — Discussion of key issues identified during the engagement, including recommendations that have been agreed upon by management with committed implementation timeframes.
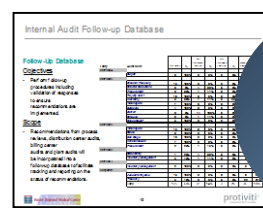
Follow-up Database — Formalized process for performing follow-up reviews to ensure recommendations are implemented.

protiviti
Risk & Business Consulting.
Internal Audit.

Sample Deliverable – Internal Audit Report

1

Investcorp

Bahrain Administration

Internal Audit Report

April 2013

INVESTCORP

protiviti® | MEMBER FIRM
Risk & Business Consulting. Internal Audit.

Powerful Insights. Proven Delivery.®

2

Contents

Our Vision:
Be recogni... global firm for internal audit, risk and business consulting services.

Our Mission:
Constantly improve how organizations create value by helping clients IDENTIFY and SOLVE critical business problems.

Our Core Values:
- professional
- productive
- proactive
- objectiviti
- creativiti
- integriti
- qualiti
- responsibiliti

protiviti MEMBER FIRM

3

Executive Summary

Internal Audit conducted a high-level review of Company XYZ's (XYZ) Accounts Payable function. This report presents the result of the review completed in June 1999. In November 1998, a reorganization occurred to create a Shared Service Organization within which Accounts Payable falls. Additionally, Company XYZ migrated to Oracle in April 1999 from Cullinet, its previous system. Internal controls over the accounts payable process are adequate, if operating effectively, to mitigate potentially significant business risks. Accounts Payable responsibilities are adequately segregated, and management has a positive attitude towards the importance of internal controls.

Management has been extremely responsive and forthcoming to our inquiries during our review. In many cases management has already started implementing some of the recommendations detailed in the "Action Matrix" section of this report.

Several opportunities for internal control and process improvements have been identified through interviews, observations and limited transaction testing.

Summary of key observations:
- All vendors are currently paid either by checks or wires.
- A high percentage of purchase requisitions are initiated after the invoice date.
- Approval of purchase requisitions and invoices is extremely manual.
- Only 3 of the top 10 vendors with highest invoice volume use EDI.

On page 5 is a summary of all the issues noted during this review. Each issue or observation has been prioritized based upon its business impact to Company XYZ and includes a reference to the Action Matrix section of the report, pages 13-15), which outlines specific action steps to address each issue/observation.

Company XYZ Confidential: Do not distribute Pro

4

Background – Accounts Payable

...ff in the Accounts Payable department. The department currently has one AP Manager.

- Approximately 4,400 invoices are processed and 1,500 checks are printed monthly.
- There are approximately 4,500 active vendors.
- Vendors are currently being paid by the vendor due date.
- The procurement card program, through American Express, is for certain colleagues and/or departments to purchase small dollar items without preparing a purchase requisition. There are approximately 125 cards in use.
- The department migrated to Oracle from Cullinet April 1, 1999.

Top 10 Vendors by Invoices Pro...

Vendor Name	# of invoices	Value ('000s)
Staples Corporation*	5,147	$1,464
Vialog Group Communications	3,605	$396
Computer Supply*	2,676	$4,721
IBM Corporation	2,387	$22,232
Xerox Corporation	2,076	$1,494
Adecco Employment Svc	1,217	$911
Company XYZ Business Int'l	748	$33,338
Bell Atlantic	698	$341
Aramark Refreshment Svc*	631	$103
Interim Office Technology	629	$462
Total	19,814	$65,454
Total FY'99 Invoices	44,450	$356,609
% of Total	45%	18%

*indicates EDI invoicing in place

Note: In FY'00, Company XYZ began using Kelly Services as a national provider of temporary services thus eliminating Adecco and Interim Office Technology as vendors. Kelly Services submit their consolidated invoices electronically.

Invoice Transaction Type FY '99

Value - $356,609,291
Volume - 44,450

(Blanket PO, PO, Repairs PO, Spares PO, No PO)

** The reason for the low volume of Repairs and Spares PO is that they are currently being handled in Cullinet. Company XYZ is in the process of implementing a new Repairs and Spares system and migrating the matching function to Oracle.

