

*Powerful Insights.
Proven Delivery.™*



Standards on Internal Audit (SIA) Importance of Standards & Compliance

ICAI Bhawan, BKC

30th July, 2016

Table of Contents

Introduction to SIA issued by ICAI

What is Internal Audit as per SIA?

Detailed SIA

Introduction to SIA



The **Council of the Institute of Chartered Accountants of India** 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.

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.

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

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*.

compliance
Internal risk Audit
independent add value effective improve
efficient assurance objective

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

But, How well do you know the standards?



SIA issued by ICAI



SIA 1 - Planning on Internal Audit



SIA 2 - Basic principles Governing Internal Audit



SIA 3 - Documentation



SIA 4 - Reporting



SIA 5 - Sampling



SIA 6 - Analytical Procedures



SIA 7 - Quality Assurance in Internal Audit



SIA 8 - Terms of Internal Audit Engagement



SIA 9 - Communication with Management



SIA 10 - Internal Audit Evidence



SIA 11 - Consideration of Fraud in an Internal Audit



SIA 12 - Internal Control Evaluation



SIA 13 - Enterprise Risk Management



SIA 14 - Internal Audit in an Information Technology Environment



SIA 15 - Knowledge of the Entity and its Environment



SIA 16 - Using the Work of an Expert



SIA 17 - Consideration of Laws and Regulations in an Internal Audit



SIA 18 - Related Parties

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

SIA 1

Planning an Internal Audit

SIA 1 – Planning an Internal Audit

The basic **objective** of this SIA is to **establish standards and provide guidance in respect of planning** an Internal Audit and **helping in achieving the objectives of an Internal Audit function**.

The internal auditor should, in consultation with those charged with governance including the audit committee, develop and document a plan for each internal audit engagement to **help him conduct the engagement in an efficient and timely manner**.

Adequate planning **ensures that appropriate attention is devoted to significant areas of audit, potential problems are identified and that the skills and time of the staff are appropriately utilised**.

Knowledge of entity's business helps to identify areas of special focus and priorities for smooth running of business. Ideally, such knowledge can be obtained from following resources:

- Past experience
- Understanding basic documents e.g. MOA, AOA, minutes of various meetings, etc.
- Discussion with staff and management
- Policy and Procedure's Manual
- Visit to entity's Plant and Accounts department

The **internal auditor** should, **in consultation** with those charged with governance including the **audit committee**, **develop and document a plan** for each internal audit engagement to help him conduct the engagement in an efficient and timely manner. He should also assess the client expectations as to the assurance level on different aspect of entity's operations and controls.

In addition, the internal **audit plan** should also **reflect the risk management strategy of the entity**.

Risk Management - Internal Audit Activity must evaluate the effectiveness of risk management process

Responsibilities of Internal Audit towards Managing the Risk

- Evaluate risk exposures relating to the organization's governance, operations, and information systems.
- Evaluate the potential for the occurrence of fraud.
- Address risk consistent with the engagement's objectives.
- Refrain from assuming any management responsibility.

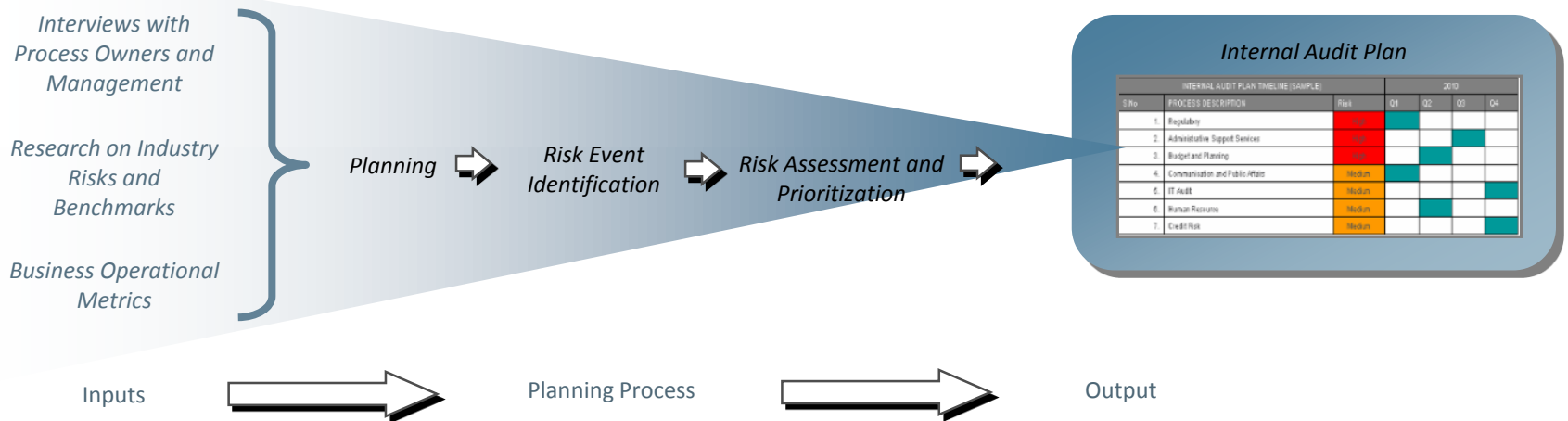


Planning – Chief Audit Executive (CAE) must establish a risk - based plan to determine the priorities of the internal audit activity

What all are the Responsibilities of CAE?

- To develop a risk – based plan.
- To study the organization’s risk management framework, if framework does not exist CAE uses his/her own judgment of risk after considering the input of senior management and board.
- To review and adjust the plan, as necessary, in response to changes in the organization’s business, risks, operations, programs, systems and controls.

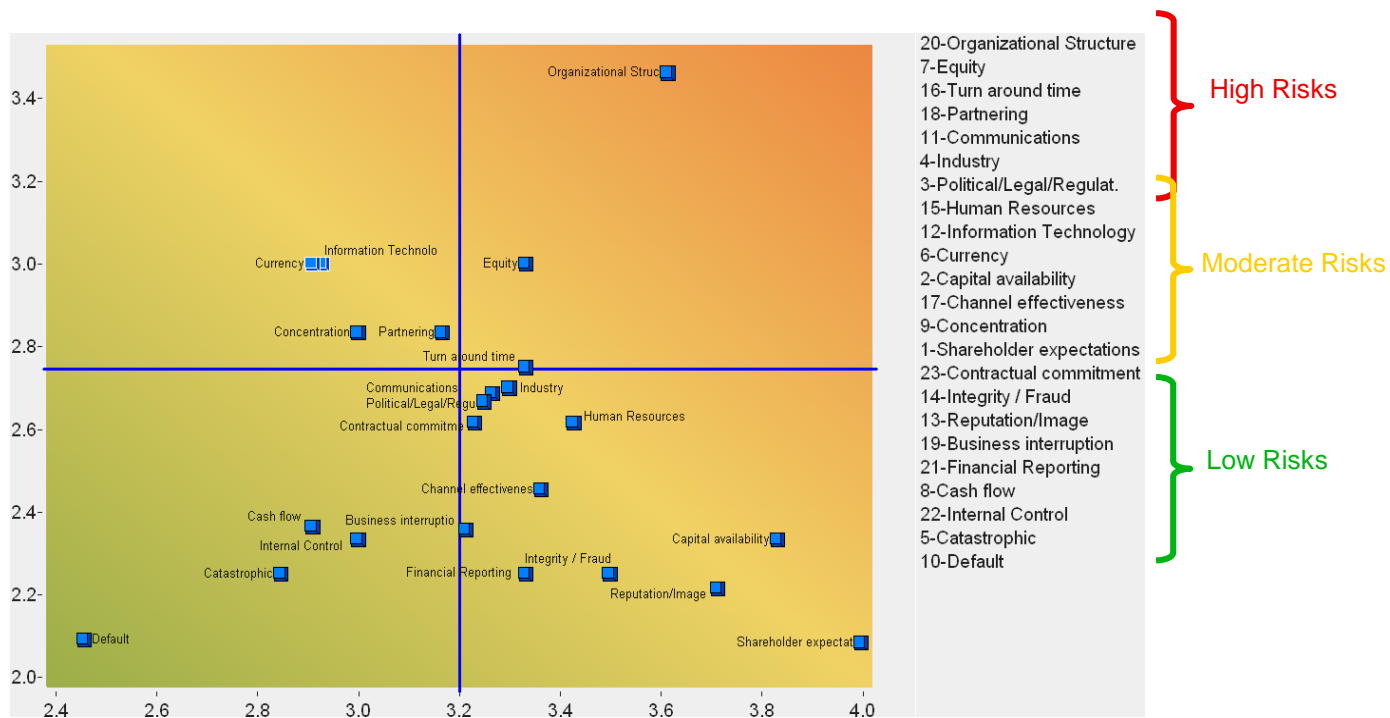
Cycle of Internal Audit Plan



Planning Considerations

What should an internal auditor consider while planning the engagement?

- Identify significant risks to the activity, its objectives, resources and operations.
- The objectives of the activity are being reviewed.



Engagement Resource Allocation

- To perform the engagement on time and effectively the internal auditors should allocate only those resource who meet the nature and complexity of the engagement.

Engagement Work Program

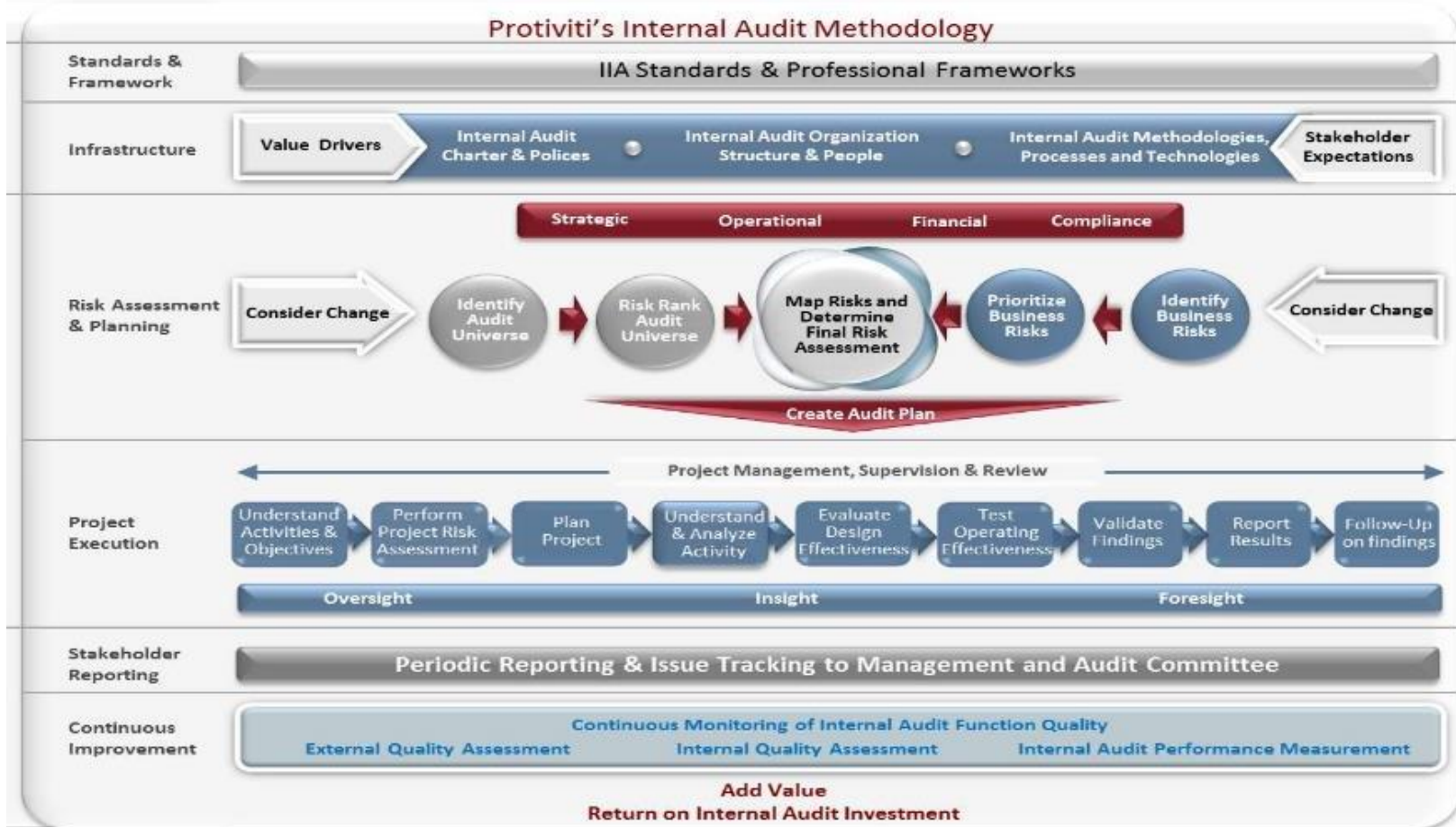
- Work program includes procedures for identifying, analyzing, evaluating, and documenting information during the engagement.
- Work program should be approved prior to its implementation & any adjustments approved promptly.

Planning Process of Internal Audit



Our Internal Audit Methodology

Our Internal Audit services are supported by a consistent, field tested 'risk-based' methodology derived from our experiences on hundreds of internal audits and is consistent with the International Standards for the Professional Practice of Internal Auditing.



SIA 2

Basic Principles Governing Internal Audit

SIA 2 – Basic Principles Governing Internal Audit

Internal auditor should adhere to the basic principles governing an internal audit. Such *basic principles* are as under:



Internal Control (IC) and Risk Management (RM) Systems are heart and brain of Internal Audit.

Internal Auditor should:

- Understand the IC and RM framework.
- Assess its adequacy.
- Review its adequacy periodically.
- Perform risk based audit.

Risk based Audit adopts following flow cycle:



In Internal Audit, what is Independence and Objectivity?

Independence:

- Having freedom to report on control weakness in the organization.
- E.g.: If the Internal Audit Department Manager is reviewing the payroll system and also auditing it on the same time this is where his/her Independence is compromised.

Objectivity:

- Being neutral and unbiased while performing Audit Activity.
- E.g.: Internal Audit Staff does not report a material weakness since the auditor is a close personal friend and might get fired, then the Internal Audit Activity is compromised and not being objective.

Due Professional Care, Skills & Competence

- 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*.

Proficiency - Internal Auditor must have adequate knowledge, skills to perform their individual responsibilities

What proficiency should Internal auditor possess for better functioning of Internal Audit?

- Internal Auditor should have a professional qualification, such as CIA (Certified Internal Auditor), CA (Chartered Accountant), CPA (Certified Public Accountant) and CISA (Certified Information Systems Auditor).
- Internal auditors must have sufficient knowledge to evaluate the risk of fraud or have Fraud Related qualifications (Certified Fraud Examiner CFE).
- Internal auditors must have sufficient knowledge of key risks and controls of all processes.



SIA 3

Documentation

SIA 3 – Documentation

Paragraph 10 of SIA 2, Basic Principles Governing Internal Audit, states that:

“The internal auditor should document matters, which are important in providing evidence that the audit was carried out in accordance with the Standards on Internal Audit and support his findings or the report submitted by him.”

“Internal audit documentation” means the record of audit procedures performed, including audit planning as discussed in **SIA 1, Planning an Internal Audit**, relevant audit evidence obtained and conclusions the auditor reached.

Internal Audit (IA) documentation should record the **internal audit charter, the internal audit plan, the nature, timing and extent of audit procedures performed, and the conclusions drawn from the evidence obtained**. If internal audit is outsourced, the documentation should contain a copy of the internal audit engagement letter, containing the Terms & Conditions of appointment.

To ensure the reliability and effectiveness of documentation, following requirements should be given adherence:

- IA documentation should be **sufficiently complete** and detailed for an internal auditor to **obtain an overall understanding** of the audit.
- All the significant matters which require **exercise of judgment**, together with the internal auditor’s conclusion thereon should be included in the **IA documentation**.
- The documentation prepared by the internal auditor should be such that enables an experienced **internal auditor** (or a reviewer), **having no previous connection** with the internal audit to **understand the audit plan**, terms of reference, scope of work, audit procedures, significant issues and conclusion.
- The **extent of documentation** is a matter of **professional judgment** since it is neither practical nor possible to document every observation, finding or conclusion in the IA documentation.
- The **IA file** should be **assembled** within **60 days after the signing** of the internal audit report. Assembly of the IA documentation file is only an administrative process and does not involve performance of any new audit procedures or formulation of new conclusions. Changes may be made to the audit documentation file only if such changes are administrative in nature.

Internal Audit Charter

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.

SIA 4 Reporting

What is a Report?

End product of your work

Final deliverable



Image of your own self and the Organization

The only tangible outcome of your work

Differentiator

SIA 4 – Reporting

Objective:

- To **review and assess the analysis drawn from internal audit evidence** obtained as the basis for his **conclusion** on the efficiency and effectiveness of systems, processes and controls including items of financial statements.
- Report should **clearly express significant observations, suggestions/recommendations** based on the policies, processes, risks, controls and transaction processing taken as a whole and management's responses.
- To **facilitate communication** and ensure that recommendations presented in final report are practical from the point of view of implementation, the internal auditor should **discuss the draft with the entity's management prior to issuing the final report.**

Scope Limitation:

When there is a **limitation on the scope** of internal auditor's work, the internal **auditor's report should describe** the limitation.

Restriction on Usage & Report Circulation:

The internal auditor should state in the Report that the same is to be used for the intended purpose only as agreed upon and the circulation of the Report should be **limited to the recipients** mentioned in the **Report Distribution List.**

Basic Elements in IA report

- [Redacted]
- Title
- Addressee
- Report Distribution List
- Period of Coverage of report
- Opening / Introductory paragraph
- Objective paragraph
- Scope Paragraph
- Executive Summary
- Observations, Findings
- Management Comments
- Action Taken Report
- Date of the Report
- Place of Signature
- Internal Auditor's signature with Membership Number

Recommendation #n.

