

An aerial view of a city at night, with a digital overlay of white location pins and connecting lines. The pins are scattered across the cityscape, and lines connect some of them, creating a network-like pattern. The background is a dark, blue-tinted image of a city with lights and buildings.

RISK BASED INTERNAL AUDIT PLAN PREPARATION

PUNE BRANCH OF WIRC OF ICAI

8th May, 2023

TABLE OF CONTENTS



1. Introduction	02
2. Standards on Internal Audit	03
3. SIA 220: Conducting overall Internal Audit Planning	04
4. 2010: Planning	11
5. Approach – Risk Assessment And Planning	13
6. Case Study – Risk Based Internal Audit Plan Development	32

INTRODUCTION

There were **no guidelines or standards** for performing internal audit in India until early 2000s. Many professionals apart from Chartered accountants were engaged into internal audit activities. **Absence of clear set of standards or guideline lead to ambiguities and non-standardization of internal audit activities.** The **Institute of Chartered Accountants of India (ICAI)** being reputed professional body **developed Internal Audit Standards Board (IASB)** to strengthen internal audit practices and provide adequate guidance to its members and other professionals.

The **Internal Audit Standards Board (IASB)** is one of the non-standing technical Boards of the Institute of Chartered Accountants of India (ICAI) and was **constituted on February 5, 2004**. The **Board is working relentlessly to bring out high quality technical literature** in the form of Standards on Internal Audit and Technical Guides/ Studies/ Manuals, which constitute an important tool in helping the internal auditors to provide effective and efficient internal audit services to the clients and/ or employers. The Standards represent a codification of the best practices for internal auditors and will go a long way in strengthening the position and building up the performance benchmarks for internal auditors.

The **Institute continuously strives to stay at the cutting edge of best practice**, including those in the field of Internal Audit. Therefore, to be effective, Internal Audit must be conducted in accordance with a set of recognized Standards. **Standards on Internal Audit (SIAs)** issued by IASB **are aimed to increase the overall quality, credibility, consistency and comparability of the work performed by the Internal Auditors.**

SIAs are performance benchmarks as they **represent best practices in internal auditing and other assurance services** performed. IASB has initiated process of making Standards on Internal Audit mandatory for certain class of companies in a phased manner.

STANDARDS ON INTERNAL AUDIT (SIA) BY ICAI

Preface to the Framework and Standards on Internal Audit

Framework governing Internal Audits

Basic Principles of Internal Audit

❖ 100 Series: Standards on Key concepts

- SIA 110: Nature of Assurance
- SIA 120: Internal Controls
- SIA 130: Risk Management
- SIA 140: Governance
- SIA 150: Compliance with Laws and Regulations

❖ 200 Series: Standards on Internal Audit Management

- SIA 210: Managing the Internal Audit Function
- SIA 220: Conducting Overall Internal Audit Planning
- SIA 230: Objectives of Internal Audit
- SIA 240: Using the Work of an Expert
- SIA 250: Communication with those charged with Governance

STANDARDS ON INTERNAL AUDIT (SIA) BY ICAI

❖ 300-400 Series: Standards on the Conduct of Audit Assignments

- SIA 310: Planning the Internal Audit Assignment
- SIA 320: Internal Audit Evidence
- SIA 330: Internal Audit Documentation
- SIA 350: Review and Supervision of Audit Assignments
- SIA 360: Communication with Management
- SIA 370: Reporting Results
- SIA 390: Monitoring and Reporting of Prior Audit Issues

❖ 500 Series: Standards on Specialised Areas

- SIA 520: Internal Auditing in an information technology environment
- SIA 530: Third Party Service provider

SIA 220
**CONDUCTING OVERALL INTERNAL AUDIT
PLANNING**

SIA 220: CONDUCTING OVERALL INTERNAL AUDIT PLANNING

Introduction

Internal audit planning can be categorized in following manner:

SIA 220 : Conducting overall Internal Audit Planning

Overall audit plan at overall organization level for specific time period (generally a year) and presented to either Board of Directors / Audit committee



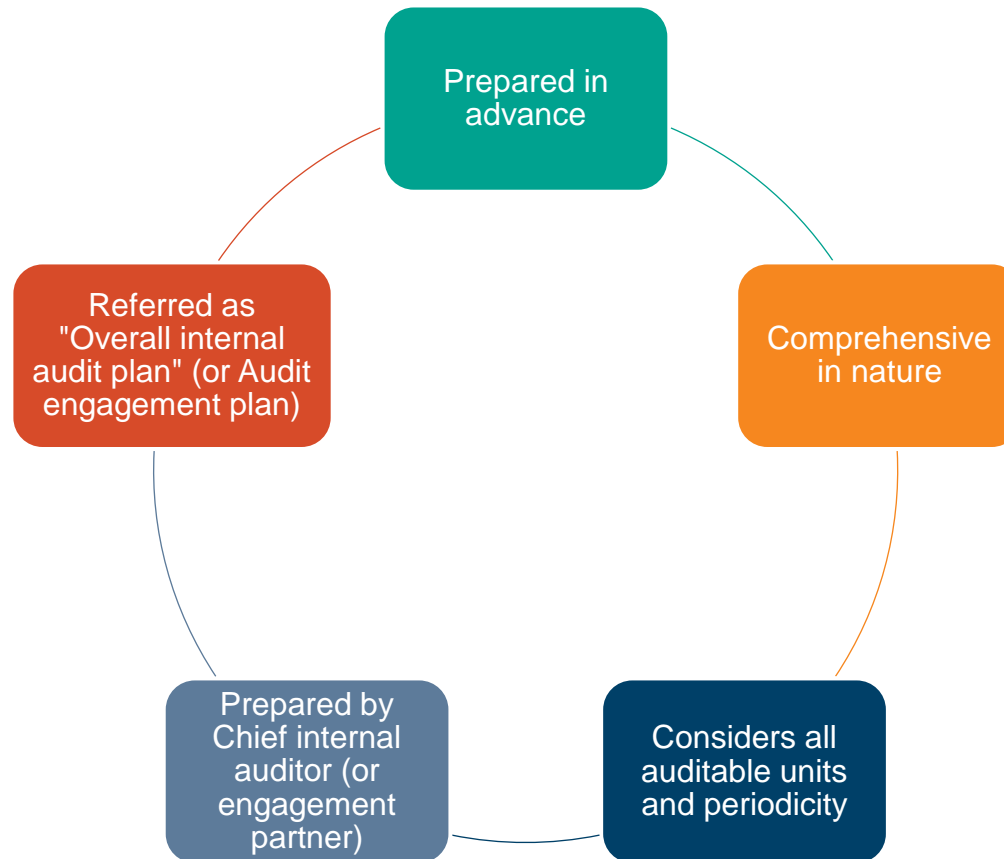
SIA 310 : Planning the Internal Audit Assignment

Specific internal audit plans at individual assignment level and presented to Chief internal auditor.

As per rule 13(2) of companies (Accounts) rules of the companies act, 2013 Board of Directors or Audit committee in consultation with internal auditor shall formulate scope, functioning, periodicity and methodology for conducting audit.

SIA 220: CONDUCTING OVERALL INTERNAL AUDIT PLANNING (CONTD.)