Company XYZ Confidential: Do not distribute Pro

5

Best Practices Summary

Best Practices	Evaluation	Action Matrix
1. Strengthen cash flow by explicitly managing payment dates and terms.	☐	
2. Manage communication with suppliers to establish mutually agreeable practices.	☐	
3. Analyze money, quality, and time costs in current accounts payable process.	☐	
4. Implement rigorous, pervasive policies to protect against disbursement fraud and overpayments.	☐	
	☐	Action Matrix #3
6. Reduce the volume of accounts payable transactions.	☐	Action Matrix #4
7. Integrate accounts payable with related operations.	☐	Action Matrix #6, #7
8. Process accounts payable electronically.	6	Action Matrix #1, #3, #4

☐ World Class   ☐ Moderate Use   6 Limited Use

Company XYZ Confidential: Do not distribute Pro

6

Appendix A: Action Matrix Detail

Observation	Recommendations/Action Steps	Responsible Person	
5. Not all vendor invoices are sent to the AP department. Per Anne Nonymous, 65%-70% of vendor invoices are sent directly to the AP department. Other invoices are sent to the requestor or the requestor's department. Establishing a central point for vendors to send invoices would not only allow more effective monitoring and visibility of invoices but also increase efficiency in invoice processing.	Ensure that all vendors submit their invoices directly to the AP department. Establish an exceptions list for those vendors under special circumstances (i.e. professional services, subcontracts) who must submit invoices directly to the requestor. Consider sending out an annual notification to all vendors regarding submitting invoices to AP.	Anne Nonymous	Ongoing
6. Approval of purchase requisition is extremely manual. Currently, only 93 Company XYZ employees have access into the online purchase requisition system. As a result, over 85% of purchase requisitions are approved offline causing significant delays in processing time. Company XYZ will be implementing a web-based purchase requisition system whereby all employees will have access and all approvals will be performed online.	Implement a web-based purchase requisition system to route purchase requisitions through the organization automatically that would eliminate the need for offline approval.	Cy Furr	9/30/99
7. Receiving of repairs and spares is still being performed on Cullinet which is not Y2K compliant. Except for the spares and repairs receiving function, the purchasing function at Company XYZ has migrated from Cullinet to the new Oracle 10.7 system. Company XYZ management is currently planning to migrate the receiving of repairs and spares function to the new Oracle 10.7 system by 10/1/99.	Company XYZ management must ensure that the migration of the spares and repairs function from Cullinet is successfully completed by the target date of 10/1/99.	Hugh Izzit	1H '00

Company XYZ Confidential: Do not distribute Pro

ILLUSTRATIVE

protiviti®
Risk & Business Consulting. Internal Audit.

Phases in the Report Writing Process

3 C's for Drafting Report

CONCISE
- Identify key finding(s) and prioritize.

COMPLETE
- Determine what types of information (and how much) are needed to support each key finding.