Title	Recommendation / Acceptance
<p>How should the process look like? What should happen?</p> <p>#n.1 The Issue here: #n.1 The Issue</p> <p>What is lacking in this particular case? What were the test results? What is the risk / conclusion of above gap? What is the effect to Organisation?</p>	<p>Recommendation</p> <p>#n.1 + #n.3 Management should ensure that / Management should consider to...</p> <p>#n.2</p> <p>Management Comments</p> <p>Agreed, statement about actions to be taken</p> <p>Not agreed, reason why risk should be accepted</p>

Responsibility	Name	Risk	Due date
----------------	------	------	----------

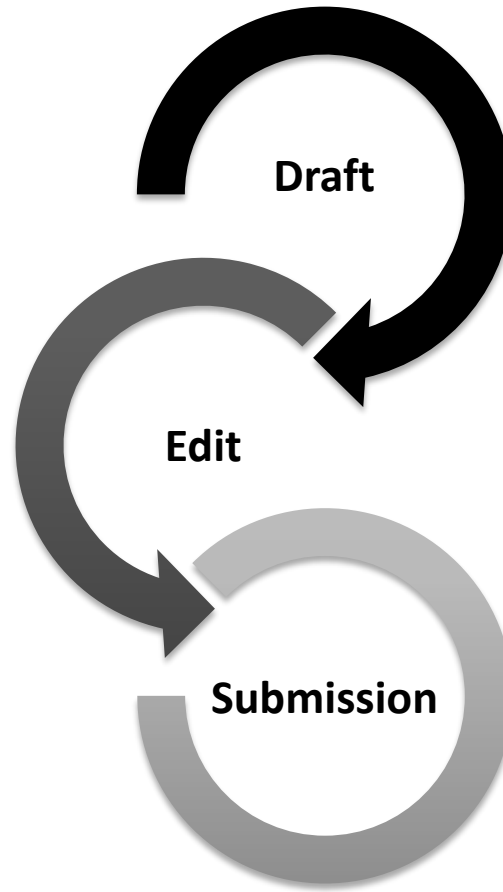
Areas covered	Ref.
---------------	------

F - fundamental control weakness requiring shareholder disclosure
 H - high control risk, requiring immediate attention
 M - medium control risk requiring timely attention
 L - low risk, management should address based on prioritisation

Report Template

1. Issue	RISK (S)	H						
<p><u>Background:</u></p> <p><u>Observation:</u></p> <div data-bbox="622 472 1170 951" style="border: 2px dashed red; padding: 10px; transform: rotate(-15deg); text-align: center; color: red; font-weight: bold; font-size: 2em;">ILLUSTRATIVE</div>		ROOT CAUSE (S)						
MANAGEMENT COMMENTS		<table border="1" style="width: 100%;"><tr><td style="width: 33%;">Process</td><td style="width: 33%;">People</td><td style="width: 33%;">Technology</td></tr><tr><td></td><td style="text-align: center;">✓</td><td></td></tr></table>	Process	People	Technology		✓	
Process	People	Technology						
	✓							
<ul style="list-style-type: none">• Agreed / Not agreed <p>Responsibility: _____</p> <p>Due Date: _____</p>	Recommendations							

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.

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? <ul style="list-style-type: none">• <i>Be specific rather than being general</i>• <i>These should be actionable rather than theoretical</i>

Tip:

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

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
	<p>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.</p> <p style="text-align: center;">Resolution Timeline : X Weeks</p>	<ul style="list-style-type: none"> <input type="checkbox"/> MD/ CEO <input type="checkbox"/> Executive Committee <input type="checkbox"/> Divisional Director/ Director
	<p>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.</p> <p style="text-align: center;">Resolution Timeline : X+A Weeks</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Divisional Director/ Director <input type="checkbox"/> Head of Division <input type="checkbox"/> Department Managers
	<p>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.</p> <p style="text-align: center;">Resolution Timeline : X+B Weeks</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Head of Division <input type="checkbox"/> Department / Section Managers

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%

SIA 5 Sampling

SIA 5 – Sampling

Introduction:

When using either **statistical or non-statistical sampling methods**, the internal auditor should **design and select an audit sample**, perform audit procedures thereon and **evaluate sample results** so as to **provide sufficient and appropriate audit evidence** to meet the objectives of the internal audit engagement unless otherwise specified by the client.

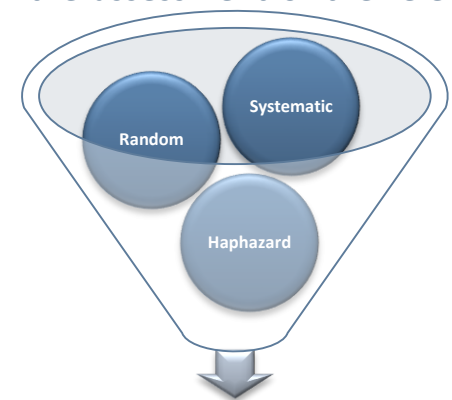
Important points to be noted:

- When designing an audit sample, internal auditor should consider specific audit objectives, the **population** from which internal auditor wishes to **sample and the sample size**.
- When determining the sample size, internal auditor should **consider sampling risk, tolerable error** and the **expected error**.
- **Sample items should be selected** in such a way that the sample can be expected to be **representative of the population**. This requires that all items or sampling units in the population have an opportunity of being selected.

Finally, the internal auditor should **evaluate the sample results** to determine whether the assessment of the relevant characteristics of the population is **confirmed or whether it needs to be revised**.

While there are a number of **selection methods**, three methods commonly used are:

- **Random selection and use of CAATs**
- **Systematic selection**
- **Haphazard selection**



Sample selection

protiviti®

Sampling – Test of Controls (TOC)

The following are some factors which the internal auditor shall consider when determining the sample size required for tests of controls (TOC). These factors need to be considered together assuming the internal auditor does not modify the nature or timing of TOC or otherwise modify the approach to substantive procedures in response to assessed risks.

Factors to be considered by an Internal Auditor	Effect on Sample Size
An increase in the extent to which the risk of material misstatement is reduced by the operating effectiveness of controls	Increase
An increase in the rate of deviation from the prescribed control activity that the internal auditor is willing to accept	Decrease
An increase in the rate of deviation from the prescribed control activity that the internal auditor expects to find in the population	Increase
An increase in the internal auditor's required confidence level	Increase
An increase in the number of sampling units in the population	Negligible effect

Note:

1. Other things being equal, the more the internal auditor relies on the operating effectiveness of controls in risk assessment, the greater is the extent of the internal auditor's tests of controls, and hence the sample size is increased.
2. The lower the rate of deviation that the internal auditor is willing to accept, the larger the sample size needs to be.

Frequency of Control Activity and Sample Size

The following guidance related to the frequency of the performance of control may be considered when planning the extent of tests of operating effectiveness of manual controls for which control deviations are not expected to be found. The internal auditor may determine the appropriate number of control occurrences to test based on the following minimum sample size for the frequency of the control activity dependant on whether assessment has been made on a lower or higher risk of failure of the control.

Factors to be considered by an Internal Auditor	Minimum Sample Size	
	Risk of Failure	
	Lower	Higher
Annual	1	1
Quarterly (including period-end, i.e. +1)	1+1	1+1
Monthly	2	3
Weekly	5	8
Daily	15	25
Recurring manual control	25	40

Note: Although +1 is used to indicate that the period-end control is tested, this does not mean that for more frequent control operations the year-end operation cannot be tested.

SIA 6

Analytical Procedures

SIA 6 – Analytical Procedures

The internal auditor should apply analytical procedures as the risk assessment procedures at the planning and overall review stages of the internal audit.

“**Analytical procedures**” means the analysis of **significant ratios and trends**, including the resulting investigation of fluctuations and relationships in both **financial and non-financial data** which are inconsistent with other relevant information or which deviate significantly from predicted amounts.

Factors to be considered in determining the extent to which the analytical procedures should be used:

- The significance of the area being examined.
- The adequacy of the system of internal control.
- The availability and reliability of financial and nonfinancial information.
- The precision with which the results of analytical procedures can be predicted.
- The availability and comparability of information regarding the industry in which the organization operates.
- The extent to which other auditing procedures provide support for audit results.

Investigating Unusual Items or Trends:

When analytical procedures **identify significant fluctuations** or inconsistencies, the internal auditor should investigate and **obtain adequate explanations and appropriate corroborative evidence**. The examination and evaluation should include inquiries of management and the application of other auditing procedures until the internal auditor is satisfied that the results or relationships are sufficiently explained. **Unexplained results** or relationships may be **indicative of a potential error, irregularity, or illegal act**. Results or relationships that are not sufficiently explained should be communicated to the appropriate levels of management. The **internal auditor may recommend appropriate courses of action**, depending on the circumstances.

Need for Data Analytics

Trends in the Industry – Indicators for growing need for analytics to be used as an audit technique

Increasingly many CAE's are seeing the need to enhance their skill set towards data analytics, which indicates they have taken significant notice of the risks posed by increasing automation, transaction sizes and data volumes.

IIA Standards

- **Standard 1220.A2** – “In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques”

Protiviti Surveys

- Key findings of IA capability needs survey 2011 indicate Data analysis tools for statistical analysis and data manipulation is one of the key needs cited by most participants.

Competitors Past Surveys

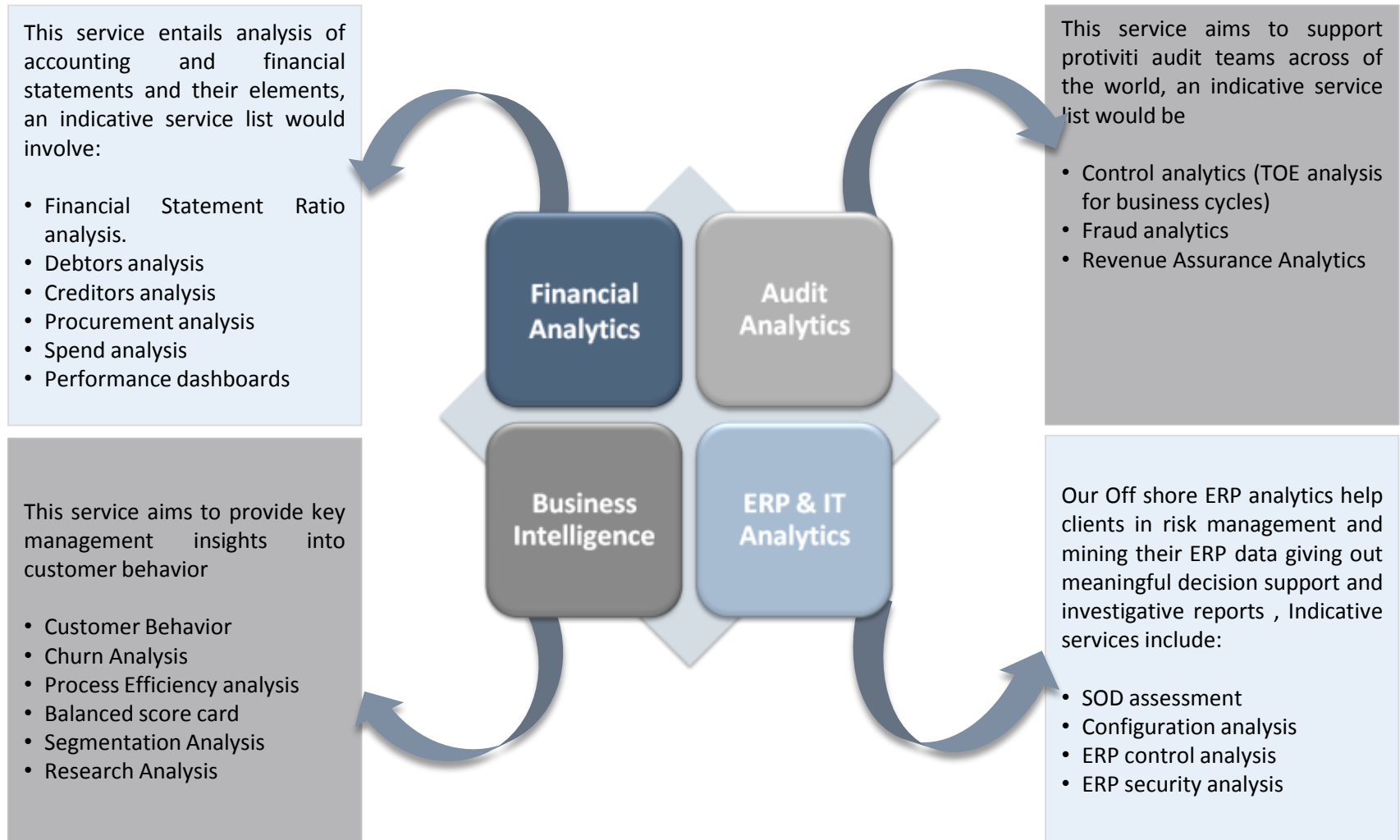
- IT Auditors represent only 10% of Internal Audit headcount – 2007 Survey
- Over half of Internal Audit functions have implemented continuous auditing through technology – 2007 Survey. Over 90% of Internal Audit functions use data analytics, however, less than half consider these skills as pervasive – 2007 Survey

Best Practice

- IIA's GTAG No. 3 on Continuous Auditing states “the power of continuous auditing lies in the intelligence and efficient continuous testing of controls. By changing their approach auditors will develop a better understanding of the business environment and risks to the company.”

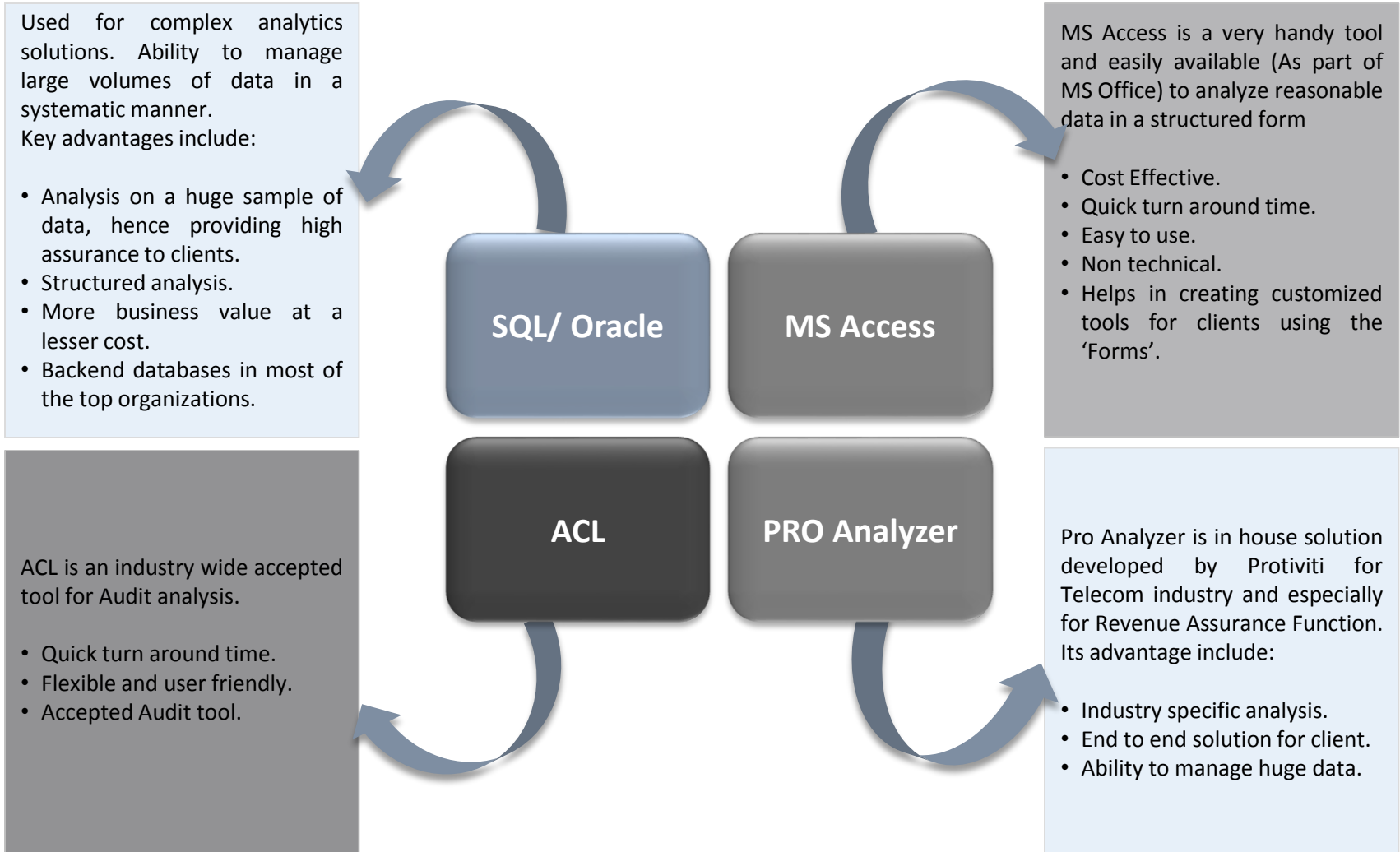
Types of Data Analytics

What analytics can be done? - elaborated



Tools used for Data Analytics

Brief summary of some key tools that may be used more often for analytics



SIA 7

Quality Assurance in Internal Audit

SIA 7 – Quality Assurance in Internal Audit

Objective:

A system for assuring quality in internal audit should **provide reasonable assurance** that the internal auditors **comply with professional standards, regulatory and legal requirements**, so that the reports issued by them are appropriate in the circumstances.

In order to ensure compliance with the professional standards, regulatory and legal requirements, and to achieve the desired objective of the internal audit, a person within the organization should be entrusted with the responsibility for the quality in the **internal audit, whether done in-house or by an external agency**.

In case of In-house internal audit or a firm carrying out internal audit, the person entrusted with the responsibility for the quality in internal audit should ensure that the system of quality assurance **includes policies and procedures** addressing each of the following elements:

- Leadership responsibilities for quality in internal audit
- Ethical requirements
- Acceptance and continuance of client relationship and specific engagement, as may be applicable
- Human resources
- Engagement performance
- Monitoring

This standard also provides extensive knowledge about the **internal quality reviews, external quality reviews and communicating the results thereof**.

Frequency: Internal Quality Review - **Ongoing** & External Quality Review - **At least once in three years**

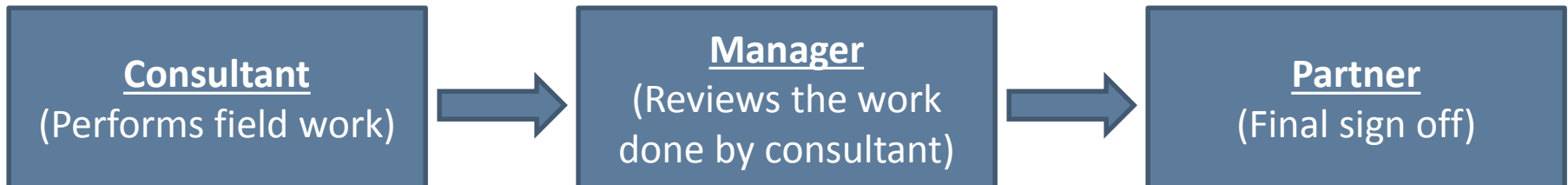
Internal Assessments

What is an Internal Assessment?

- Ongoing monitoring of the performance of the internal audit activity.
- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.
- Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

IPPF =

Mandatory
Non mandatory Strongly recommended



External Assessment (Must be conducted at least once every three years by a qualified, independent team from outside the organization appointed by the board)

Sample External Assessment Reports - Table of Comment

- Qualified assessor team should have:
- The Professional practice of internal auditing
 - The External assessment process
 - Relevant experience
 - Independent person free of conflict of interest

INDEPENDENT VALIDATION STATEMENT

INTRODUCTION.....

 BACKGROUND

 SCOPE AND PURPOSE.....

 SUMMARY AND CONCLUSION

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES.....

 Internal Review Observations.....

 Observation 1 - Standard 1300 – Quality Assurance and Improvement Program.....

 Observation 2 - Standards 2000 – Managing the Internal Audit Activity and 2100 – Nature of Work

 External Review Observations.....

 Observation 3 - Standard 2210.A1 – Engagement Objectives

 Observation 4 - Standards 2110 – Governance and 2120 – Risk Management.....

 Observation 5 - Standards 2440 – Disseminating Results and 2500 – Monitoring Progress .