Key elements of overall internal audit planning

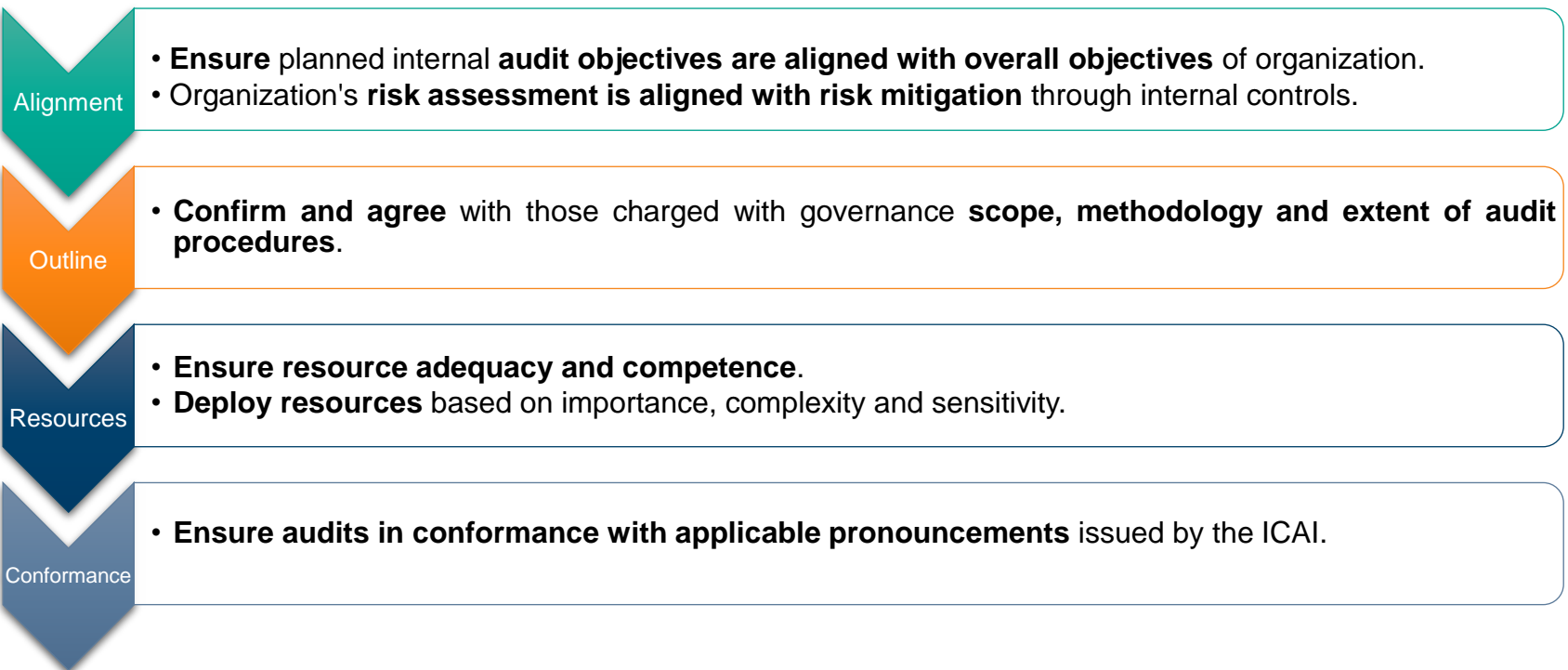


SIA 220: CONDUCTING OVERALL INTERNAL AUDIT PLANNING (CONTD.)

Scope

This SIA **deals with** internal **auditor's responsibility to develop overall internal audit plan**. Where part of internal audit is outsourced, SIA shall apply to the extent auditor needs to plan outsourced activities in accordance with terms of engagement.

Objective



SIA 220: CONDUCTING OVERALL INTERNAL AUDIT PLANNING (CONTD.)

Requirements

1

Planning shall be documented containing all essential elements required to achieve objectives. Technology deployment and resource allocation shall form essential features.

2

Overall internal **audit plan to be reviewed and approved by highest governing body** for internal audits, normally BoD or Audit committee.

3

Knowledge of entity, business and operational environment is essential to determine type of assignment which could be conducted. Discussion with management to understand intricacies.

4

Audit universe to be prepared before defining overall internal audit plan. Scope should be aligned with objectives as per audit charter, nature and extent of assurance to be provided.

5

Risk based planning exercise by undertaking independent risk assessment to be undertaken **to identify and focus high risk areas** with due attention to important, complex and sensitive matters.

6

Continuous monitoring of audit universe and audit plan to ensure achievement of objectives. Any deviations and plan modifications to be documented and approved by approver of original plan.

SIA 220: CONDUCTING OVERALL INTERNAL AUDIT PLANNING (CONTD.)

Explanatory comments

- 1. The planning process:** Internal auditor shall use professional judgement in all planning activities. Documented planning process to be in place stating essential inputs, steps to complete planning and nature of output required.
- 2. Knowledge of business and its environment:** Understand entity's business operations to understand risk faced and operational challenges. Knowledge shall be sufficient to identify significant effect on organization's financial health. Hence financial aspects then to be linked with other business elements such as industry dynamics, business model, operational intricacies, legal and regulatory environment, and system and processes in place.
- 3. Discussion with management and stake holders:** key element of planning is extensive discussion with stakeholders, executive management, risk owners, process owners, statutory auditors etc. as their inputs are critical to understand intricacies, identify important matters and align stakeholder's expectations.
- 4. Audit universe and scope of coverage:** All auditable units (locations, functions, business units, legal entities referred as "Audit universe" shall be identified before defining scope of internal audit. Establish the scope of internal audit. Clearly highlight scope limitations, if any in the internal audit plan to approving body.
- 5. Risk assessment:** Internal auditor shall independently assess risk of all auditable units and align with risk assessment by management and statutory auditor. The internal auditor may also plan to undertake a dedicated audit of the company's Risk Management Framework and processes, as a separate review or assignment.
- 6. Technology deployment:** Understanding extent of information technology deployment in business, operations and transaction processing. Internal auditor need to deploy information technology tools, data mining, analytical procedures and expertise required to conduct audit procedures.

SIA 220: CONDUCTING OVERALL INTERNAL AUDIT PLANNING (CONTD.)

- 7. Resource allocation:** Detailed work schedule to be prepared considering time required for each assignment based on attention required (based on risk assessment) and map with competencies (knowledge, experience and expertise) of available resources. Requirements are then matched to finalise scope and extent of assignment, critical skill/expertise gap in audit team and seek other means of acquiring additional resources.

Documentation

Essential documentation shall be as follows:

- a) Information about business, processes, operations, systems and past or present issues.
- b) Audit universe and summary of auditable units.
- c) Summary of meeting and communication with key stakeholders.
- d) Risk assessment documentation.
- e) Details of available resources, their competence and match with audit requirements.
- f) Final overall internal audit plan duly approved by competent authorities (i.e. Board or Audit committee).

2010: PLANNING

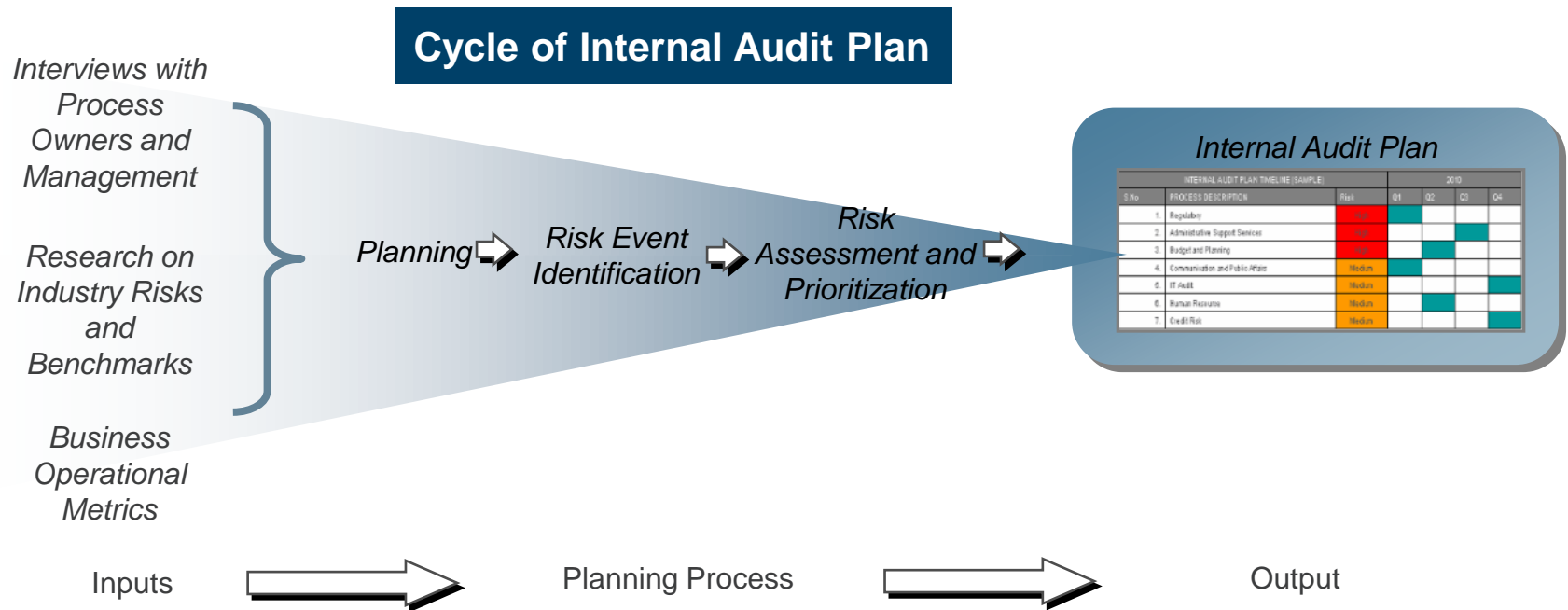
(As per International Standards for the Professional practice of Internal Auditing)