CLEAR
- Consistently apply standards for coherent written communication.
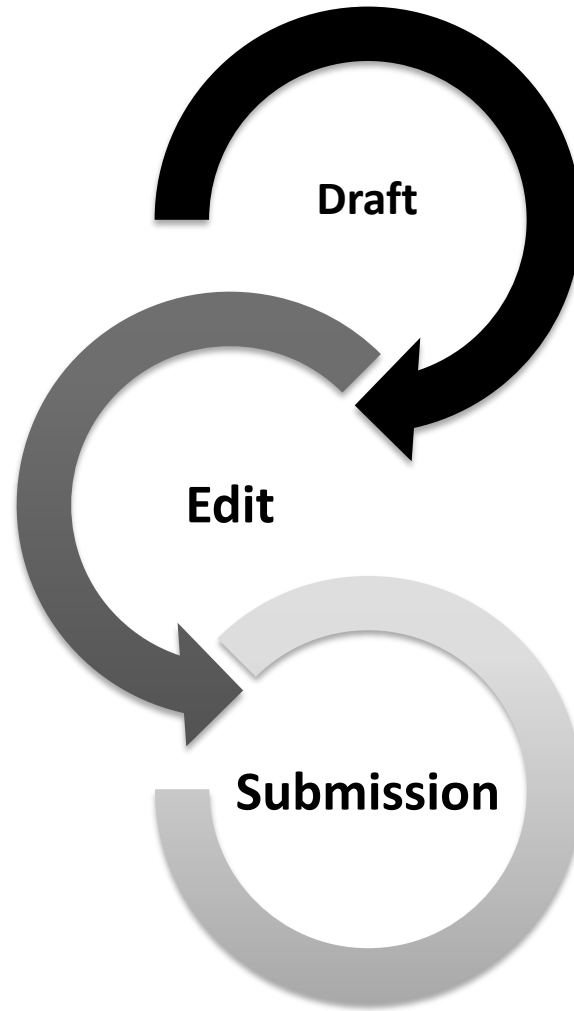
protiviti
Risk & Business Consulting.
Internal Audit.
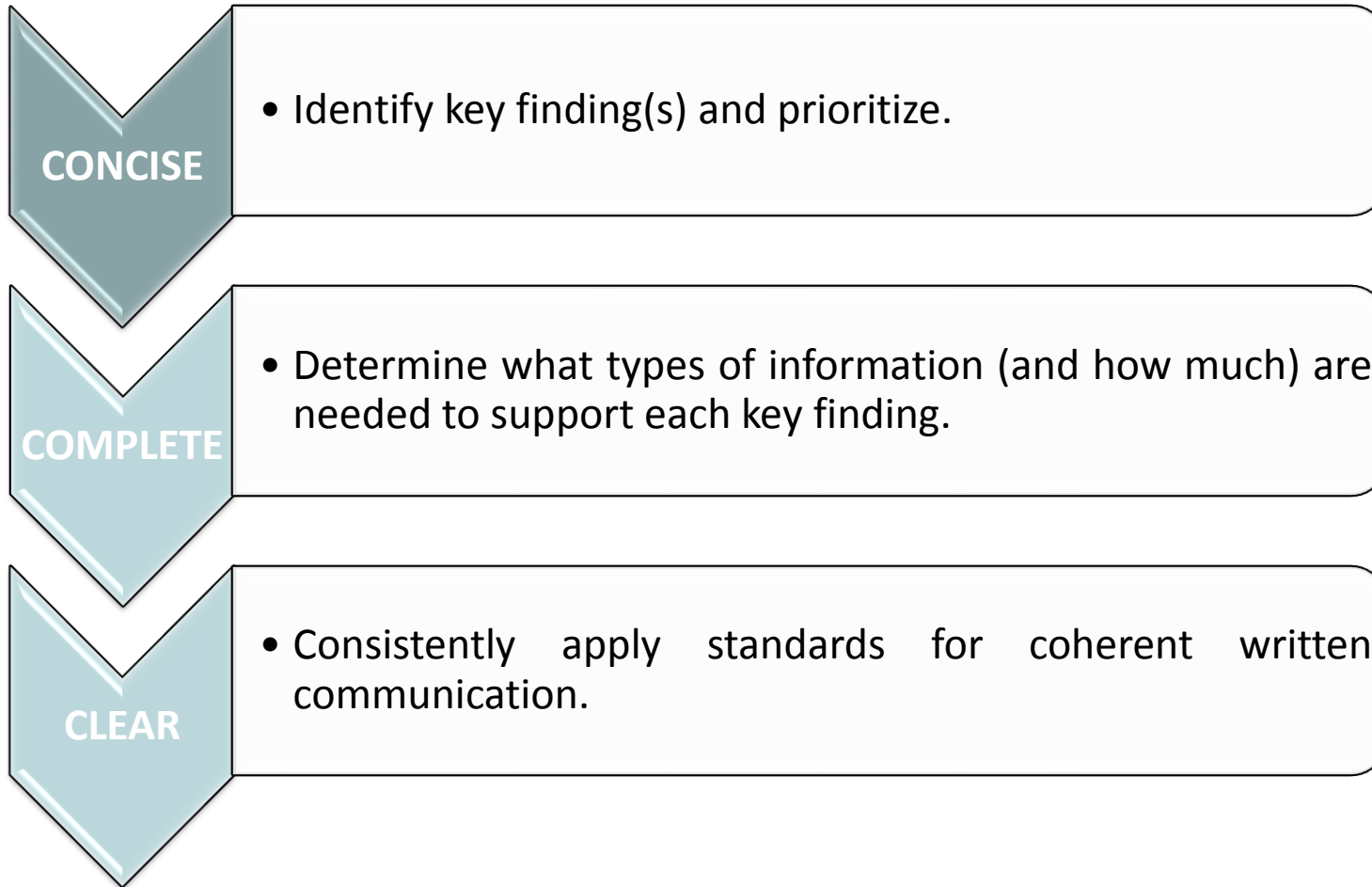
Drafting a 'Finding'? (Contd.)

Criteria	What should be the case?
Condition	What is the current case?
Cause	What is the reason for the current case?
Consequence (Effect)	What is the impact?
Corrective Action (Recommendation)	What should precisely be done to reach the 'should be' scenario? • Be specific rather than being general • These should be actionable rather than theoretical

Tip:

- *Consider the '5' Wives and A Husband rule while drafting the issue - Who, When, Why, What, Where and How*

protiviti
Risk & Business Consulting.
Internal Audit.