 Observation 6 - Standard 2340 – Engagement Supervision

APPROVALS

EXHIBIT A

SIA 8

Terms of Internal Audit Engagement

SIA 8 – Terms of Internal Audit Engagement

Objective:

To provide guidance for the clarity on the terms of the internal audit engagement between the internal auditors and auditee which is essential for inculcating professionalism and avoiding misunderstanding as to any aspect of the engagement.

The internal auditor and the auditee should **agree on the terms of the engagement before commencement.**

The terms of the engagement should contain a statement in respect of the scope of the internal audit engagement. It should **clearly delineate the broad areas of function of internal audit like evaluating internal controls, review of business process cycle controls, risk management and governance.**

The terms of engagement should clearly mention that the internal auditor would not, ordinarily, be involved in the preparation of the financial statements of the auditee. It should also be made clear that the internal audit would not result in the expression, by the internal auditor, of an opinion, or any other form of assurance on the financial statements or any part thereof of the auditee.

The terms of the engagement should clearly mention the responsibility of the auditee vis-à-vis the internal auditor.

Ideally, terms of engagement should clearly define the **Scope, Authority, Responsibility, Confidentiality, Limitations, Reporting requirements, Compensation & Compliance with standards.**

Withdrawal from the engagement:

In case the internal auditor is unable to agree to any change in the terms of the engagement and/ or is not permitted to continue as per the original terms, he should withdraw from the engagement and should consider whether there is an obligation, contractual or otherwise, to report the circumstances necessitating the withdrawal to other parties.

Engagement Objectives

- Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review.
- Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures.
- Consulting engagement objectives must address governance, risk management, and control processes.

Engagement Scope

- The scope of engagement must be precised and clear.
- It must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

Specimen Engagement Letter

Private and Confidential

Mr. _____
Vice President - Internal Audit
ABC Limited
Plot No. 141 A, Sector 18,
Mumbai -400001

Date: 30th July, 2016

Dear Mr. _____,

Engagement letter: Internal Audit at ABC Limited, Mumbai

The purpose of this letter (the "Engagement Letter") together with Appendix 1: General Terms of Business is to agree the terms of engagement of XYZ's member firm for India, XYZ India Member Private Limited ("XYZ" or "us" or "we" or "our") to provide Internal Audit to ABC Limited ("the company" or "you" or "your"). In the event of any conflict between the Engagement Letter and Appendix 1: General Terms of Business, the terms set forth in the Engagement Letter shall govern.

1. Scope of work

XYZ's terms of reference for this engagement is to provide one full time Consultant resource that will be based in ABC office or ABC designated office in Mumbai to assist the Company in discharging its responsibilities related to internal audit and compliance in the Internal Audit function. The personnel provided by XYZ to the Company will perform activities required as per the ABC Authority in Mumbai.

For the avoidance of doubt, XYZ's scope of work in this engagement is to complete the tasks that can be carried out based on work that can be done by one seconded personnel in an eight hour working day.

The personnel deployed by XYZ will report directly and exclusively to ABC's Vice President of Internal Audit who shall be solely responsible for reviewing and approving the work performed by the personnel. Our full time deployed personnel will observe the Company's policies on work conditions and business hours, to the extent such policies are made known to the personnel prior to commencement of our services. The leave, training and other employee related benefits for the personnel will be governed by XYZ policies.

2. Fees

- 2.1 Our fees for the engagement are INR _____ per month excluding out-of-pocket expenses and any applicable taxes.
- 2.2 In addition to our fees specified in clause 2.1 above, we shall bill the Company for out-of-pocket expenses incurred on the engagement such as for travel, hotel, lodging, internet, etc.
- 2.3 XYZ shall submit invoice for the fees at the end of every calendar month and our fees are payable within 15 days from the date of submission of the invoice to the Company.

3. Commencement and duration of engagement

- 3.1 This engagement shall commence on _____ and shall continue for a minimum period of one and half month.
- 3.2 Following completion of the minimum period specified in 3.1 above, this engagement will continue until it is terminated by either party by giving a written notice of one month.
- 3.3 If either party terminates this contract, XYZ remains obligated to continue to perform the services during the notice period and the Company will be liable to pay for work performed up to and including the notice period.

4. Agreement

Please confirm your agreement to and acceptance of this Engagement Letter and the terms and conditions set forth in Appendix 1: General Terms of Business by signing and returning to us the enclosed copy.

Yours sincerely,

Authorized Signatory

Encl: Appendix 1 – General Terms of Business

We confirm our agreement and acceptance of the terms and conditions of this Engagement Letter and Appendix 1: General Terms of Business.

On behalf of ABC Limited

Authorized signature : _____
Name : _____
Title : _____
Date : _____

SIA 9

Communication with Management

SIA 9 – Communication with Management

The internal auditor while performing audit should:

- **Communicate** clearly the **responsibilities** of the internal auditor and an **overview of the planned scope and timing** of the audit with the management.
- **Obtain information** relevant to the internal audit from the management.
- **Provide timely observations** arising from the internal audit that are significant and relevant to their responsibility as described in the scope of the engagement to the management.
- **Promote effective two-way communication** between the internal auditor and the management.

Different **stages of communication and discussion** should be:

- **Discussion of draft:** At the conclusion of fieldwork, discussion draft should be submitted to the entity management for their review before the exit meeting.
- **Exit meeting:** At this meeting, the entity's management should comment on the draft and the internal audit team should work to achieve consensus and reach an agreement on the internal audit findings.
- **Formal draft:** The internal auditor should then prepare a formal draft, taking into account any revision or modification resulting from the exit meeting and other discussions.
- **Final report:** The internal auditor should submit the final report to the appointing authority or such members of management, as directed.

Appropriate timing for communications will vary with the circumstances of the engagement. Relevant circumstances include significance and nature of the matter, and the **action expected to be taken by management**.

Where matters required by this SIA to be communicated, are orally communicated, internal auditor shall document them and when and to whom they were communicated. Where matters have been communicated in writing, the **auditor shall retain a copy of the communication** as part of internal audit documentation.

Communicating Result - Internal auditor must communicate the result of the engagement

- Communication must include the engagement's objectives and scope
- Communication must be accurate, objective, clear, concise, constructive, complete, and timely
- CAE is responsible for reviewing and approving the final engagement communication before issuance and for deciding to whom and how it will be disseminated
- Final communication of engagement result must contain the internal auditor's opinion supported by the relevant, reliable and useful information
- If Final communication contains a significant error or omission, CAE must communicate to all parties who received the original communication

Reporting - Exit Meeting

- Audit Resource complete the working files and discuss the audit observation with the audit reviewer. Audit reviewer conduct a desktop review and call a Exit Meeting.
- Exit Meeting is a formal meeting with the auditees is called to conclude the audit fieldwork and the objectives is to discuss the following:
 - Audit Observation
 - Audit Recommendation
 - Target Date for closure of Recommendation
 - Improvement areas not falling under the scope of audit, and
 - Additional requirements, if any.
- Sensitive matters is discussed with senior management by setting a separate Exit meeting.
- This is very helpful to reduce the time required to get the management comments on the audit observation.

Reporting – Follow-up on Recommendations

- Audit can be considered as completed after the implementation of the Audit Recommendation issued into the Audit Report.
- Auditor should ensure the implementation within the target date agreed by the management. Overdue recommendation can be questioned by the Audit Committee.

Audit Number	IO No.	Responsibility	Improvement Opportunity Title	IO Description	Mgt Acceptance	Grade	Current Due Date
2011.119	1	XYZ	Training Policy	Policy not in place	Documented	H	30-Aug-16
2011.119	2	ABC	Training Program	Program is not published	Published on Monthly basis	L	31-July-16
2011.119	3	MNO	Training Budget	Budget is not tracked regularly	Will be tracked	M	31-Mar-17

- Evidences should be obtained prior to the closure of the audit recommendation. Evidences can be called by the statutory auditor or at the time of **Peer Review** hence should be kept as key working paper.

SIA 10

Internal Audit Evidence

SIA 10 – Internal Audit Evidence

Paragraph 14 of the SIA 2, Basic Principles Governing Internal Audit (IA), states:

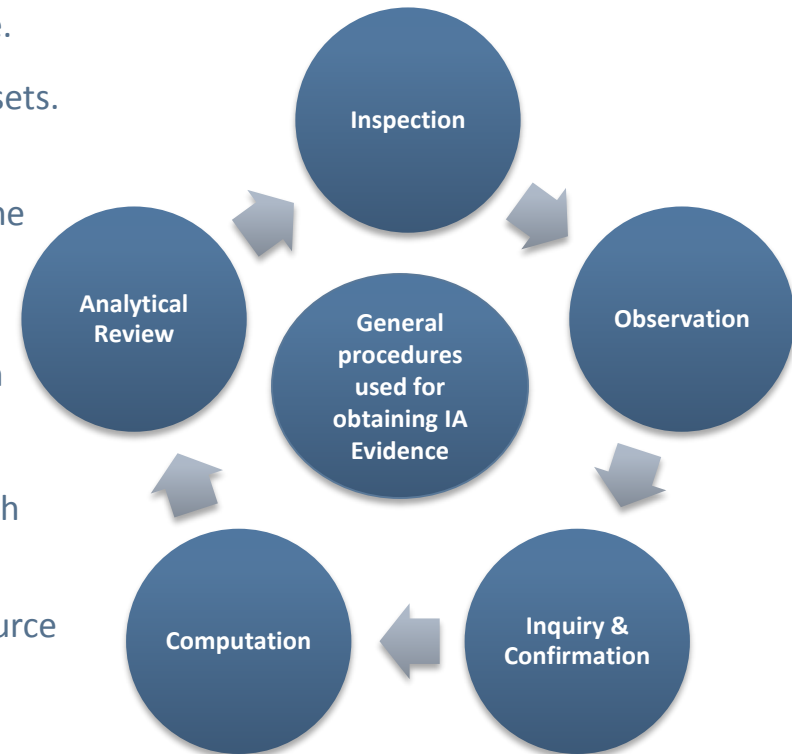
“The internal auditor should, based on his professional judgment, obtain **sufficient appropriate evidence** to enable him to draw reasonable conclusions therefrom on which to base his opinion or findings.”

Sufficiency – It refers to the quantity of audit evidence. It is affected by the auditor’s assessment of the risk of material misstatements & also by the quality of such audit evidence.

Appropriateness – It refers to the measure of the quality of such evidence i.e. its relevance and its reliability in providing support for the conclusions on which the auditor’s opinion is based.

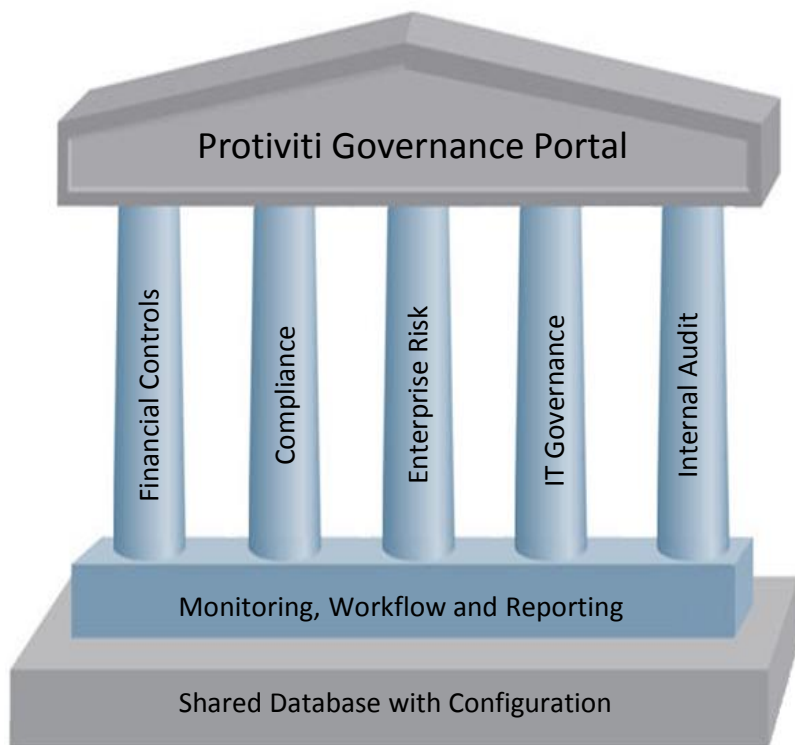
Following are the **general procedures** used for obtaining IA evidence.

- **Inspection** consists of examining records, documents, tangible assets.
- **Observation** consists of witnessing a process or procedure being performed by others. For e.g., the internal auditor may observe the counting of inventories by client personnel.
- **Inquiry** consists of seeking appropriate information from knowledgeable persons inside or outside the entity. **Confirmation** consists of the response to an inquiry to corroborate information contained in the accounting records. For e.g., the internal auditor requests confirmation of receivables by direct communication with debtors.
- **Computation** consists of checking the arithmetical accuracy of source documents and accounting records or performing independent calculations.
- **Analytical review** consists of studying significant ratios and trends and
61 investigating unusual fluctuations and items.



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.

SIA 11

Consideration of Fraud in an Internal Audit

SIA 11 - Consideration of Fraud in an Internal Audit

The internal auditor should:

- Exercise **due professional care**, competence and **diligence** expected of him
- Use his knowledge and skills to reasonably enable him to identify indicators of frauds



Common Fraud Situations:

An internal auditor should have **reasonable knowledge** of factors that might increase the **risk of opportunities for frauds** in an entity and **exercise reasonable care and professional skepticism** while carrying out internal audit.

Responsibilities of the Internal Auditor:

The internal auditor should -

- **Help the management fulfill its responsibilities** relating to fraud prevention and detection.
- **Understand** the various aspects of the **control environment and evaluate** the same as to the **operating effectiveness**.
- Specifically evaluate and assess the operating effectiveness of the policies and procedures established by the management to identify and assess the risk of frauds, including the possibility of fraudulent financial reporting and misappropriation of assets and communicate relevant information to the concerned persons in the entity to make timely and effective decisions. Also **document fraud risk factors** identified.
- Assess whether the controls implemented by the management to ensure that the risks identified are responded to as per the policy or the specific decision of the management, as the case may be, are in fact working effectively and whether they are effective in prevention or timely detection and correction of the frauds or breach of internal controls.

SIA 12

Internal Control Evaluation

SIA 12 - Internal Control Evaluation

The internal auditor should:

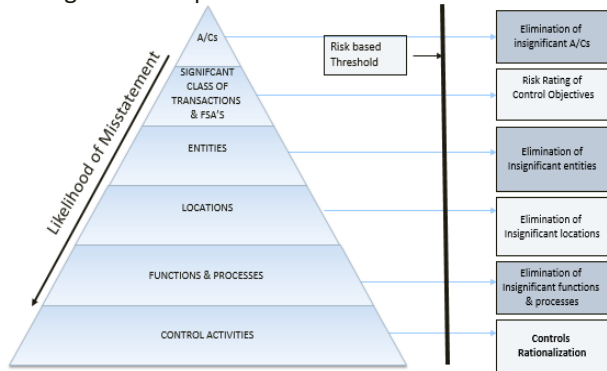
- **Examine continued effectiveness** of the **internal control system** through **evaluation and make recommendations** for improving effectiveness. Also, focus towards improving internal control structure and promoting better corporate governance.
- Evaluate the **maturity of the entity's internal control** and also obtain an understanding of the control environment sufficient to assess management's attitudes, awareness and actions regarding internal controls and their importance in the entity and to develop the audit plan and assess risks at the entity level and activity (process) level.
- Ascertaining from the Business Controls worksheet, those risks for which **no controls exist or existing controls are inadequate**. This process is the stage of '**controls gap**' analysis.
- Evaluate the **information technology controls** and should determine whether the entity uses Encryption tools, protocols, or similar features of software, Back-up and restore features of software applications and Virus protection software, Passwords that restrict user access to networks, data and applications.
- Identify and evaluate **internal control weaknesses** that have not been corrected and **make recommendations to correct those weaknesses** and also inquire from the management that either audit recommendations have been effectively implemented or that senior management has accepted the risk of not implementing the recommendations.
- The internal auditor in his report to the management, should provide a **description of the significant deficiency or material weakness in internal control**; his opinion on the possible effect of such weakness on the entity's control environment.

Internal Financial Controls & SOX

Top Down Approach

1 Identify SCOT

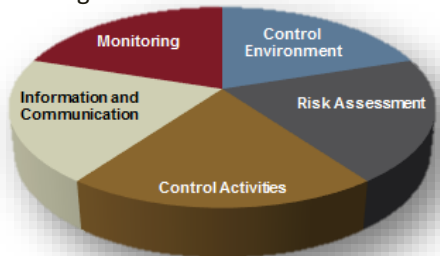
Significant class of transaction (SCOT) is any transaction that has a significant impact on the financial statement.



Risk evaluation and assessment is done based on the top-down-risk approach considering the significant judgment and management override of control. Materiality of entities, units, processes and transactions will be done considering the same approach. Financial statement line items are appropriately disaggregated to identify the significant account balances, classes of transactions, disclosures at component level.

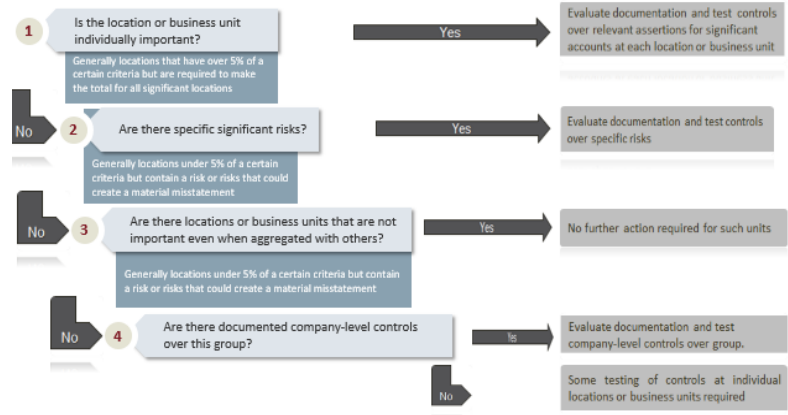
3 Identify Entity Level Controls

Each of these Entity Level Component has also been explained in ICAI guideline..



2 Identify Significant Business Units / Locations

Determined the relevance of business units/locations for scoping and evaluated factors such as the relative financial significance of the business unit/location and the risk of material mis-statement arising from the business unit/location



4 Identify IT General Controls



Critical IT processes

- Program Development
- Program Change
- Computer Operations
- Access to Program and Data
- Interface Controls



- Segregation of incompatible duties (SOD)
- Limit access to transactions and data
- Data validation/error checking routines
- Complex calculations

Critical OS/DB control (End User Computing)

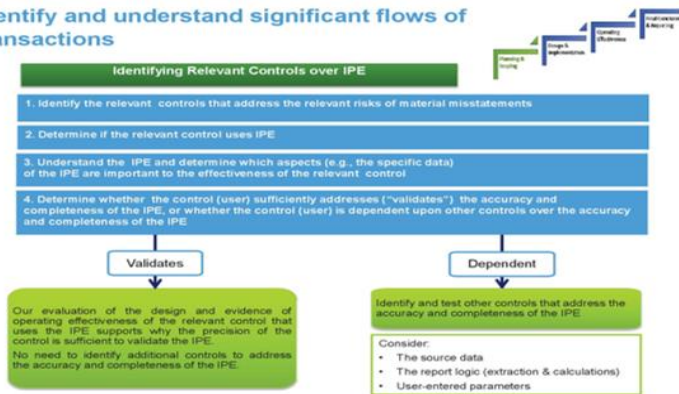
- Access to OS/DB
- Change management
- Data backup
- Data protection
- Input control, etc.