2010: PLANNING

CAE must establish a risk - based plan to determine the priorities of the internal audit activity.

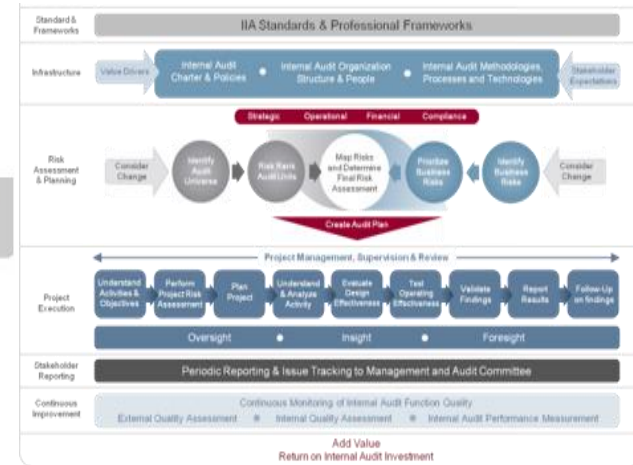
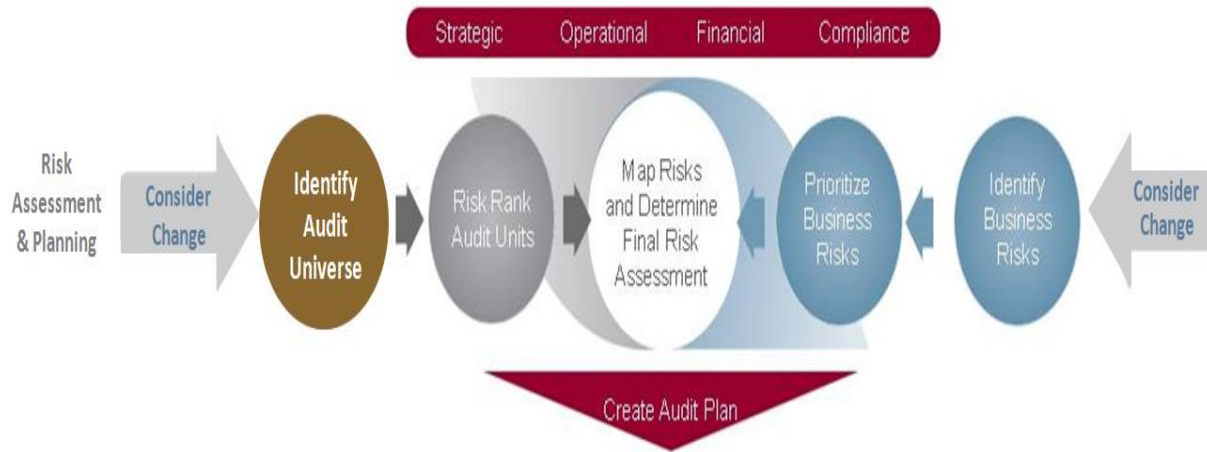
What all are the **Responsibilities of CAE?**

- 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.



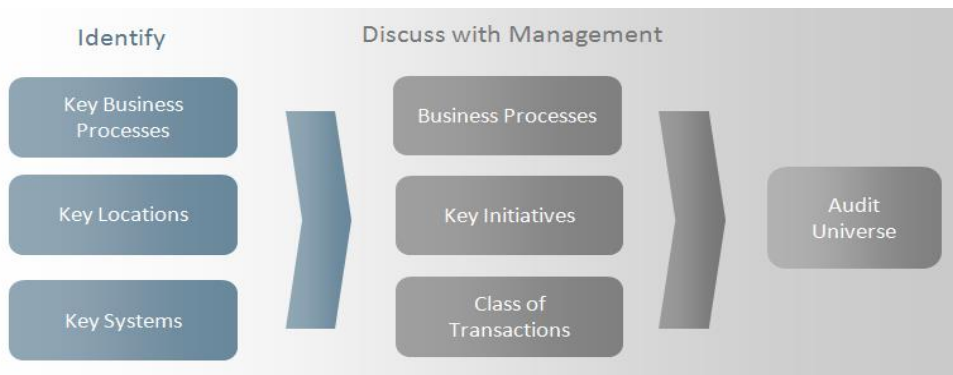
APPROACH RISK ASSESSMENT AND PLANNING

APPROACH – RISK ASSESSMENT & PLANNING



Identify Audit Universe

- We will identify the audit universe at the beginning of our relationship with audit client.
- Identifying an audit universe entails the following considerations:



Audit Universe – Process Listing

Sr. No.	Process Name	Name of the Process and Sub-process
	<u>Section 1</u>	<u>Customer Management</u>
	<u>Section 1.1</u>	<u>Marketing</u>
1	CM.01.01.01	Capture Customer Insights and Develop Marketing Strategies
2	CM.01.01.02	Manage Brand, Advertising, and Sponsorship Agreements
3	CM.01.01.03	Manage Subsidies/Upgrades and Promotions
4	CM.01.01.04	Manage Customer Loyalty and Churn Prevention
	<u>Section 1.2</u>	<u>Customer Relations Management</u>
5	CM.01.02.01	Vet Credit and Accept Customers
6	CM.01.02.02	Provision Services and process Customer Orders
7	CM.01.02.03	Implement and Update Customer Master Data including Customer Privacy
8	CM.01.02.04	Adjustments and Issue Credits
9	CM.01.02.05	Customer Complaint Management
	<u>Section 1.3</u>	<u>Sales Management</u>
10	CM.01.03.01	Manage Individual Customer Contracts and Conditions
11	CM.01.03.02	Manage Distributors and Other Channels
12	CM.01.03.03	Manage Retail Outlets including Sales
13	CM.01.03.04	Manage Enterprise Sales
14	CM.01.03.05	Commission and Incentive
	<u>Section 2</u>	<u>Supply Chain Management</u>
15	SC.02.01	Procurement - Planning, Demand Management and Sourcing
16	SC.02.02	Supplier Management
17	SC.02.03	Inventory, Warehousing and Logistics
	<u>Section 3</u>	<u>Product Management</u>
18	PM.03.01	New Product Development, Product Portfolio and Product Life Cycle
19	PM.03.02	Manage Tariff Information
20	<u>Section 4</u>	<u>Human Resource Management</u>