Issue Grading

Issues are graded on a three point scale - Red, Orange and Green. Red signifies the highest risk and Green the lowest risk. The description and level of management which needs to address the issues are given below:

Level	Description	Issue requires involvement of one or more of
🔴	A fundamental objective is not met or there is a critical weakness in controls. Resolution would help avoid a potentially critical negative impact involving loss of material assets, reputation, critical financial information, or ability to comply with the most important laws, policies, or procedures. **Resolution Timeline : X Weeks**	❑ MD/ CEO ❑ Executive Committee ❑ Divisional Director/ Director
🟠	An important objective is not met or there is a significant weakness in controls. Resolution would help avoid a potentially significant negative impact on the unit's assets, financial information, or ability to comply with important laws, policies, or procedures. **Resolution Timeline : X+A Weeks**	❑ Divisional Director/ Director ❑ Head of Division ❑ Department Managers
🟢	Objectives are mostly met but further enhancement of the control environment is possible. Resolution would help improve controls and avoid problems in the unit's operations. **Resolution Timeline : X+B Weeks**	❑ Head of Division ❑ Department / Section Managers

protiviti
Risk & Business Consulting
Internal Audit.

Report Grading

Reports are graded on a three point scale - Satisfactory, Needs Improvement or Unsatisfactory. The description of each grading is given below:

Satisfactory	No important control weaknesses were noted, but some needed control enhancements and other issues were noted that need to be addressed within a reasonable time frame.
Needs improvement	One or more important weaknesses were noted, which, if not corrected promptly, could result in unacceptable levels of risk.
Unsatisfactory	One or more critical weaknesses and/or a preponderance of important issues were noted that exposes the organization to an unacceptable level of risk.

Report Grading Matrix

The report grading is assigned based on the number of issues and the rating of the issues. The matrix for the assignment of the report grading is given below:

Grading	Rating	Definition
Satisfactory	🟥	No observations
	🟧	Less than 20% of the total observations
	🟩	
Needs Improvement	🟥	Less than 20% of the total observations
	🟧	Less than 65% of the total observations
	AND	
	🟥	Less than 70%
	🟧	
Unsatisfactory	🟥	= or > than 20% of the total observations
	🟧	= or > than 65% of the total observations
	AND	
	🟥	= or > than 70%
	🟧	

protiviti
Risk & Business Consulting.
Internal Audit.

Our Approach – Continuous Improvement

Continuous Monitoring of Internal Audit Function Quality

We adopt the following mechanism to ensure continuous monitoring of internal audit function quality:

External Quality Assessment

When we act as the outsourced internal audit function, we encourage organizations to conduct an external quality assessment review at least once every five years in accordance with the IIA Standards. For the last several years, we have engaged an outside third party to review and report on the design effectiveness of the Protiviti Way as it relates to conformance with the IIA Standards.

Internal Quality Assessment

Outside of our project management and supervision process over individual projects, we also assure quality on our audits by performing Annual Internal Quality Assessment reviews of selected Internal Audit engagements across Protiviti. These operational and compliance-based reviews test adherence to Protiviti's policies that govern the planning, conduct and reporting on all work performed.
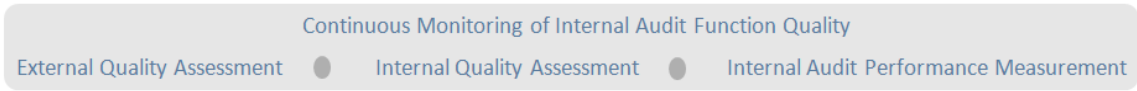
Internal Audit Performance Measurement

We assist organizations in the development of metrics to monitor the performance of the internal audit function.