Internal Financial Controls & SOX (Contd.)

5 Identify Significant Flow of Transactions

Though the auditing standards do not provide a specific definition of Information Produced by Entity (IPE). IPE is in the form of a report which is either system generated, manually prepared or a combination of both. IPE evaluation by Protiviti is represented as below:

Identify and understand significant flows of transactions



6 Identify Key Controls

- Controls which are most likely to prevent and detect errors/fraud in a process.
- General controls (e.g. information technology) on which other significant controls are dependent.
- Controls over significant non-routine and non-systematic transactions.
- Controls over the period end financial closing process, including controls over procedures used to enter transaction totals into the general ledger.
- Controls with a high likelihood that its failure would result in a material financial misstatement.

Remember!

All controls are *not* key controls. Operationalizing and Testing controls **cost** the Company

7 Finalize Project Plan, Reporting Templates for IFC Implementation (As per ICAI Guideline/Additional Client Requirements)

Identify Processes

Document Processes

Risk Assessment

Identify key controls and KCI

Test of Design

Test of Effectiveness

SIA 13

Enterprise Risk Management

SIA 13 - Enterprise Risk Management

The role of the internal auditor is **to provide assurance to management on effectiveness of risk management.**

The Internal auditor should:

- **Not manage any of the risks** on behalf of the management or take risk management decisions.
- **Review the maturity of an enterprise risk management structure** by considering whether the framework so developed:
 - **Protects** the enterprise against surprises.
 - **Stabilizes overall performance** with less volatile earnings.
 - Operates within established **risk appetite**.
 - **Protects** ability of the enterprise to attend to its core business.
 - Creates a system to **proactively manage risks**.
 - Report on the results of the **assessment of key risks** at the appropriate levels

The **internal audit plan** should be **approved by the audit committee and based on risk assessment**. The risk assessment process should be of a **continuous nature**. It should be **conducted formally at least annually**, but more often in complex enterprises.

Process of ERM

Establishing Context

Identify the Risks

Analyze / Quantify Risks

Integrate the Risks

Prioritize the risks

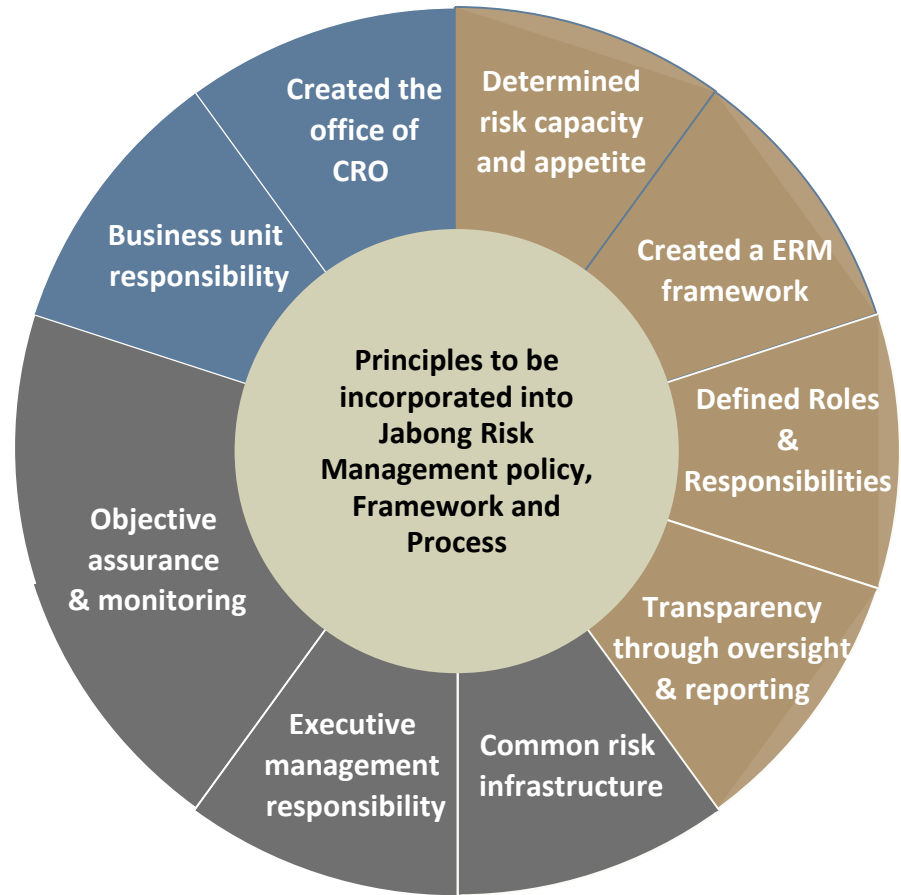
Treat/Exploit the Risks

Monitor & Review

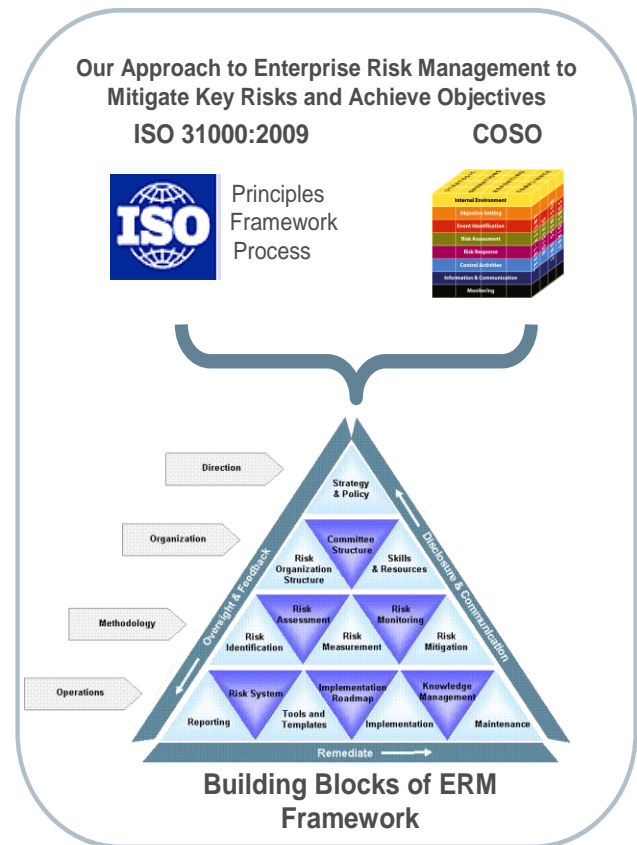
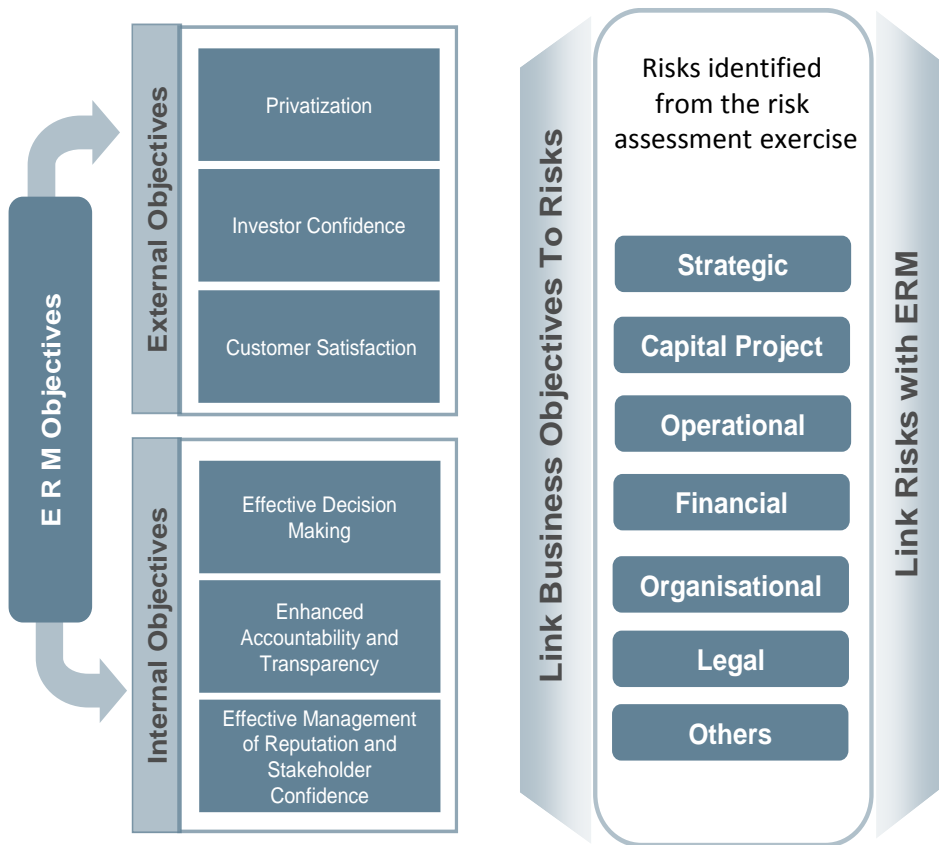
Enterprise Risk Management

Our guiding principles - Building a Risk Intelligent Enterprise

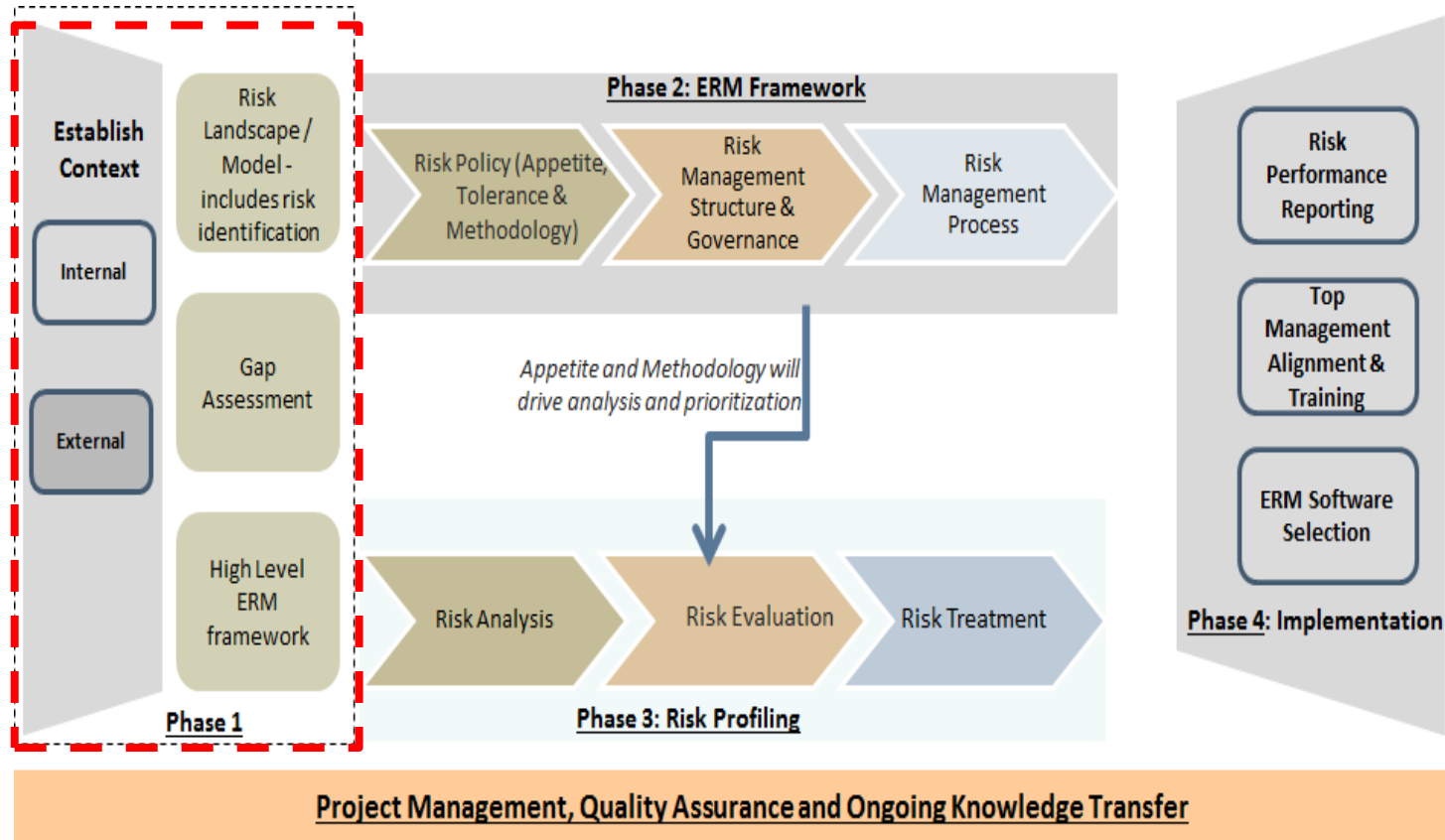
Nine Principles for Building a Risk Intelligent Enterprise



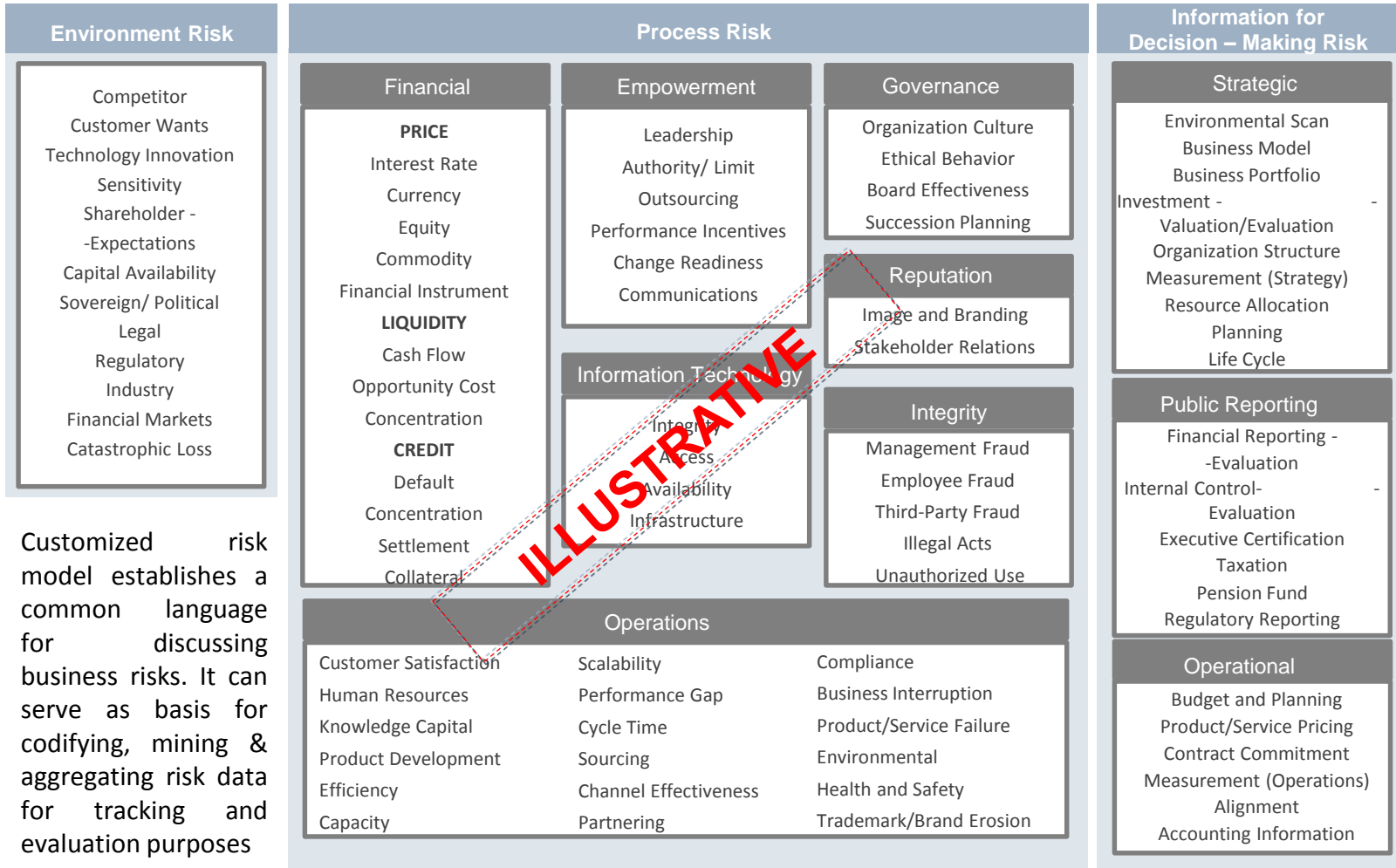
Enterprise Risk Management (Contd.)