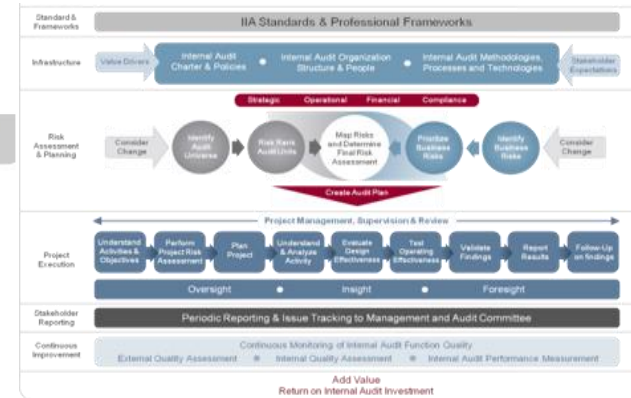
Extract of Audit Universe (Process listing) for manufacturing organization		
Sr. No.	Process code	Name of process and sub-process
	<u>Section 1</u>	<u>Supply Chain Management</u>
1	SCM.01.01	Strategy and Planning
2	SCM.01.02	Sourcing
3	SCM.01.03	Procurement
4	SCM.01.04	Supplier Management
5	SCM.01.05	Inventory, warehousing and Logistics
	<u>Section 2</u>	<u>Product Life Cycle Management</u>
6	PLC.01.01	New product development
7	PLC.01.02	Product portfolio and lifecycle management
	<u>Section 3</u>	<u>Production Management</u>
8	PM.01.01	Production planning
9	PM.01.02	Production capacity utilization
10	PM.01.03	Quality management

Extract of Audit Universe (Process listing) for service organization

Sr. No.	Process code	Name of process and sub-process
	<u>Section 1</u>	<u>Sales Management</u>
1	SM.01.01	Manage customer contracts and conditions
2	SM.01.02	Manage distributors and other channels
3	SM.01.03	Manage enterprise sales
4	SM.01.04	Commission and incentives
	<u>Section 2</u>	<u>Technology Management</u>
5	TM.01.01	Change technology
6	TM.01.02	Manage system development
7	TM.01.03	Manage technology change
	<u>Section 3</u>	<u>Strategic Management</u>
8	STM.01.01	Programme formation and execution
9	STM.01.02	Manage alliances, partnerships and outsourced services
10	STM.01.03	Mergers and Acquisitions

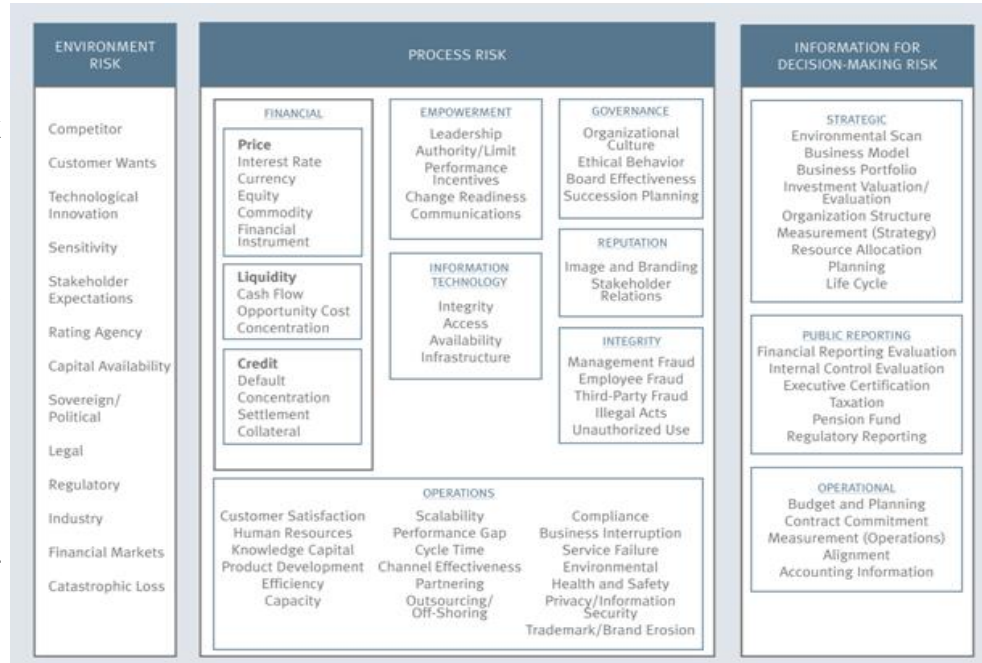
Extract of Audit Universe (Process listing) for finance sector organization		
Sr. No.	Process code	Name of process and sub-process
	<u>Section 1</u>	<u>Lending operations</u>
1	LO.01.01	Commercial Loans
2	LO.01.02	Consumer Loans
3	LO.01.03	Real Estate Loans
4	LO.01.04	Credit Administration
	<u>Section 2</u>	<u>Treasury Management</u>
5	TM.01.01	Securities
6	TM.01.02	Cash Management
7	TM.01.03	Asset/Liquidity Management
8	TM.01.04	Automated Clearing House
	<u>Section 3</u>	<u>Accounting and Financial reporting</u>
8	AFR.01.01	General Accounting
9	AFR.01.02	Financial reporting

APPROACH – RISK ASSESSMENT & PLANNING (CONTD.)

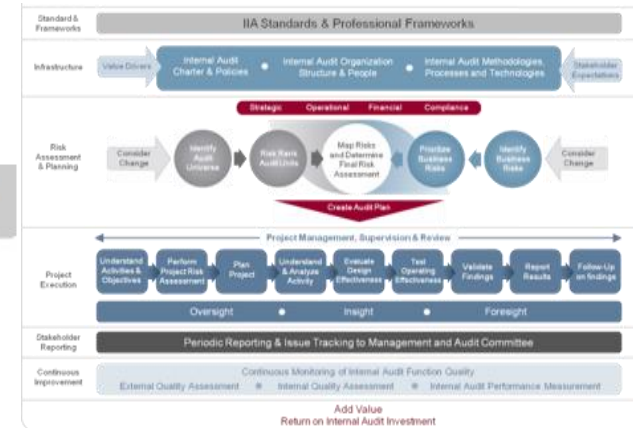


Identify Business Risks

- 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 client's industry, business and environment **by utilizing 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 in information relevance and reliability
- We shall consolidate this information to develop an initial business risk universe.

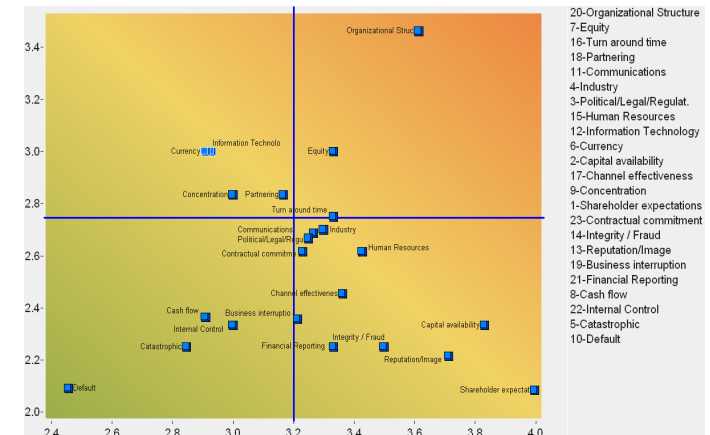


APPROACH – RISK ASSESSMENT & PLANNING (CONTD.)

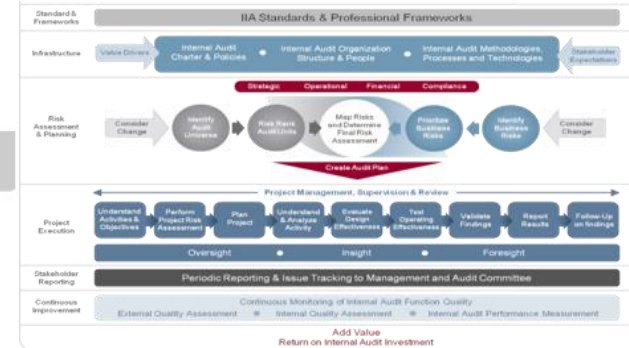


Prioritize Business Risks

- During identification of business risks, we shall **gain an understanding of the overall “tone at the top”** of client 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, organization wide assessment of all types of risk affecting Client** 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 client organization.
- 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.