protiviti
Risk & Business Consulting
Internal Audit
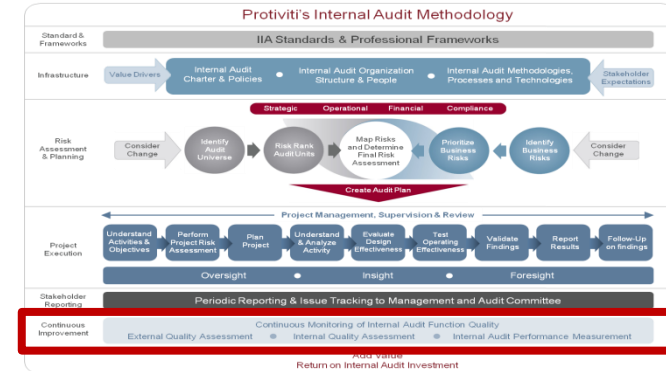
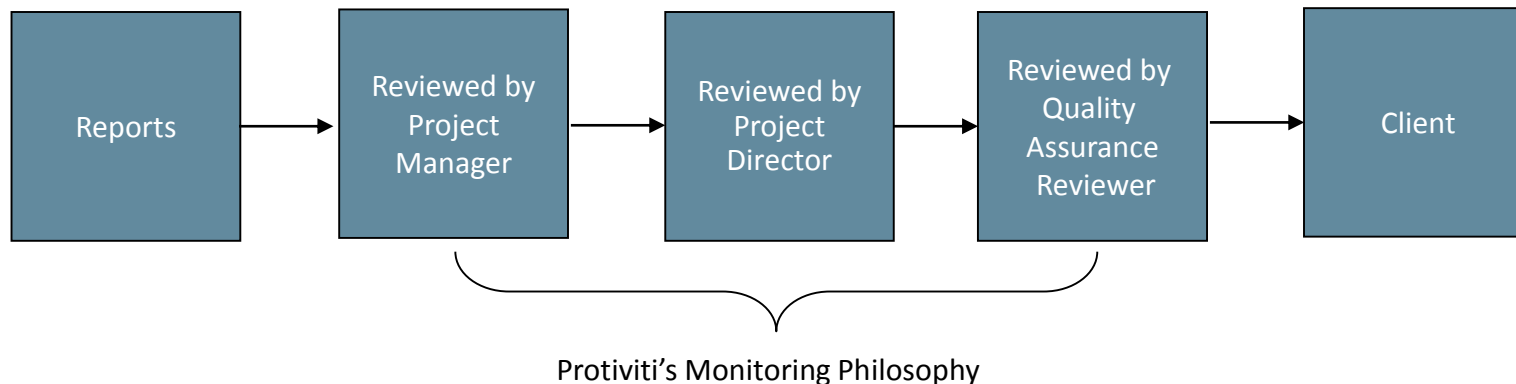# Our Approach – Continuous Improvement (Contd.)

We perform the following continuous monitoring on the quality of the internal audit function:

Each of our projects goes through a 3-tier Quality Assurance Review as detailed below:

- the first level of review is performed by the Project Manager;

- the second level of review is performed by the Project Director; and

- the third level of review is performed by a Quality Assurance Reviewer.
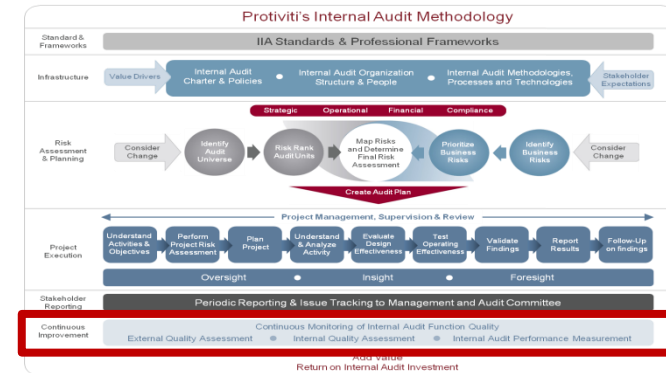
In accordance with the 3-tier Quality Assurance Process the engagement team includes a Quality Assurance Reviewer, a Project Director and a Project Manager. The Project Director will have overall responsibility for managing our relationship with the client as well for the assignment as he will be leading the team. The Project Director's principal task is to advise the client on all significant business issues arising from the assignment. The Project Manager is responsible for managing the assignment on a day-to-day basis, resolving problems and developing the solutions. In addition the Quality Assurance Reviewer provides comprehensive oversight of the overall quality of the services provided as well as the deliverables to ensure that they are in line with the highest of standards.

Reports → Reviewed by Project Manager → Reviewed by Project Director → Reviewed by Quality Assurance Reviewer → Client

Protiviti's Monitoring Philosophy

protiviti
Risk & Business Consulting
Internal Audit

Murtuza Kachwala
Managing Director
Telecom, Media & Entertainment

murtuza.kachwala1@protiviti.co.in
Contact no. +91 9833 015 334
Web: www.protiviti.in

protiviti
Risk & Business Consulting.
Internal Audit.