Our Approach – Phase 1: Establish Context and Current State Assessment of ERM



Risk Landscape

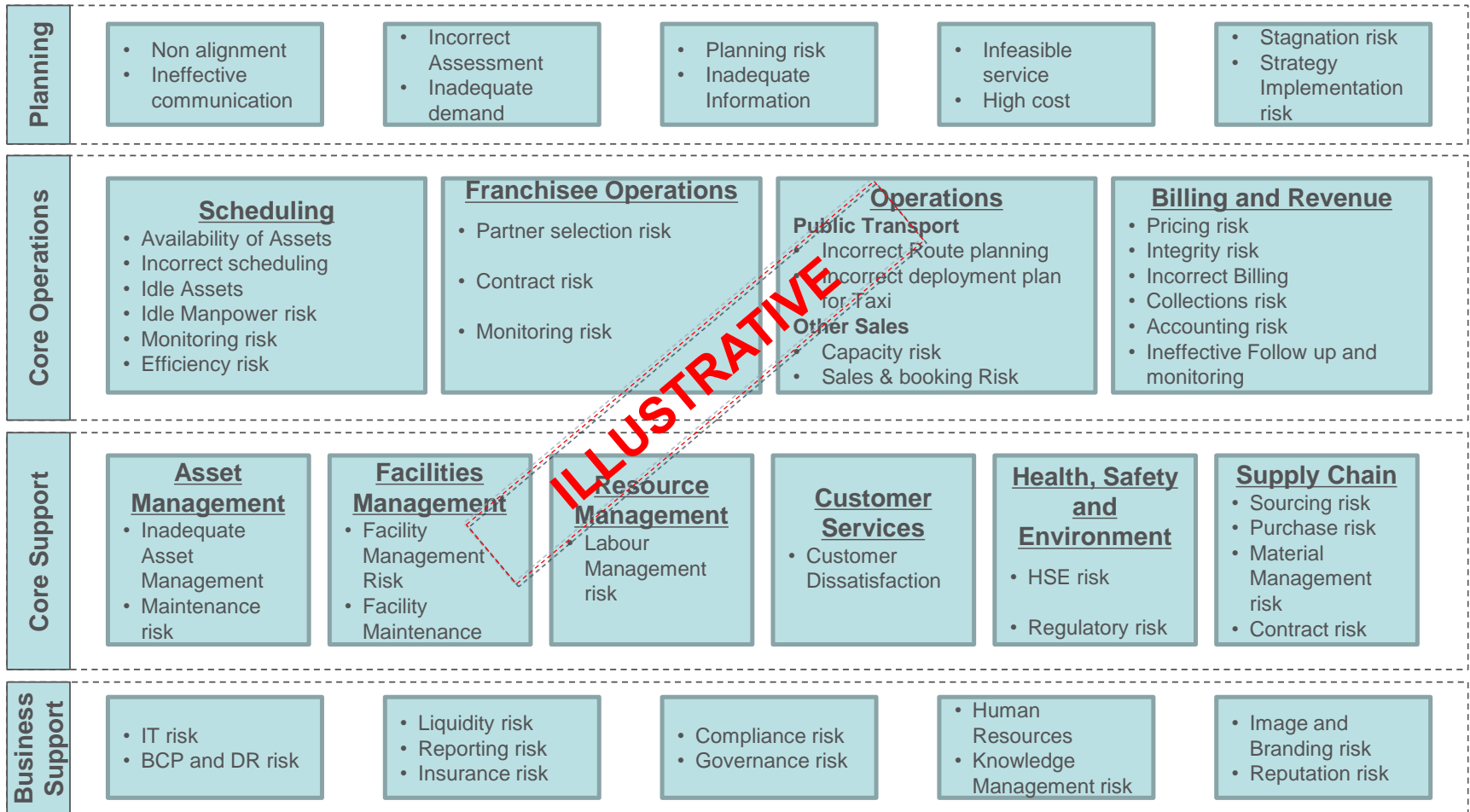


ILLUSTRATIVE

Customized risk model establishes a common language for discussing business risks. It can serve as basis for codifying, mining & aggregating risk data for tracking and evaluation purposes

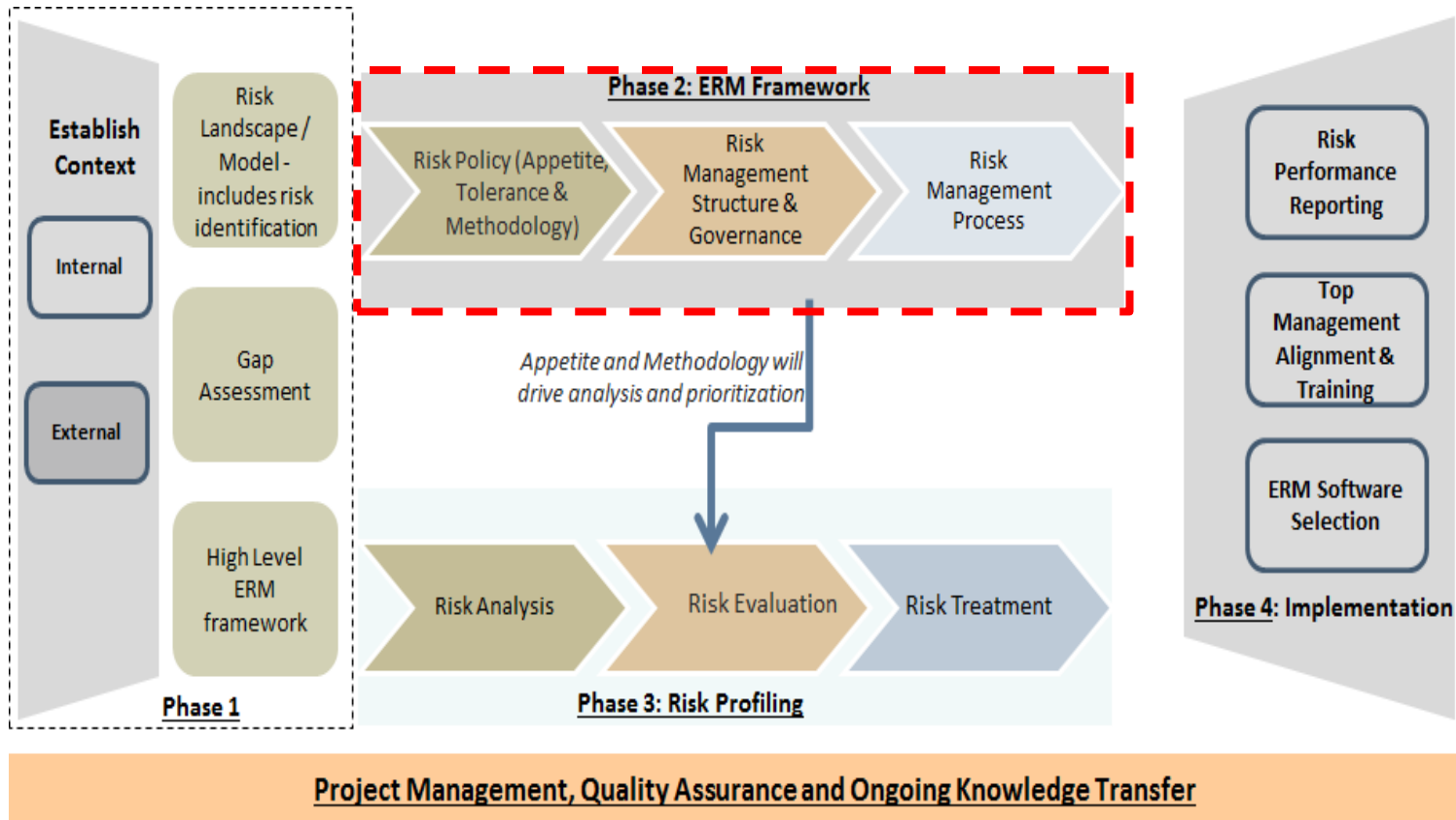
This can act as a reference or a starting point. Customization to industry and business is important. Protiviti has developed standard industry specific risk inventories that can be leveraged upon for sourcing risks in the beginning of the engagement

Risk Landscape (continued)



ILLUSTRATIVE

Our Approach – Phase 2: ERM Framework



Strategy Articulation, Mapping Objectives & Risks

The enterprise's purpose and where it is ultimately headed



Capabilities

How the enterprise differentiates itself to execute its mission



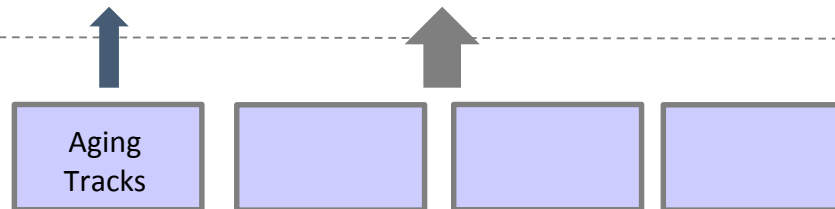
Objectives

Statements around what is to be achieved through leveraging capabilities



Risk Mapping

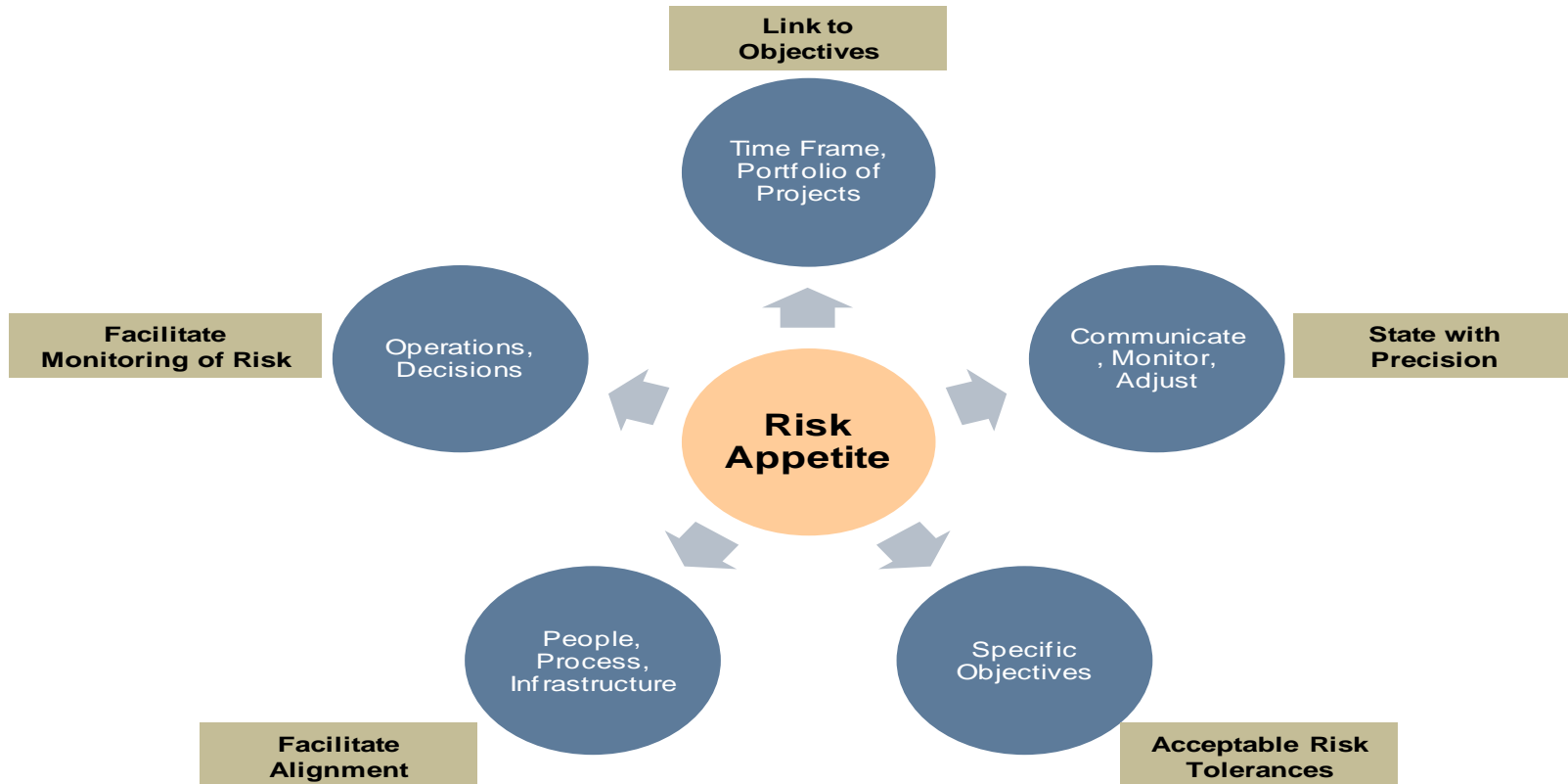
Key risks mapped to objectives that will be impacted



This framework will be used in the risk profiling stage to identify **strategic risks**

Strategy articulation will also be the context in which risk appetite will be developed

Phase 2: Articulating Risk Appetite



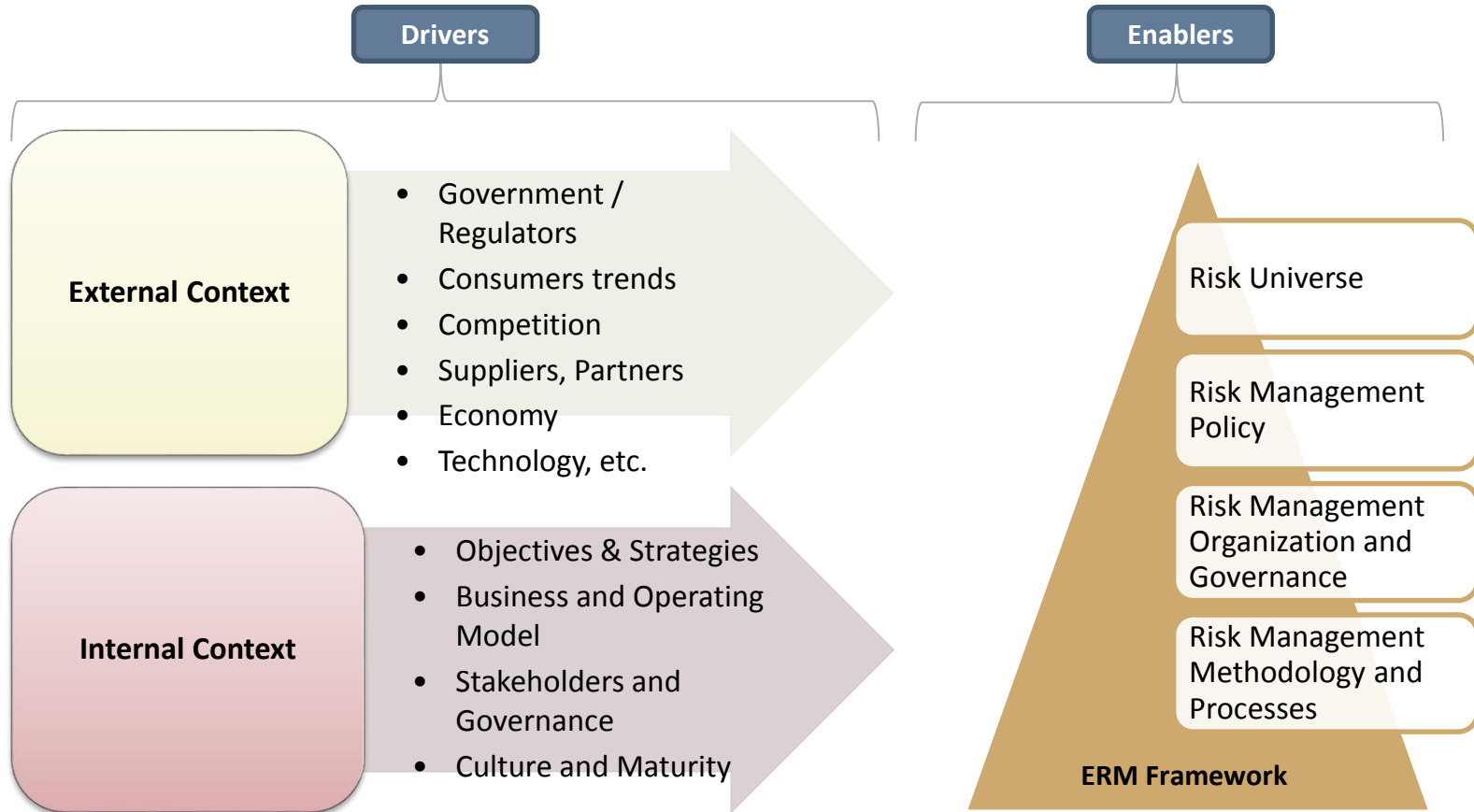
- Risk Appetite can be defined as capacity to bear risk and willingness to accept risk in pursuit of objectives.
- In order to develop the risk appetite, Protiviti will understand the strategy and identify key objectives.
- Risk appetite will be developed in context of the strategy and the strategic objectives. Appetite once developed will form part of the Risk Policy and will also be embedded in the Risk Assessment Criteria Matrix that will be used for evaluation of risks.

Phase 2: Risk Appetite

An event or risk is assessed in the risk appetite table and assigned a risk score by multiplying the impact and likelihood scores. Ranges of risk scores are then established depending upon the risk appetite of the organization.

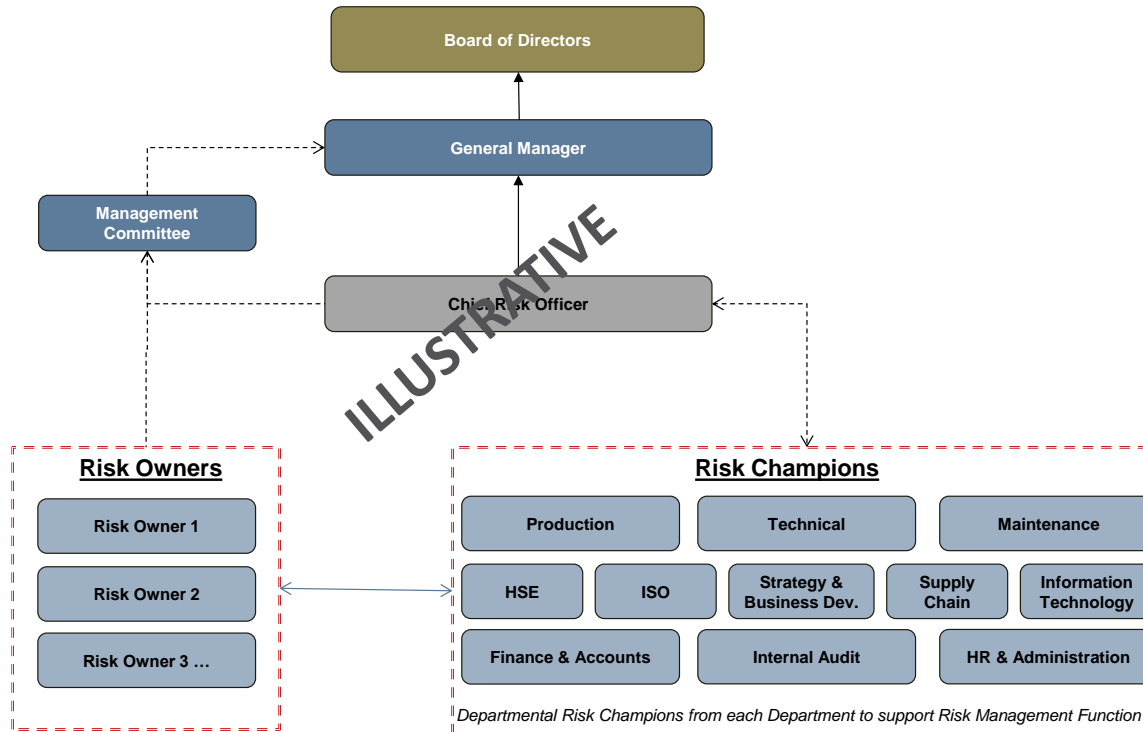
IMPACT						LIKELIHOOD			
Score	Rating	Financial Impact based on Income (PBT)	Organizational & Operational Scope	Reputational Impact	Regulatory Impact	Score	Rating	Certainty	Frequency
5	Critical	> RO 700K (~10%) Fraud Limit: > RO 50K	Enterprise-wide; Inability to continue normal business operations across the enterprise.	Bad publicity, Litigation, etc. which may lead to loss of confidence/reputation in main audience	Violation, which may lead to major penalties (> RO 25K) from regulatory / statutory bodies or loss of permit/license or temporary suspension.	5	Expected	> 90%	Yearly
4	Significant	RO 500-700K (7.5-10%) Fraud Limit: RO 35-50K	2 or more Businesses; Significant, ongoing interruptions to business operations within 2 or more BUs	Bad publicity, Litigation, etc. which may lead to loss of confidence/reputation in 2-3 segments of audience/stakeholders	Violation, which may lead to penalties (RO 15-25K) from regulatory / statutory bodies or warning to withdraw permit or license.	4	Highly Likely	≤ 90%	Every 2-3 Years
3	High	RO 300-500K (5-7.5%) Fraud Limit: RO 15-35K	1 or more Business(es); Moderate impact within 1 or more BUs.	Bad publicity, Litigation, etc. which may lead to loss of confidence/reputation in 1-2 segments of audience/stakeholders	Violation, which may lead to penalties (RO 5-15K) from regulatory / statutory bodies or warnings.	3	Likely	≤ 60%	Every 4-6 Years
2	Moderate	RO 150-300K (2-5%) Fraud Limit: RO 6-15K	1 Business; Limited impact within 1 BU.	Bad publicity, Litigation, etc. which may lead to loss of confidence/reputation in limited (individual) audience/stakeholders	Violation, which may lead to penalties (< RO 5K) from regulatory / statutory bodies or warnings.	2	Not Likely	≤ 30%	Every 7-9 Years
1	Low	< RO 150K (2%)	Limited Impact			1	Slightly	< 10%	10 Years and Beyond

Phase 2: Methodology for ERM Framework



Any management framework will be grounded in its business environment (internal and external). The risks that an organization faces with regard to its objectives have their source in its environment.