APPROACH – RISK ASSESSMENT & PLANNING (CONTD.)

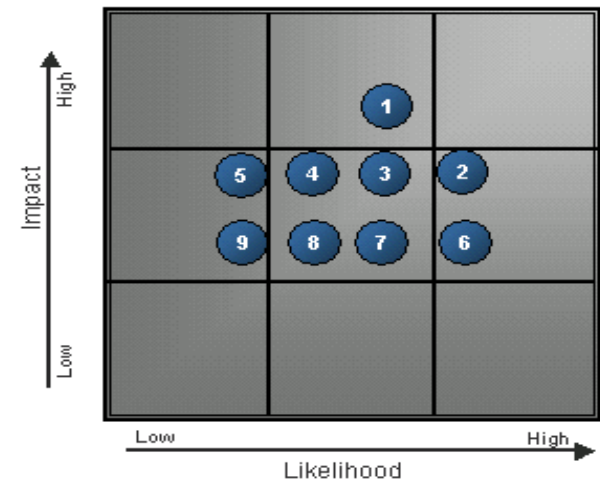


Risk Rank Audit Units

- 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.



Criteria in Audit Planning

New inputs

Strategic risk Perception

❖ Strategic risk

Process and Entity Risk Perception

❖ HoA / MPoR
❖ Entity risk factor

Financials

❖ Financials*

Entity Control Environment

❖ KCQ*
❖ COSO
❖ Top management turnover
❖ Time since last audit
❖ Past audit results

Each input will be appropriately weighted in the audit plan

* = KCQ and Financials will still be used as key inputs in the planning process but their weight will be reviewed

APPROACH – RISK ASSESSMENT & PLANNING (CONTD.)

Internal Audit Risk Rating Criteria

Risk Factors	Impact		
	High	Medium	Low
Materiality / Financial Impact	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. LAs exist but needs some amendments. Minor project delays leading to loss. Project expenses escalating affecting profitability. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Violations, which may lead to financial penalties from regulatory / statutory bodies. 	<ul style="list-style-type: none"> Violations, which may lead to warnings being issued by regulators / statutory bodies. 	<ul style="list-style-type: none"> Violations of negligible impact.
Reputation	<ul style="list-style-type: none"> Bad publicity or damage to reputation from a country / regional / global perspective. Major loss of trustees confidence. Major loss in confidence of financial institutions. 	<ul style="list-style-type: none"> Bad publicity or damage to reputation from some segments of customers / parties. Minor loss in confidence of trustees or financial institutions. 	<ul style="list-style-type: none"> Bad publicity or damage to reputation from few customers / parties.

ILLUSTRATIVE

APPROACH – RISK ASSESSMENT & PLANNING (CONTD.)

Internal Audit Risk Rating Criteria

Impact			
Risk Factors	High	Medium	Low
Customer impact	<ul style="list-style-type: none"> Dissatisfaction of a large segment of customers or high value customers 	<ul style="list-style-type: none"> Dissatisfaction of few key customers 	<ul style="list-style-type: none"> Dissatisfaction of few low segment customers
Legal	<ul style="list-style-type: none"> Legal action leading to significant reputation / financial damage 	<ul style="list-style-type: none"> Legal action leading to moderate reputation / financial damage 	<ul style="list-style-type: none"> Legal action leading to minor reputation / financial damage
Information Technology	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Less confidential information / data loss from server Breakdown of key IT applications System Downtime for 4 hours 	<ul style="list-style-type: none"> Information / data loss from server, which are of least importance. Breakdown of minor IT application (say email system) System Downtime for 2 hrs.
People	<ul style="list-style-type: none"> Employee has recently been transferred, no experience or training on current profile. Earlier track record of disciplinary cases against the Employee. 	<ul style="list-style-type: none"> Employee has recently been transferred, no experience but has undergone training on current profile. 	<ul style="list-style-type: none"> 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%

ILLUSTRATIVE

Planning Database / Tools

Key inputs

MPoR

- CFO
- CEO
- Other top mgrs

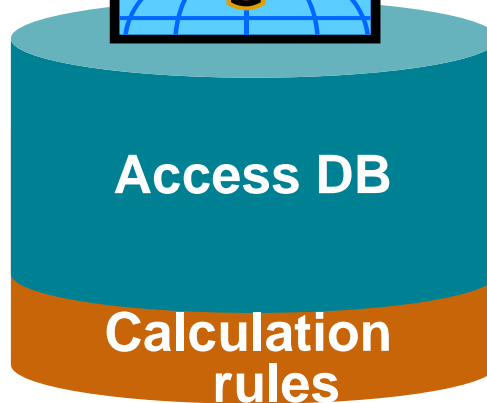
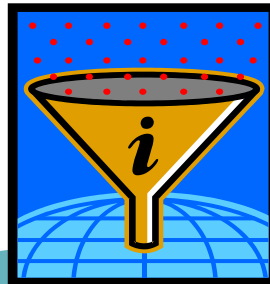
Financial risk

- Total Revenues
- Total Assets
- EBITDA
- Operating Cash Flow

KCQ

- C1.01 Manage New Product Development
- C1.02 Manage Brand, Advertising
- ...

Tool



Key Output

plan

Internal Audit Plan

25 Sep

Nick Ho

Group A

	PK Risk	Follow UP	Change A/R
Risk banding: 1			
Vodafone Group Plc			
R402 Group Financial Reporting	200	0	0
R404 Manage Group Treasury	200	0	0
R406 Manage Payment Security	200	0	0
R407 Manage Tax Plan and Ensure Tax Compliance on Group level	200	0	0
Vodafone UK			
C304 Manage Legal Security	0	0	40
Vodafone Spain			
C202 Provision Services	270	0	4
F002 Manage Strategic Alliance and Outsourced Services	40	0	0
Vodafone Germany			
C7 Business Continuity Planning	200	0	0
Total days for the Risk Band	162	0	44
Risk banding: 2			
Vodafone Group Services			
C101 Manage New Product Development, Product Portfolio and Product Life Cycle	200	0	0
C302 Manage Individual Customer Contracts and Conditions	0	0	0
C401 Manage Systems Development	0	0	20
C7 Business Continuity Planning	200	0	0
F109 Share Contract Service Revenue with Third parties	200	0	0
Vodafone UK			
C401 Manage Systems Development	200	0	1
C402 Manage Technology Changes	200	0	20
C805 Manage Physical Security	200	0	0
C7 Business Continuity Planning	0	0	0
F103 Recruitment Transfer Employees	200	0	0
F107 Process Pre-paid Contract Service Transactions	200	0	0
F108 Process Pre-paid Contract Service Transactions	200	0	0
F112 Bill Wholesale Customers	0	10	0
F115 Bill Other Revenue	200	0	0

Other the covered

1.0

10 Sept

Page 1

© 2006

© 2006 Vodafone Group
Other Plan as described by law. No part of this document may be reproduced, stored or distributed in any form or by any means, without the prior written consent of Vodafone Group Plc.
10 September 2006
Page 1 of 16

PROCESS LEVEL RATING MECHANISM

- Risk factor approach is generally used while performing organization wide risk assessment since it provides macro level view.
- Under risk factor approach auditor first identifies factors common to all auditable units which may have impact on organization's ability to achieve its objectives.
- Risk factors are not risks themselves but conditions likely to be associated with presence of risk.
- Risk factors can be grouped into categories like strategic, compliance, operational and financial.