Phase 2: Risk Management Organization Structure



- Risk categories and nature of Risks would determine the risk management structure. Different skills and competencies would be required to manage and monitor different categories of Risks.
- Risks that organization faces on continued basis will require routine management and enhanced reporting.
- Risk sources or impact points within the organization will drive definition of risk ownership and need for management through higher staff engagement (risk champions).
- The Risk Management structure would leverage on the existing governance structure .

Phase 2: Risk Policy & Procedures

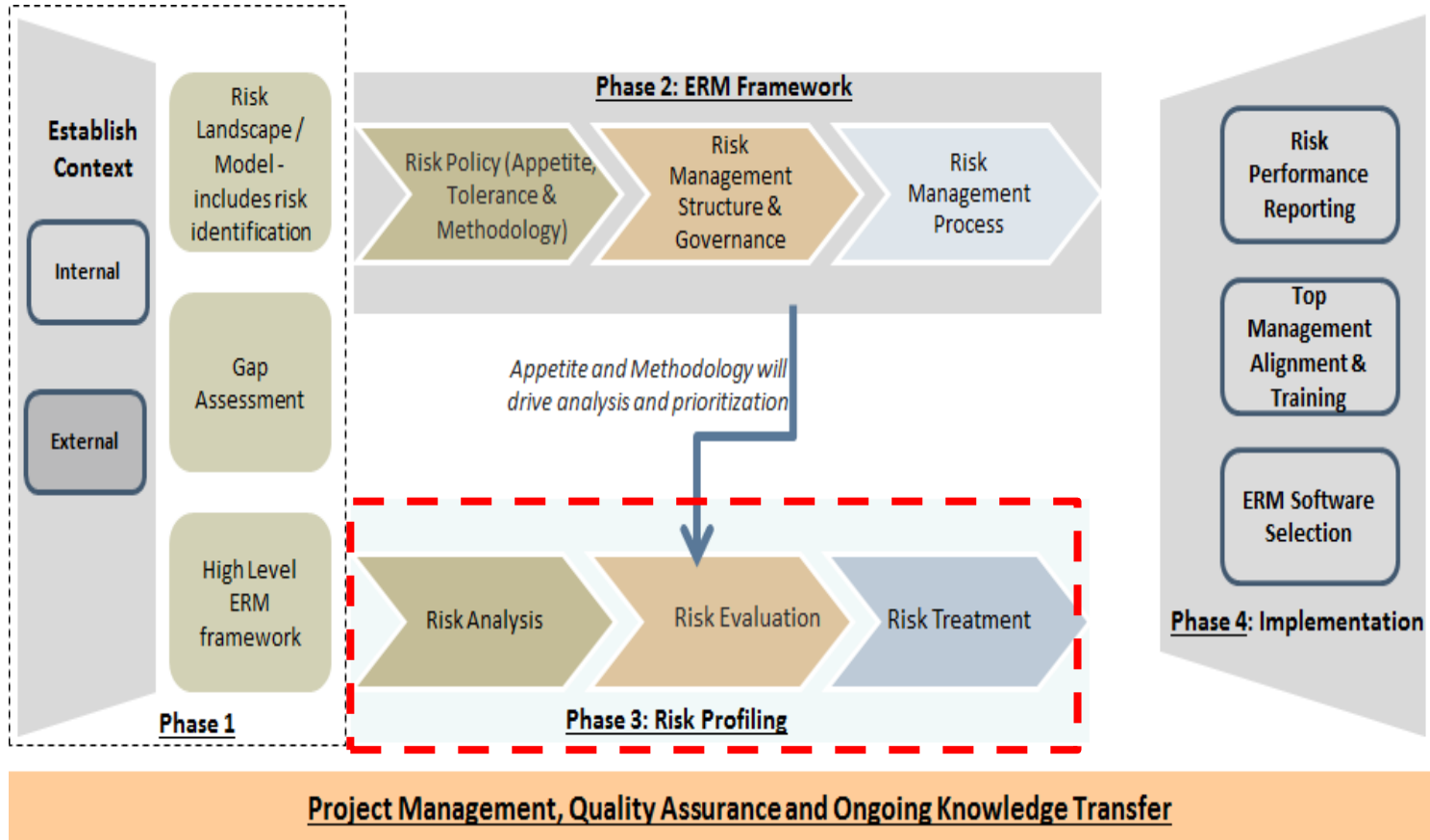
Risk Management Policy - An ERM "Users Guide" with step-by-step guidance on the Risk Management process

Table of Contents

1. INTRODUCTION	4.2 Risk Mitigation
1.1 Vision and Risk Management Mission	4.3 Risk Monitoring and Assurance
1.2 Enterprise Risk Management philosophy	5. ENTERPRISE RISK MANAGEMENT STRUCTURE
1.3 Regulatory Requirement	5.1 Roles and Responsibilities - Risk Management Process
1.4 Risk – A Definition	5.2 Roles and Responsibilities - Risk Management Structure
1.5 Risk Appetite – A Definition	A. Board of Directors
2. ENTERPRISE RISK MANAGEMENT FRAMEWORK	B. Corporate Risk Team
3. ENTERPRISE RISK MANAGEMENT ORGANISATION	C. Risk Champions
A. Board of Directors	D. Risk Owners
B. Apex Risk Council	5.3 Risk Leaders– Roles and Responsibilities
C. Corporate Risk Team	5.4 Risk Management Activity Calendar
D. Risk Champions	
E. Management Assurance	
4. ENTERPRISE RISK MANAGEMENT PROCESS	
4.1 Risk Assessment and Reporting	
i. Risk identification	
ii. Risk prioritization	
iii. Risk reporting	

ILLUSTRATIVE

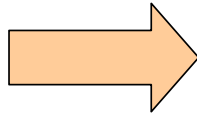
Our Approach – Phase 3: Risk Profiling



Phase 3: Risk Assessment

Identified Risks

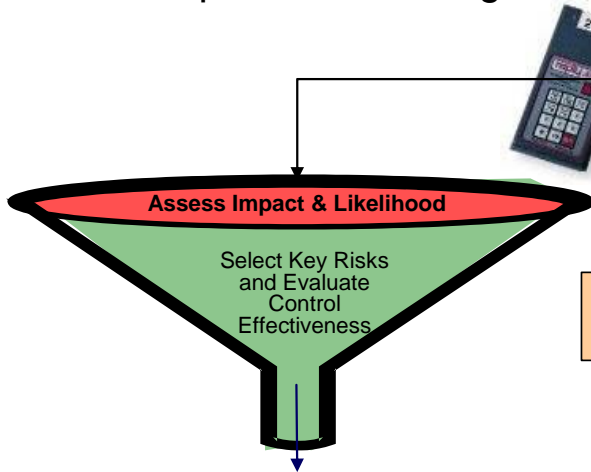
Assessed Through



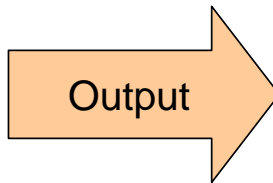
Risk Assessment Criteria Matrix

IMPACT					LIKELIHOOD			
Score	Rating	Financial Impact based on business (A-D)	Operational & Reputational Impact	Regulatory Impact	Score	Rating	Frequency	Response T
5	Critical	+ AEO (B)(4) (+10%) Fixed cost + AEO (B)	Customer credit, inability to conduct normal business operations to meet the demand	Regulatory, litigation, etc. which may lead to loss of confidence/reputation in news articles, CR, loss of life	5	Expected	+ 90%	Hours
4	Significant	AEO (B)(3)(B) (+5-10%) Fixed cost AEO (B)(3)	2 or more Business Operations, ongoing disruption to business operations within 2 or more (B)(3)	Regulatory, litigation, etc. which may lead to loss of confidence/reputation in 20 segments of subordinated functions	4	Major	+ 50%	Days 20
3	High	AEO (B)(3)(B) (+1-5%) Fixed cost AEO (B)(3)	1 or more Business Operations, Moderate disruption 1 or more (B)(3)	Regulatory, litigation, etc. which may lead to loss of confidence/reputation in 12 segments of subordinated functions	3	Minor	+ 30%	Days 90
2	Medium	AEO (B)(3)(A) (0-1%) Fixed cost AEO (B)(3)	1 Financial Line of work with 1 (B)(3)	Regulatory, litigation, etc. which may lead to loss of confidence/reputation in limited (individual) subordinated functions	2	Not Likely	+ 20%	Days 150
1	Low	+ AEO (B)(2)	Single event	Regulatory, litigation, etc. which may lead to loss of confidence/reputation in limited (individual) subordinated functions	1	Highly	+ 10%	30 Days, and Beyond

Risks prioritized through voting mechanism

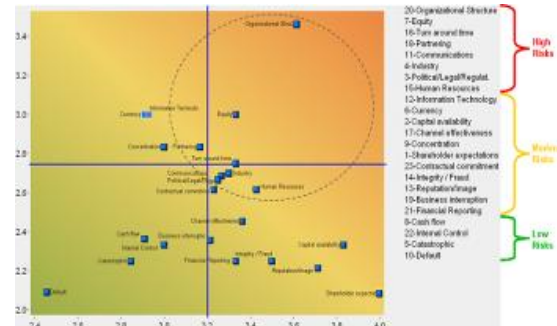


Resolver Ballot

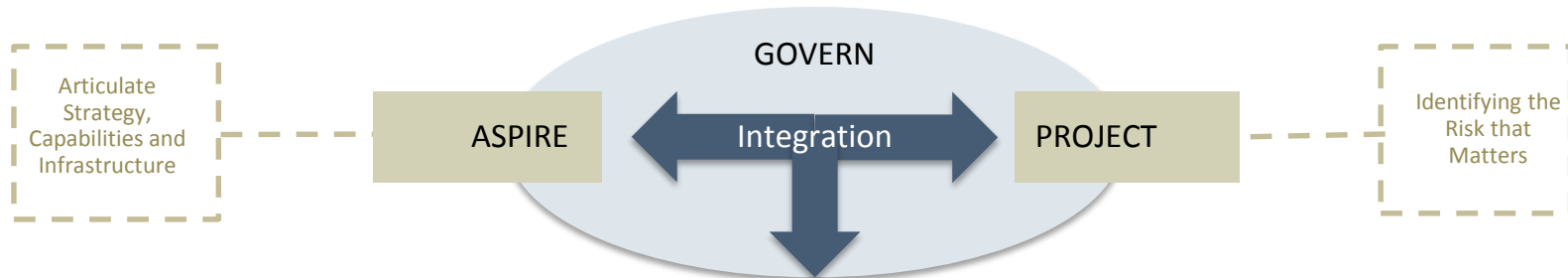


Output

Risk Map



Phase 3: Strategic Risk Assessment



- Strategic Management is a governance process through which an organization strikes balance between opportunity seeking activities (for value enhancement) and controls for value protection.
- Strategic risk can be summed as lack of alignment of business model with strategy, possibility of one or more critical assumptions losing validity due to some future events and risks inherent in strategic objectives.
- Strategic risks are difficult to identify or analyze.
- Integration of risk management at governance level will lay down the conceptual basis for further integration at performance management level.
- Our methodology will lay down the steps for mapping of strategy and identification of critical assumptions, risk model / landscape developed as part of Phase 1 can be used to source risks against the strategic objectives.
- All risks are not strategic but most of the critical risks or risks that matter will form part of strategic risks.
- This step will be a sub set of the Phase 3 - Risk Profiling. Strategy Articulation and mapping will be performed in Phase 1.
- Suitable for strategy focused organization with mature or serious strategic management program in place.

Phase 3: Risk Treatment

- Risk avoidance
- Acceptance or increasing the risk in order to pursue an opportunity
- Removal of the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision

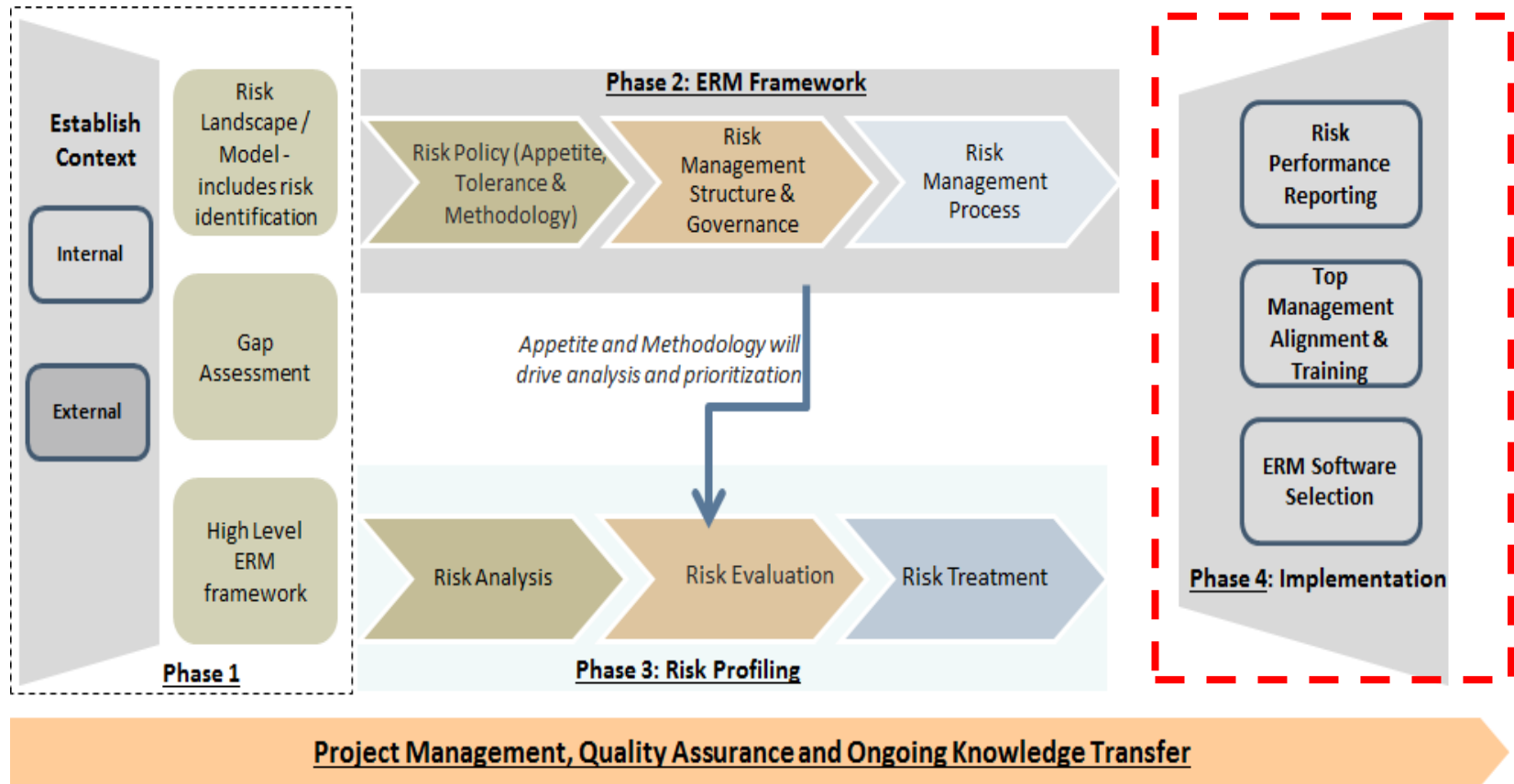
Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived.

Time and Resources should be committed for the Risk Treatment.



Risk Treatment Process

Our Approach – Phase 4: Implementation



Phase 4: Risk Reporting

Reporting of results of risk management to all relevant personnel for ensuring acceptability, review, inputs, expedition and monitoring is very important aspect of an ERM framework.

Sharing the results of the annual risk assessment on a timely basis (identification and prioritization) with the Senior Management provides the required support from the senior management.

Risk Reporting Contents:

- Risk Action Plan Reporting;
- Reporting for critical and significant risk category;
- and
- Root cause and Mitigation plan reporting.

Implementation status - Risk Action Plan					
Risk No. 1: Risk Title and Definition					
Category (as per Co's Risk Map): Strategic					
Risk Priority (Pre-Treatment) <small>(See Note 3)</small>					HIGH
Risk Action Plan Implementation Date:					
Action Plan Owned by:					
Status Review of Action Plan by:					
S.No.	Agreed Action Plans	Individual Action Plan Weightage (A) <small>(See Note 4)</small>	Percentage Completion (B) <small>(See Note 5)</small>	Delay (with respect to original Timeline) <small>(See Note 6)</small>	Total Action Plan Completion % (A * B)
1	Action Plan Title	0.5	70%	On track	35%
2		0.3	20%	Yes (2 Weeks)	6%
3		0.2	90%	On track	18%
Total		1.0			59%

Risk Action Plan Reporting

Department Name										
S.No	Process Name	Risk Number	Risk Description	Ratings				Mitigation Plans	Risk Owner	Date of Implementation
				RR Impact	RR Likelihood	Score	CE			
Reasons for not defining Mitigation plans, if applicable										
Department Name										
S.no	Process Name	Risk Number	Risk Description	Ratings				Mitigation Plans	Risk Owner	Date of Implementation
				RR Impact	RR Likelihood	Score	CE			
Reasons for not defining Mitigation plans, if applicable										
Residual Risk (RR) Impact	Residual Risk (RR) Likelihood	Score - Impact * Likelihood	Control Effectiveness (CE)							
1- Critical	3- Expected	>16	1 - Excellent							
2- Significant	4- Highly likely	9 and <=16	2 - Good							
3- High	5- Likely	> 4 and <=9	3 - Fair							
4- Moderate	6- Slightly	> 1 and <=4	4 - Poor							
5- Low	7- Not likely	<=1	5 - Unsatisfactory							

Reporting for Critical and Significant Risk Category

Phase 4: Knowledge Transfer

Aligned to the completion of each phase of the assignment would be designed a **“Training and Knowledge Transfer Plan”**. The plan would explain the participants in details all the relevant frameworks used for the assessments.

Knowledge Transfer Plan

Protiviti disseminates knowledge within the organization using its Knowledge Transfer approach. This approach is designed to educate and train Enterprise’s Risk Management team and management with a view to develop Risk Champions at department level.