Following are examples of defining risk factors, criteria and ratings:

Risk Factor Name	Considerations/Criteria	Ratings and Definition
Loss/Material Exposure	<ul style="list-style-type: none"> ▪ Dollar value at risk. ▪ Annual operating expenses. ▪ Number of transactions. ▪ Impact on other areas of organization. ▪ Degree of reliance on IT. 	<ul style="list-style-type: none"> 5 = high exposure. 4 = above average exposure. 3 = average exposure. 2 = less than average exposure. 1 = little exposure.
Strategic Risk	<ul style="list-style-type: none"> ▪ Public perception / reputation. ▪ Local economic conditions. ▪ Volatility. ▪ Significance to strategy. ▪ Degree of external regulation. ▪ Recent change in legislation or regulatory scrutiny. ▪ Changes in business lines or services. ▪ Significant new contracts. 	<ul style="list-style-type: none"> 5 = high risk. 4 = above average risk. 3 = average risk. 2 = less than average risk. 1 = low risk.

PROCESS LEVEL RATING MECHANISM (CONTD.)

Risk Factor Name	Considerations/Criteria	Ratings and Definition
Control Environment (CE)	<ul style="list-style-type: none"> ▪ Degree of process isolation. ▪ Degree of formalization and alignment of objectives. ▪ New process/system implementation. ▪ In-house vs. third-party process. ▪ Operational management turnover. ▪ Degree of performance monitoring is in place. ▪ Tone at the top. ▪ Formality of processes/procedures. ▪ Impact on customers. 	<p>5 = high risk (very weak CE). 4 = above average risk (weak CE). 3 = average (average CE). 2 = below average risk (strong CE). 1 = low risk (very strong CE).</p>
Complexity	<ul style="list-style-type: none"> ▪ Degree of automation. ▪ Degree of specialization required to perform. ▪ Level of technical detail. ▪ Complexity of structure, architecture involved. ▪ Frequency of change. 	<p>5 = highly complex. 4 = above average complexity. 3 = average complexity. 2 = less than average complexity. 1 = simple.</p>

PROCESS LEVEL RATING MECHANISM (CONTD.)

Risk Factor Name	Considerations/Criteria	Ratings and Definition
Assurance Coverage	<ul style="list-style-type: none"> ■ Type of engagement. ■ Other reviews (external, regulatory). ■ Second line coverage. ■ Follow-up already in place. 	<p>5 = not reviewed in last 4 years (3 years for compliance or high-impact risks).</p> <p>4 = not reviewed in last 3 to 4 years (2 to 3 years for compliance or high-impact risks).</p> <p>3 = reviewed in last 2 to 3 years (1 to 2 years for compliance or high-impact risks).</p> <p>2 = review in last 1 to 2 years (1 year for compliance, high impact).</p> <p>1 = reviewed in last year or initiative in place currently.</p>
Management Awareness	<ul style="list-style-type: none"> ■ Concerns expressed in responses to surveys. ■ Concerns expressed in interviews. ■ Level of risk awareness. 	<p>5 = management concerned, has specific issue and reason.</p> <p>4 = management has general concerns.</p> <p>3 = management is neutral.</p> <p>2 = management has no specific concerns.</p> <p>1 = management can demonstrate effective control over risks.</p>

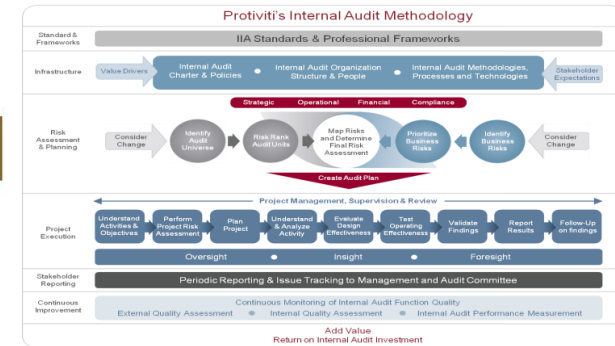
PROCESS LEVEL RATING MECHANISM (CONTD.)

Following are examples of determining total risk score:

Auditable unit	Impact-related Risk Factors			Likelihood-related Risk Factors				Subtotal	Total risk score
	Loss/ material exposure	Strategic risk	Subtotal	Control environment	Complexity	Assurance coverage	Manage- ment awareness		
<i>Weight</i>	50%	50%		35%	35%	20%	10%		
Unit 1	1	2	1.5	2	1	3	1	1.75	3.25
Unit 2	5	5	5	3	1	5	1	2.5	7.5
Unit 3	1	5	3	4	5	4	2	4.15	7.15
Unit 4	5	5	5	5	4	5	4	4.15	9.15
Unit 5	5	2	3.5	4	2	2	4	2.9	6.4
...
Total Risk Score Key	2 to 4 = Low		4.1 to 6.5 = Moderate		6.6 to 8.5 = High		8.6 to 10 = Very High		

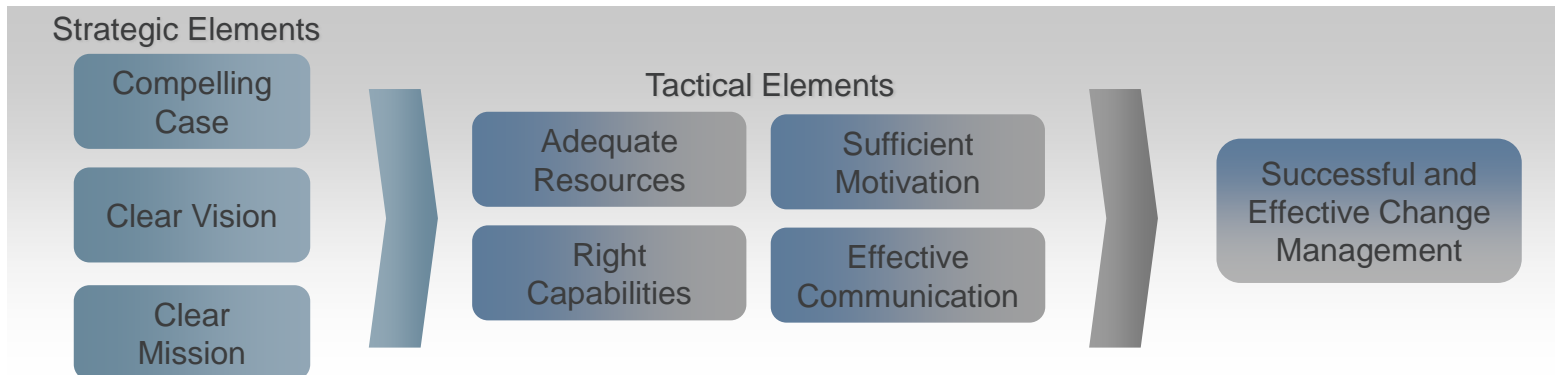
Ranking scale: 1 is lowest; 5 is highest. Lowest possible total score = 2. Highest possible total score = 10.

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.**



Ideal effort allocation and Time coverage

Audit activity nature	Effort
Protect existing value	
❖ Process areas	75 - 80 %
Ensure value creation	
❖ Group projects / Initiatives	20 %
❖ Local Projects / Specials	20 %

CASE STUDY
**RISK BASED INTERNAL AUDIT PLAN
DEVELOPMENT**

RISK BASED IA PLAN - ACTIVITIES PERFORMED

In accordance with the engagement letter, signed between audit client and Internal auditor, the following activities were performed :

1. Internal Auditor **agreed with the client Internal Audit (IA) universe**
2. **Reviewed documents** pertaining to businesses of client
3. **Prepared initial listing of risks** applicable to client
4. **Performing the risk assessment** – ‘Inherent’ & ‘Residual’ Risk
5. **Mapped the risks to various departments/ functions** (IA universe) of client
6. **Performed individual interviews** with client’s senior management
7. **Obtained inputs on total time available for audits** - Client IA department
8. **Developed a risk based IA plan** for Year 1 & Year 2.