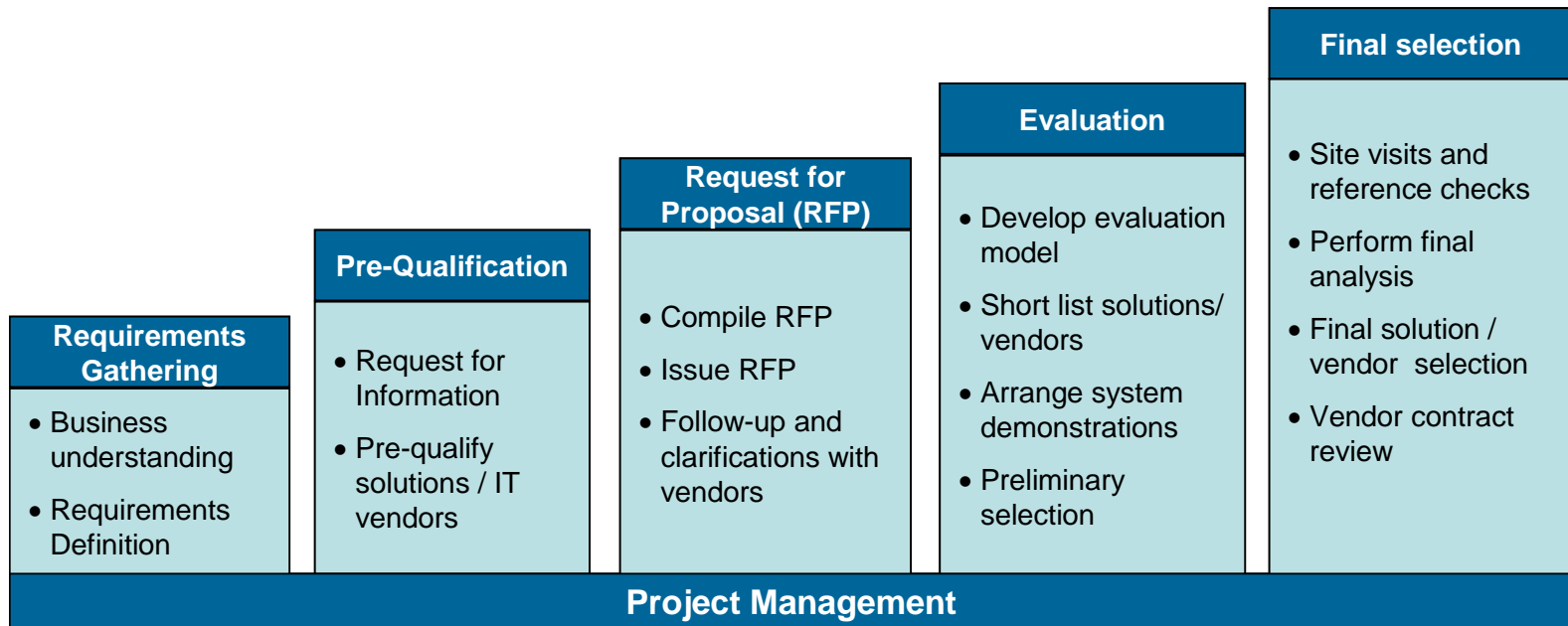
The Knowledge Transfer Plan should have the following stages:

- Initial Skill Assessment.
- Development of Knowledge Transfer Approach.
- Conducting Risk Workshop.
- Assessment of Knowledge Transfer.
- Identification of Areas of Improvement / Lessons Learned.
- Development of Training Calendar.



Phase 4: ERM Software Evaluation

Protiviti's 'Quick Select' methodology is to assist in quick selection of an appropriate ERM solution. The methodology provides well-structured work-steps, as set out in the following diagram-



SIA 14

Internal Audit in an Information Technology Environment

SIA 14 - Internal Audit in an Information Technology Environment

The internal auditor should:

- Consider the effect of an IT environment on the **internal audit engagement, the flow of authorized, correct and complete data to the processing center, the processing, analysis and reporting tasks** and the impact of computer-based accounting system on the audit trail.
- Have sufficient knowledge of the information technology systems to **plan, direct, supervise, control and review** the work performed. Consider whether any specialized IT skills are needed in the conduct of the audit.
- Obtain an **understanding of the systems, processes, control environment, risk-response activities and internal control systems** sufficient to plan the internal audit.
- Ensure that **authorized, correct and complete data** is made available and provide for **timely detection and correction of errors; accuracy and completeness of output; provide adequate data security; prevent unauthorized amendments; provide for safe custody of source code of application software and data files.**
- Review the **effectiveness and safeguarding of IT resources**, including – people, applications, facilities and data.
- Review the **robustness of the IT environment** and consider any **weakness** or **deficiency** in the **design** and **operation** of any IT control within the entity:
 - System Audit Reports.
 - Reports of system breaches, unsuccessful login attempts, passwords compromised and other exception.
 - Reports of network failures, virus attacks and threats to perimeter security.
 - General controls like segregation of duties, physical access records, logical access controls.
 - Application controls like input, output, processing and run-to- run controls.
 - Excerpts from the IT policy of the entity relating to business continuity planning, crisis management and disaster recovery procedures.

Information Technology Assurance

Our insights in IT operations across globe suggests consistent need for “IT Audit Assurance Services” from companies large and small. The reviews, which are influenced by recent trends in technology, deliver valuable insights into key IT risk areas and are directly linked to the objectives of the organization and have actionable findings to improve controls and business processes. Protiviti has the specialized array of skills, knowledge and experience for successful delivery of these critical reviews:

IT Risk Assessment and Planning

- IT Risk Assessment- Risk Register, Rating and Prioritization
- Integrated Risk assessments

IT SOX/ Internal Controls Over Financial Reporting

- Walkthrough of IT processes
- Design and Test Operating Effectiveness assessment
- Document and remediate control gaps

IT General Controls

- IT Policy and Procedures
- Application Security
- Change Management
- Logical and Physical Access Controls
- Back-Up and Recovery Controls

Technology Infrastructure, Components and Configuration

- Technology Architecture
- Operating System and Database
- IT Network Infrastructure

Application and Automated Controls

- Input, Processing and output controls
- Automated Business Process Control reviews
- Review of Critical Business Applications and ERPs
- Segregation of Duties reviews

IT Processes and Operations

- Review of IT Processes and Operations
- Data Center and NOC reviews
- IT Service Management

Information Security and Data Management

- Information Security Policy and Procedure reviews
- Database Security/ Data Privacy reviews

Business Continuity Management and Testing

- Business Continuity Management
- Crisis Management
- Disaster Recovery Planning

IT Risk & Consulting – Information Technology Governance

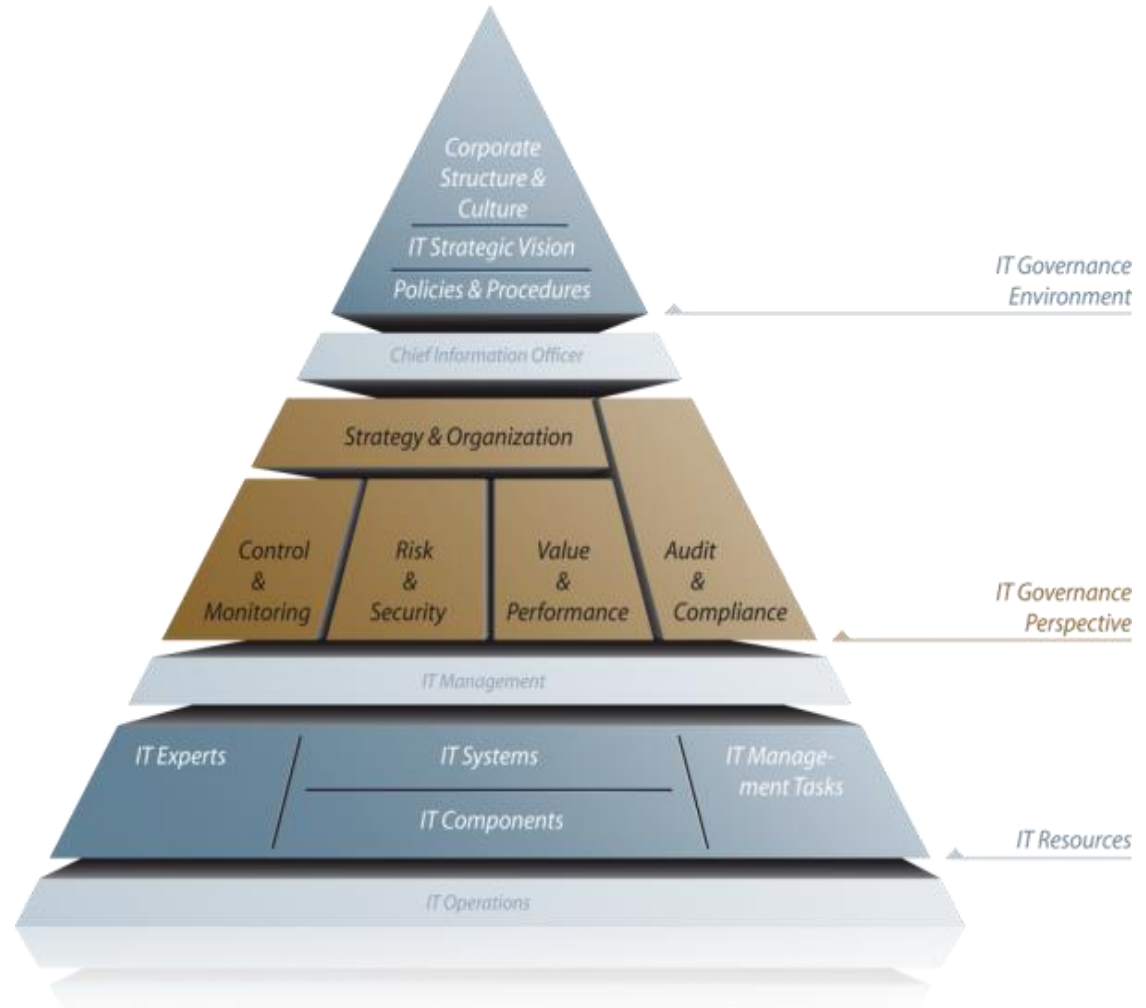
IT Governance is the management environment used to align, control and assure the delivery of technology to the business.

IT governance helps ensure that IT supports business goals, optimizes business investment in IT, and appropriately manages IT-related risks and opportunities.

IT Governance also encompasses the management of the risks associated with the use of technology, the delivery risk of providing an application environment and the control of technology-based resources.

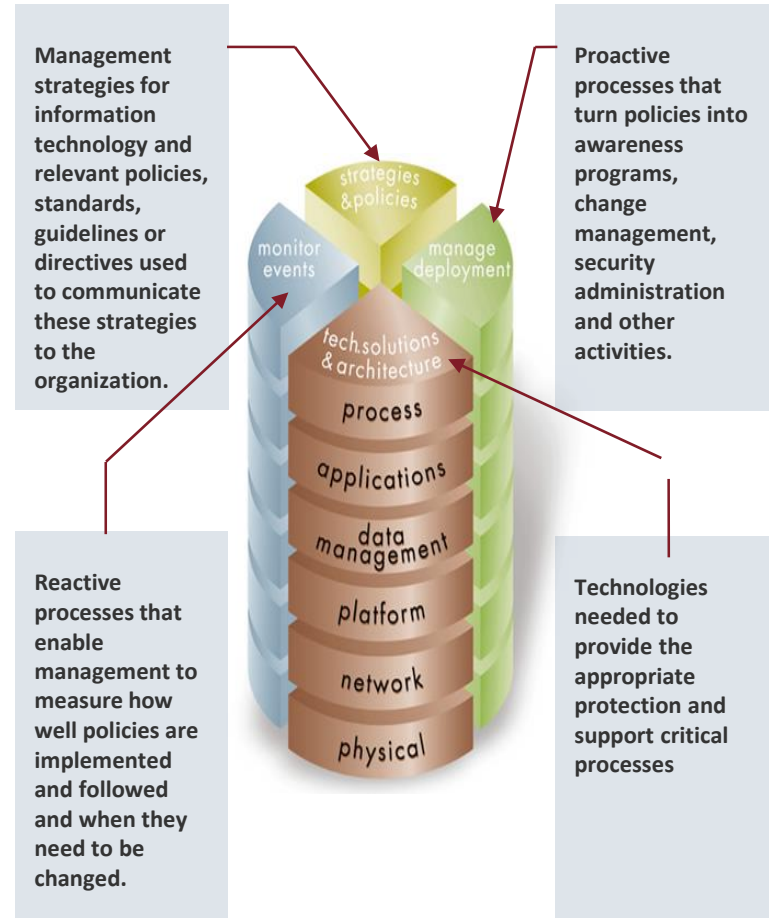
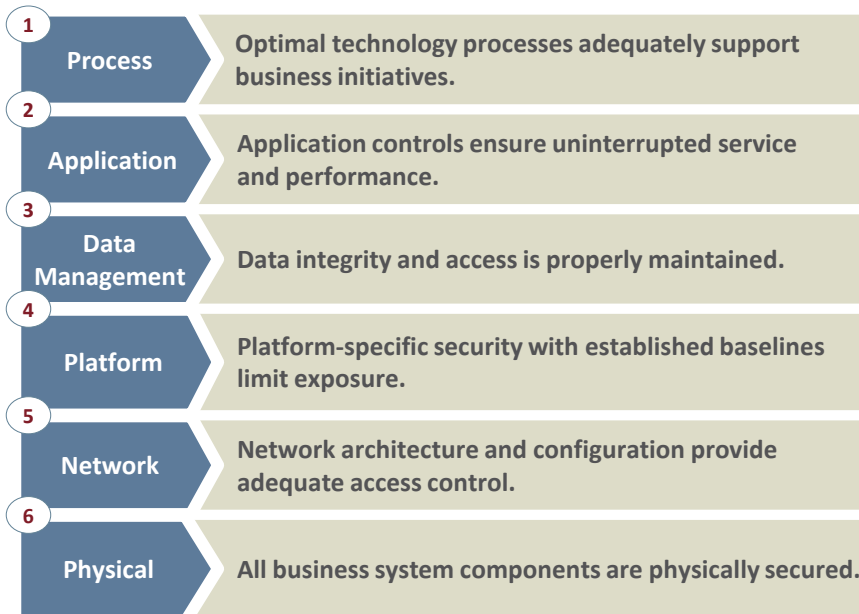
We customise our approach to IT Governance to each client's requirements. Protiviti has identified three core areas in which organisations require support in the area of IT Governance and they are as follows:

- IT Risk Management
- Building and Validating Business and System Architectures (IT Governance)
- Technology-enabled Business Concepts and Delivery (Portfolio Management)

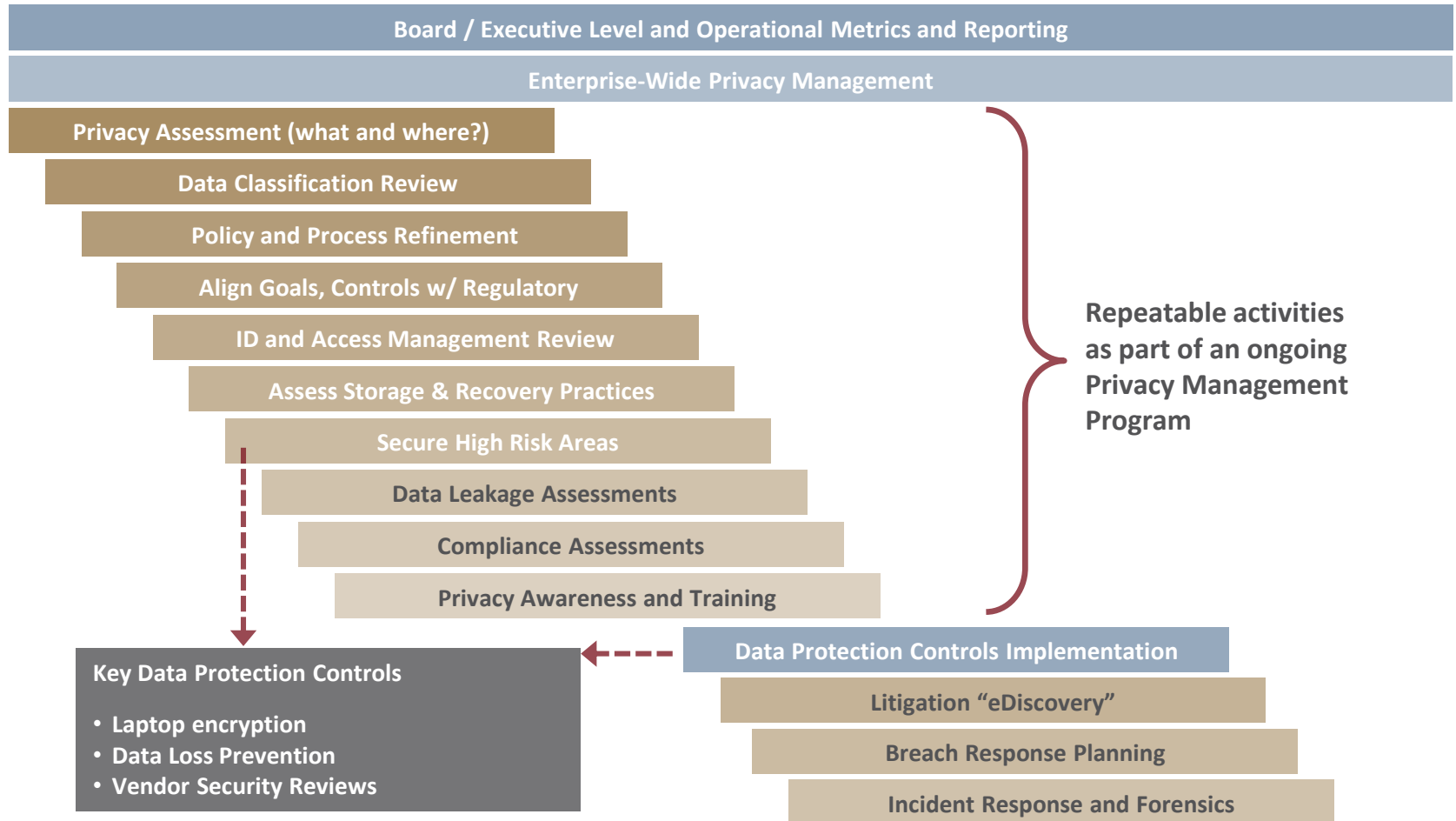


IT Risk & Consulting – Information Security Framework

A comprehensive, yet flexible, approach to identifying technology-related business risks. We use our proprietary Information Security Framework SM (ISF) as the basis for performing security assessments. The framework is based on the simple concept of balance: that information security risk management techniques should create a balance between the cost and nature of controls implemented and the benefit of risks assessed and controlled. Effective security risk management is achieved by implementing four broad, interrelated security risk management techniques applied at each layer.