1. CLIENT'S BUSINESS STRUCTURE

Corporate

- Centralised: a) Board & Senior Management, b) Corp Development & Communications, c) Legal, d) IT, e) Procurement, f) HR, g) Finance, h) Admin and i) Internal Audit

Client's Group – Various Businesses

1. Maritime & Logistics	2. Offshore	3. Capital	4. Trading	5. Gas & Petrochem
<p>Comprehensive range of services to major importers, exporters and shipping companies in the region, including oil & gas majors. Activities include logistics services, container feeder shipping, NVOCC operations, bulk shipping, shipping agencies, port management and operations, shipyard repairs</p>	<ul style="list-style-type: none"> • Full offshore support services to oil and gas industry locally and across region. • Operates a fleet of more than 30 offshore service vessels, which include safety standby vessels, anchor handling tugs, crew boats, workboats and dynamic positioning (DP) vessels. • Complete range of diving services including saturation diving. 	<ul style="list-style-type: none"> • Corporate finance advisory services to holding group (HG) • Manages HGs proprietary portfolio of financial and real estate investments • Holds the investment in a Quarries Building Materials Company. 	<ul style="list-style-type: none"> • Representation, product marketing, sales and post sales services locally for well-known international truck, heavy equipment, machinery and lubrication brands. • IATA approved travel agency. 	<ul style="list-style-type: none"> • Owns, manages and operates a fleet of LPG and LNG carriers • Provides ocean transportation services to international energy and industrial companies • Owns and manages fleet of container ships • Operates a number of product tankers in partnership with international companies.

2. REVIEWING DOCUMENTS

- The following details were provided by Client's IA team :
 - ❖ Organisation Structure
 - ❖ Management Charters
 - ❖ Annual Report/ Corporate Governance documents/ Audited financials
 - ❖ Chart of Accounts/ DOA/ Policies & Procedures/
 - ❖ IA Audit Reports
 - ❖ IA RCMs
 - ❖ Monthly Company performance Reports
 - ❖ Various Certifications
- These were reviewed by the Audit team along with other industry reports/ own database and list of risks were prepared

3. PREPARING LIST OF APPLICABLE RISKS

- All **applicable risks were divided into the following categories:**
 - ❖ Strategy and business planning
 - ❖ Business Operations
 - ❖ Central Operations and financial planning
 - ❖ Governance & Responsibilities
- The following activity was performed while preparing this document:
 - ❖ List down individual risks under categories mentioned above using sources such as Previous year RACM's, Audit Reports, Knowledge repository, etc.
 - ❖ Risk Owners were defined and documented

4. PERFORMING THE RISK ASSESSMENT

- A **scoring matrix** was mutually decided between Client and Internal Auditor.
- **Risks were assessed, using this scoring matrix at inherent and residual levels** based on likelihood of the event and impact to the business in case of occurrence

Criteria		Very Low	Low	Medium	High	Very High
		1	2	3	4	5
1. Impact	1. Financial	Less than 0.1 % of 2013 group revenue/ group expenses (depending on revenue centre /cost centre) - Less than 3 million QAR	Greater than 0.11 % but lower than 1% of 2013 group revenue/ group expenses (depending on revenue centre /cost centre) - 3 million - 30 million QAR	Greater than 1 % but lower than 3% of 2013 group revenue/ group expenses (depending on revenue centre /cost centre) - 30 million - 90 million QAR	Greater than 3 % but lower than 5 % of 2013 group revenue/ group expenses (depending on revenue centre /cost centre) - 90 million - 150 million QAR	Greater than 5 % of 2013 group revenue/ group expenses (depending on revenue centre /cost centre) - Greater than 150 million QAR
	2. Reputation / Media	No national, regional or international media coverage. However, company has to make public announcement. No impact on share price	Some low level national media coverage, with minor temporary change in share price	High profile short term negative national or regional coverage. Not sustained. Sudden sharp change in share price. However, only temporary	Significant negative national coverage and some short lived international coverage for sustained period of time. Some sustained impact on share price	Significant international negative coverage for sustained period of time. Significant and sustained impact on share price
	3. Regulatory compliance (including stock exchange)	Employees will undertake actions violating corporate ethics standards or implementation and enforcement of these standards will not be effective and consistent with corporate objectives.	Warning or strong recommendation for improvement from regulator but no fine and not made public	Public Warning and minor penalty / fine	Public warning, significant penalty or fine or intense investigation by regulator	Loss of licence / suspension of trade and business for period of at least 6 months
	4. Fraud tolerance	na	na	na	Any employee or customer fraud, including breach of ethics code	Any management fraud
2. Likelihood	Frequency	Potentially once every 11+ years	At least once every 3 - 10 years	At least once every 1-3 years	At least once per annum	Multiple times per annum
3. Vulnerability	Use to assess strength of controls to mitigate the likelihood and impact of the inherent risk	Controls in place mitigate more than 90% of inherent risk	Controls in place mitigate 75 to 90% of inherent risk	Controls in place mitigate 50 to 75% of the inherent risk	Controls in place mitigate 30 to 50% of the inherent risk	Controls in place mitigate less than 30% of the inherent risk

5. MAPPING THE RISKS TO CLIENT'S BUSINESS DIVISIONS

Objective

- ❖ To ascertain where risks lie for each business division
- ❖ A risk rated high for one business division may be rated lower for other business division
- ❖ Facilitate in focusing on individual business units for specific risks rated high/medium

List of Various business divisions of client organization

Corporate Functions	Maritime and Logistics Business Division	Offshore Business Division	Capital Business Division	Trading Business Division	Gas & Petroleum Division
Corporate Devt & Communications	Shipping Agencies	Diving Operations	Real Estate services	Trading management office	Commercial / Chartering
Legal	Marine & logistics management office	Offshore management office	Capital management office	Navigation Travel & Tourism (NTT)	Management office
IT	Port Services	Construction and maintenance	Investment management	Navigation Trading Agencies (NTA)	Operations
Procurement	Navigation Logistics Services	Fleet & technical management office	Financial investments	Bunker Sales (BS)	-
HSSEQ	Container Shipping	QHSE	-	Marine sales & services	-
HR	Shipyard	-	-	Navigation Service Center (NSC)	-
Insurance	Bulk shipping department	-	-	-	-
Finance	Asset Management	-	-	-	-
General Services	-	-	-	-	-