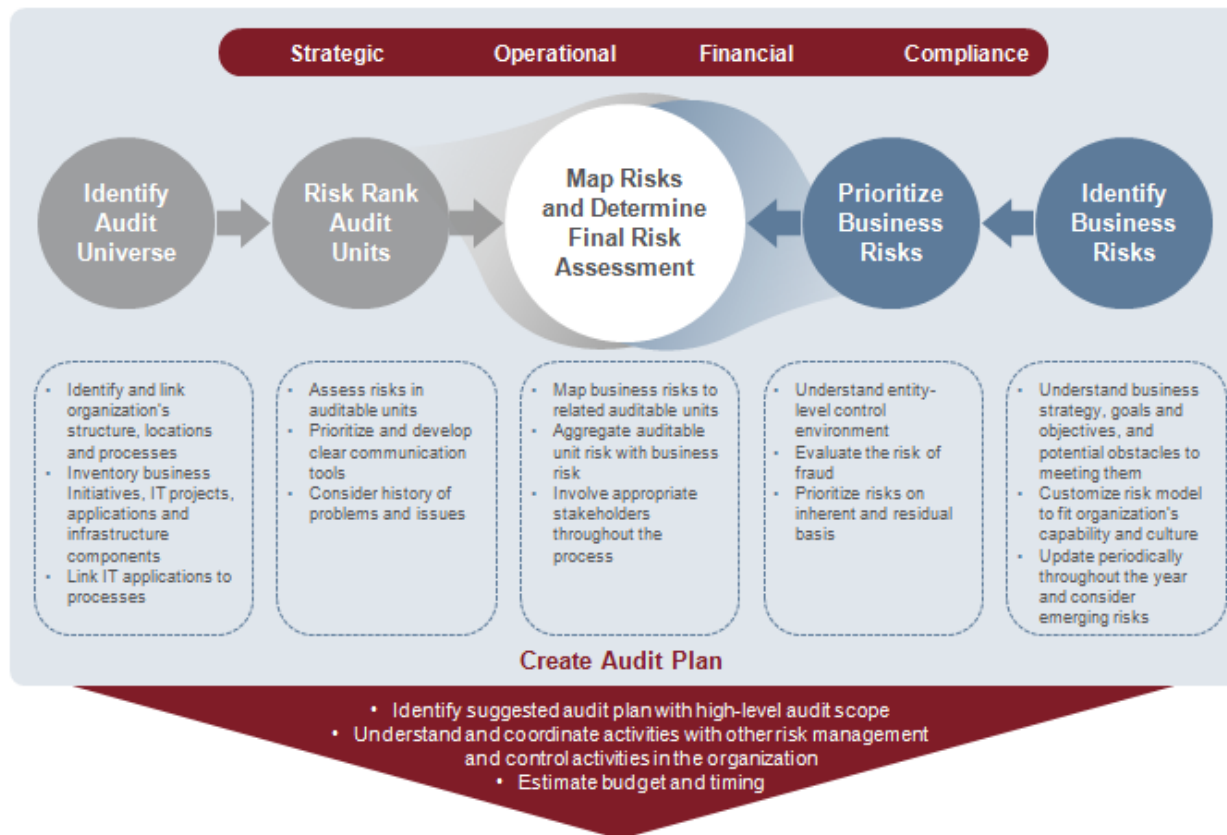


IT Risk & Consulting – Data Lifecycle & Information Protection Roadmap



Protiviti's Risk Assessment Approach

Below is Protiviti's Risk Assessment Approach. We understand you may already have an approach, or have already conducted one. In that case, we will discuss the results and associated audit plan once finalized.

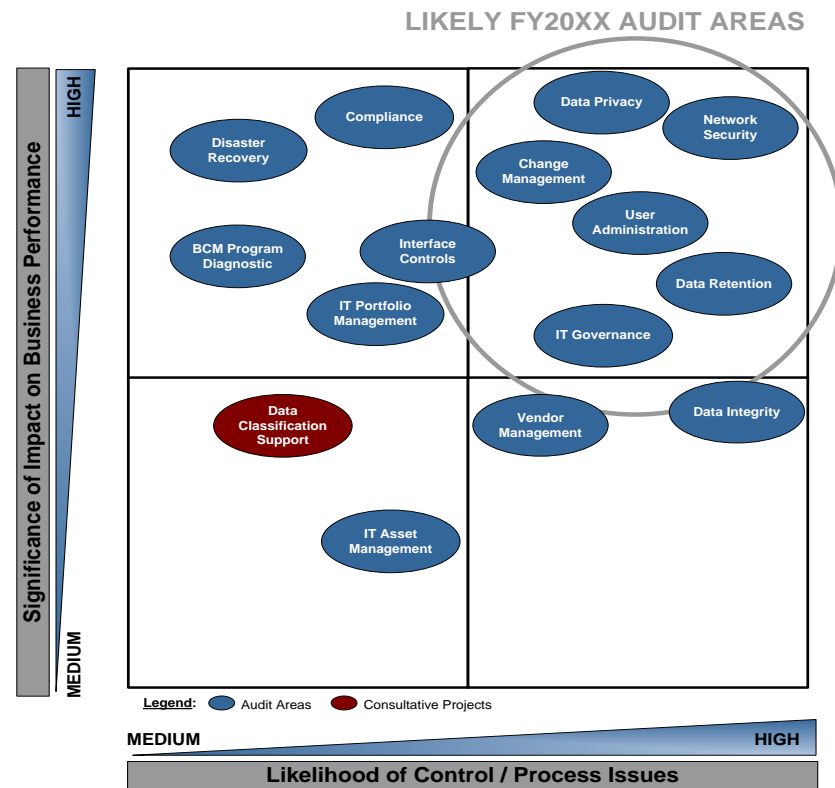


IT Risk Prioritization

The **Risk Map** below summarizes the results of a sample **IT risk assessment**. It summarizes all risks evaluated as low, medium or high. Lower priority issues collected during the risk assessment process are captured and recorded for future review and monitoring. Our goal is to identify the key risks faced by the Company and prioritize them as per the criticality:

We will help you:

- Define criteria to evaluate the focus areas which your management teams have identified for potential review.
- Determine each focus area's importance to your business strategy and the likelihood of a control weakness in that area.
- Assess and prioritize your risks and overall risk appetite.
- Select potential focus areas and prioritize focus areas by risk / value.



IT Risk Rating

Prioritize the risks applicable to the audit universe components using the risk criteria.

Confirm the *risk criteria* used and defined for prioritization.

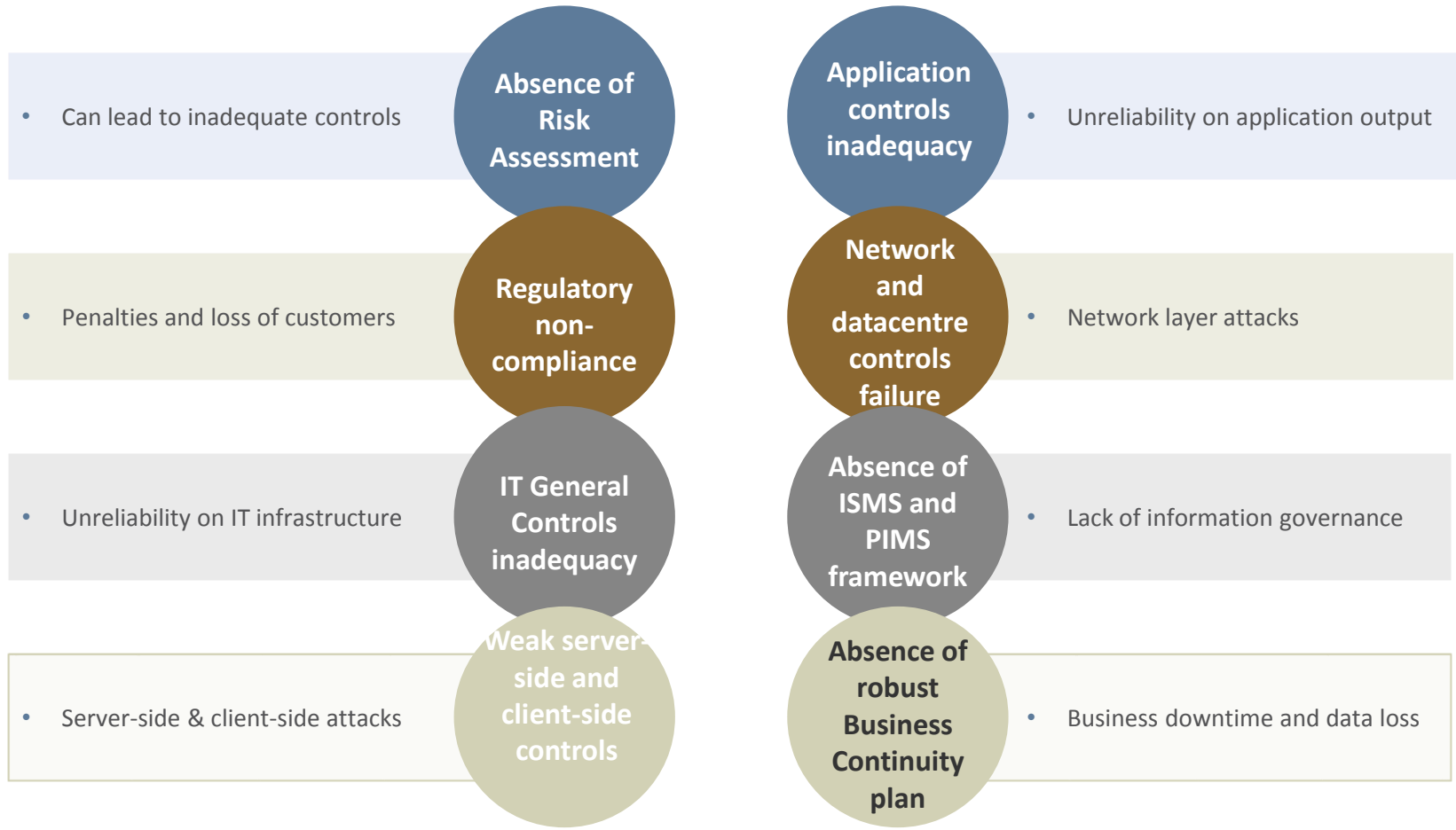
Assign weighting to different components to arrive at the overall risk score for each business unit.

Identify *inherent risks*.

Create *IT risk maps* plotting the impact / likelihood risk scores for entities.

Illustrative IT Risk Universe

Key IT Risk Areas and Repercussions



SIA 15

Knowledge of the Entity and it's Environment

SIA 15 - Knowledge of the Entity and its Environment

The internal auditor should:

- Obtain **knowledge of the economy, the entity's business and its operating environment**, including its **regulatory environment** and the industry in which it operates, sufficient to enable him to review the key risks and entity-wide processes, systems, procedures and controls.
- Prior to accepting an engagement he should obtain a **preliminary knowledge of the industry**.
- Follow the acceptance of the engagement, further and more detailed information should be obtained.
- In case of continuing engagements, he should **update and re-evaluate information** gathered previously.
- Relevant industry factors include industry conditions such as the **competitive environment, supplier and customer relationships, and technological developments**.
- Consider how this knowledge is acquired, affects his review of the internal controls and systems taken as a whole and whether his overall entity-wide assessment of systems, procedures, controls and risk management principles are consistent with his knowledge of the entity's business.
- The information and knowledge obtained by the internal auditor on the entity and its environment should be adequately **documented in the engagement working papers**.

SIA 16

Using the Work of an Expert

SIA 16 - Using the Work of an Expert

The internal auditor should:

- Obtain technical advice and assistance from competent experts if the internal audit team does not possess the necessary knowledge, skills, expertise or experience needed to perform all or part of the internal audit engagement.
- When the internal auditor uses the work of an expert, **he should satisfy himself about the competence, objectivity and the independence of such expert.**
- When determining whether to use the work of an expert or not, the internal auditor should consider:
 - The **materiality** of the item being examined.
 - The **nature and complexity** of the item including the risk of error therein.
 - The **other internal audit evidence** available with respect to the item.
- He should satisfy himself as to the expert's skills and competence by considering:
 - The expert's professional qualifications or membership.
 - The reputation of the expert in the relevant discipline.
 - The knowledge and specific experience of the expert.
- Satisfy himself that the expert has no personal, financial or organizational interests that will prevent him from rendering **unbiased and impartial judgments and opinion.**
- Gain knowledge regarding the terms of the expert's engagement, **the objectives and scope of the work, a general outline as to the specific items, access to records, personnel and physical properties, the ownership and custody of engagement documentation, the confidentiality of the expert's work, expert's relationship with the auditee, confidentiality of the auditee's information used by the expert.**
- Should seek **reasonable assurance** that the expert's work constitutes **appropriate evidence** in support of the overall conclusions formed during the internal audit engagement.

SIA 17

Consideration of Laws and Regulations in an Internal Audit

SIA 17 - Consideration of Laws and Regulations in an Internal Audit

The objectives of the internal auditor are:

- To obtain **sufficient appropriate audit evidence regarding compliance with the provisions of those laws and regulations** generally recognized to have a direct effect on the determination of material amounts and disclosures in the financial statements.
- To **perform specified audit procedures to help identify instances of non-compliance with other laws and regulations** that may have a significant impact on the functioning of the entity.

The internal auditor shall remain alert to the possibility that other audit procedures applied may bring instances of non-compliance or suspected non-compliance with laws and regulations to the internal auditor's attention, for example:

- Inquiring of the entity's management.
- Performing substantive tests of details of classes of transactions.
- The internal auditor shall request management and, where appropriate, those charged with governance to provide written representations that all known instances of non-compliance or suspected non-compliance with laws and regulations. **Written representations provide necessary audit evidence about management's knowledge of identified or suspected non-compliance** with laws and regulations.
- The internal auditor may consider whether, unless prohibited by law or regulation, **withdrawal from the engagement** is necessary when management or those charged with governance do not take the remedial action that the internal auditor considers appropriate in the circumstances.
- In the internal auditor's judgment, the non-compliance referred to in paragraph 41 is believed to be intentional and material, the internal auditor shall communicate the matter to those charged with governance as soon as practicable.

SIA 18

Related Parties

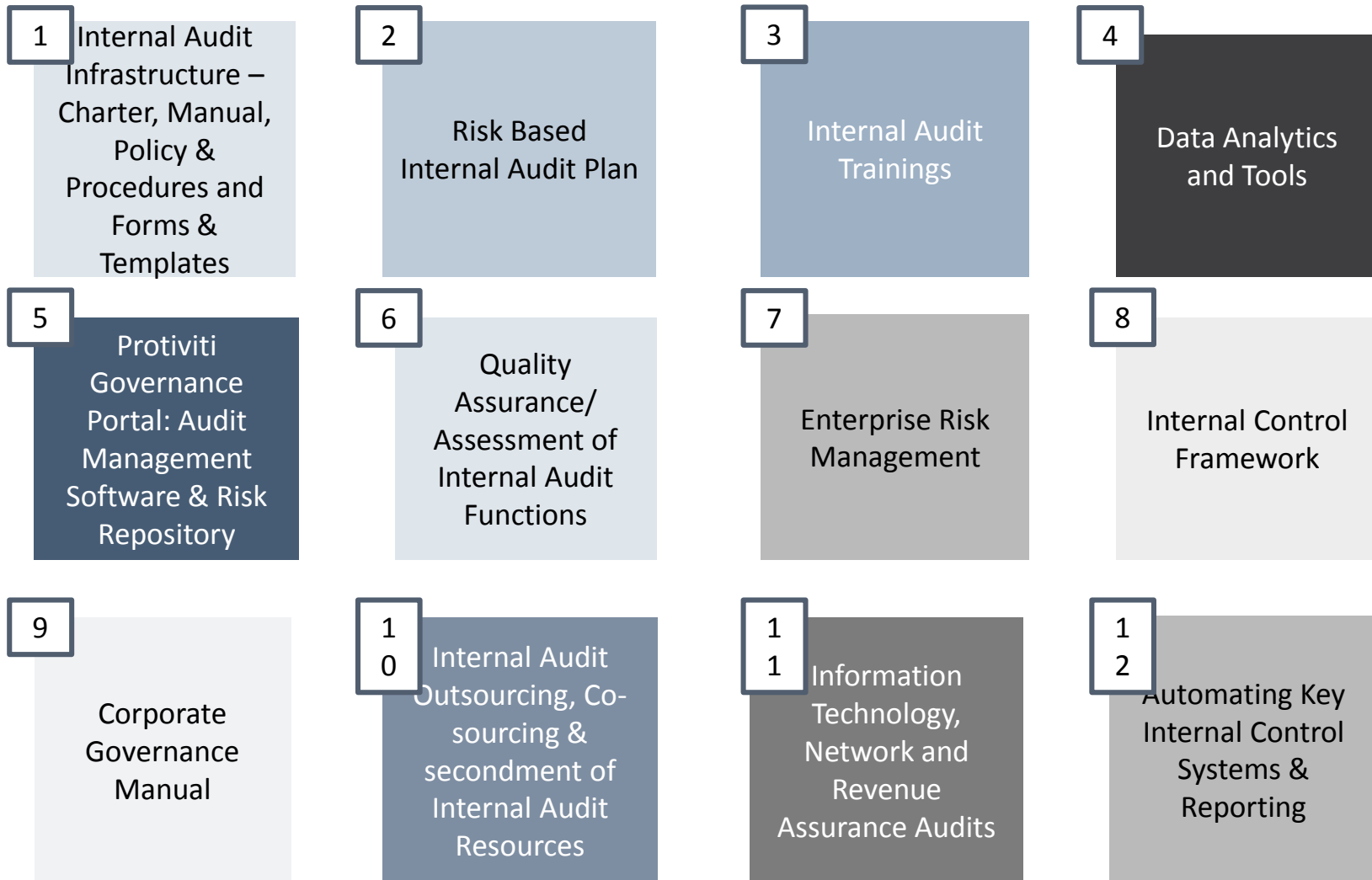
SIA 18 - Related Parties

The purpose of this SIA is to **establish standard and provide guidance on the procedures** to be followed by the internal auditor **in ensuring that related party activities of the entity are properly captured through internal controls.**

- The internal auditor **shall gather the following information** pertaining to related party relationships and transactions:
 - The **identity of the entity's related parties** including changes from the prior period; The nature of the relationships between the entity and these related parties.
 - Whether the entity has **entered into any transaction** with these related parties during the period and, if so, the nature and extent, and the purpose of the transaction.
 - **Document the names of the identified related parties and the nature** of the related party relationships.
 - Communicate with those charged with governance, or relevant committee thereof, such as, audit committee, any significant matters arising during the internal audit in connection with related parties.
- With regard to significant related party transactions outside normal course of business, the internal auditor should inspect underlying contracts or agreements, if any, and evaluate whether:
 - Rationale suggests possible **fraudulent financial reporting or concealment** of misappropriated assets.
 - Terms are consistent with management's explanations.
 - Transactions are accounted for and disclosed in accordance with the generally accepted accounting principles.
 - Ensure transactions have been appropriately authorized and approved.
- The internal auditor should **obtain sufficient appropriate audit evidence** about management's assertion that a related party transaction was conducted on terms equivalent to those prevailing in an arm's length transaction.

Q&A Time!

Professional Support towards SIAs





*Powerful Insights.
Proven Delivery.®*

Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti India, a Member Firm of Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.