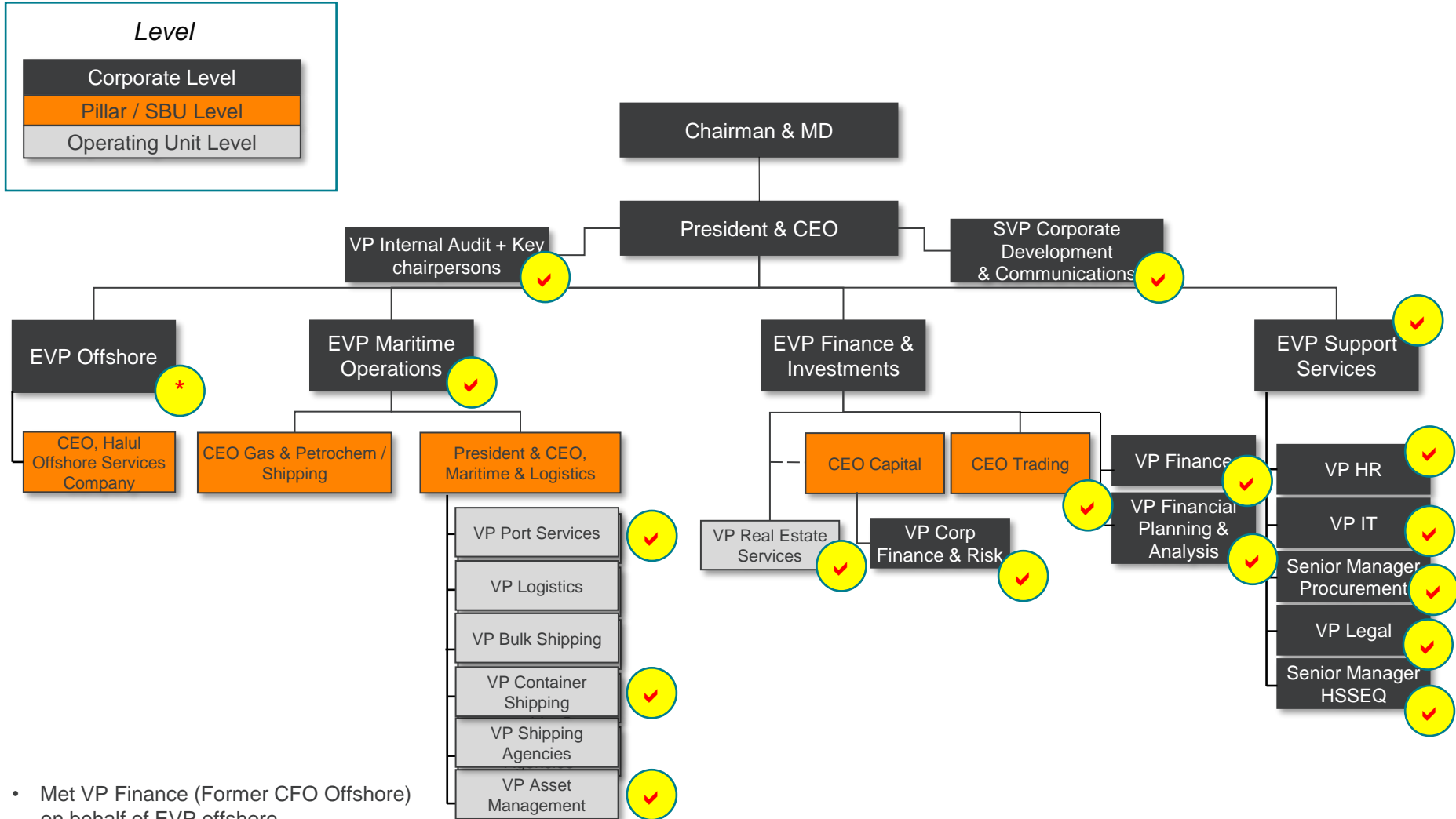
6A. INTERVIEW WITH SENIOR MANAGEMENT

Objective

- ❖ To **enhance awareness of the risk based exercise** and the forthcoming risk based IA plan
 - ❖ To **confirm identified risks and their inherent and residual risk scores** and facilitate mapping to business divisions
 - ❖ To **help identify new risks not previously in the risk list** either in or outside their business unit/ division
 - ❖ To **understand their views on areas internal audit must focus on**
-
- The following activity was performed while preparing for interviews:
 - ❖ Identify and mutually agree with the Head of Internal audit, the list of risk owners to be met (Business Heads/ Group Heads/ Department Heads)
 - ❖ Set up interviews with the risk owners and provide agenda if required
 - ❖ List down individual risks relevant to the risk owner
 - ❖ Prepare questionnaire for the interview

6B. LIST OF CLIENT'S REPRESENTATIVES INTERVIEWED

In delivering risk assessment and IA plan we met with the following representatives:



7. TIME AVAILABILITY OF IA STAFF

- The following activity was performed:
 - ❖ Receive inputs from Client on holidays, leave eligibility, Various management meetings, etc. for the year 1 & year 2.
 - ❖ Estimate total time for follow up reviews of audits performed in prior years.
 - ❖ Estimate time taken for activities such as staff meeting, seminars, IA trainings, etc.

7. TIME AVAILABILITY OF IA STAFF (CONTD.)

Particulars	HIA	Resource							Total
		1	2	3	4	5	6	7	
Total Number of days in year	365	365	365	365	365	365	365	365	
Less : Weekends	104	104	104	104	104	104	104	104	
Less: Public Holidays	10	10	10	10	10	10	10	10	
Less: Ramadan reduced working	9	9	9	9	9	9	9	9	
Less: Annual Leave + Sick leave	32	32	32	32	32	32	32	32	
Total working days	210	210	210	210	210	210	210	210	1680
Less: Audit Follow ups	44	32	20	20	20	20	20	20	196
Less: Preparing Audit Committee Presentation	12	12	0	0	0	0	0	0	24
Less: Arabic Translation	0	4	0	0	0	0	12	0	16
Days required for follow up of audits and audit committee pack preparation	56	48	20	20	20	20	32	20	236
Less: Audit Committee meetings	4	4	0	0	0	0	0	0	8
Less: Management meetings/ tender committee representation	24	6	0	23	0	0	0	0	53
Less: Department Staff meetings	4	4	4	4	4	4	4	4	32
Less: Internal Audit Trainings	5	5	5	5	5	0	5	5	35
Less : IIA Seminars	4	4	4	4	4	0	4	4	28
Less: Administration Work	24	12	12	12	12	12	12	12	108
Days required for trainings / other meetings	65	35	25	48	25	16	25	25	264
Total days for performing internal audits	89	127	165	142	165	174	153	165	1180

8. PROPOSED IA PLAN – YEAR 1

The IA risk assessment identified 93 risks of which 18 were deemed to be high, 55 medium and 20 low. The 2014 and 2015 IA Plans cover all key risks and 50% of the medium risks.

Auditable area	Key Risk	Business Units to be audited	Number of resource days		
			In house*	Outsource	Total
1. MIS & reporting	Ineffective or impractical KPIs to track performance and productivity resulting in not reaching optimum or desired revenue, growth and incurring additional costs (Risk A7) Management is not able to effectively interpret new management accounts and KPIs (Risk A9)		60		60
2. Employee health & safety	Potential oil product pollution, spillages and damages to health (Risk A10)		120		120
3. Contracts management	Customer Contracts are not standardised, not complied with and not legally vetted (Risk A1)		90		90
4. Pricing & discount management	Incorrect pricing resulting in loss of customers, sales and profitability(Risk A16)		90		90
5. Customer management	Over reliance on a small number of key customers and lack of diversification strategy (Risk A2) Inadequate marketing strategy (customer targeting, after sales service, etc.) (Risk A17)		90		90
6. Internal & 3 rd party fraud monitoring & reporting	Ineffective mechanism to identify and report potential frauds and irregular transactions (Risk A4)		90		90
7. Corporate governance framework	Involvement of employees and suppliers in activities of potentially fraudulent nature including misappropriation of assets (Risk A8)		75		75
8. Strategy & Mergers / acquisitions	Planned investments in high value operational assets (vessels, etc) do not generate growth.(Risk A14) Investments in Financial Instruments (AFS, HTM, HFT, FVTPL etc.) did not yield planned results(Risk B2)		60		60
9. Collections management	Ineffective customer & credit management resulting in liquidity issues & financial loss (Risk A12)		120		120
10. Human Resource: Recruitment	Key management resources are not available in sufficient quantity/ quality to operate key business divisions (Risk A13)		45		45
11. Operat'ns & Maintenance	Ineffective resource scheduling (Risk B13)		90		90

Corporate

Marine & Logistics

Trading

Capital

Offshore

Gas & Petroleum

8. PROPOSED IA PLAN – YEAR 1 (CONTD.)

Auditable area	Key Risk	Business Units to be audited	Number of resource days		
			In house	Outsource	Total
12. Planning & budgeting	Ineffective monitoring of strategies by management (Risk B12) Ineffective financial reporting process, including consolidation and preparation of financial reports in accordance with US Accounting Standards & other disclosure requirements (Risk B10)	●	90		90
13. Insurance	Incomplete or delayed insurance coverage of key business operations and people (note: not key assets) (Risk A18) Inadequate insurance coverage over key business assets (Risk B15)	●	45		45
14. Compliance Audit: Labour regulations	Non compliance with Qatar Labour laws (Law 14, 2004 – Labour Rights) (Risk A3)	●	45		45
15. Corporate social responsibility	Ineffective corporate social responsibility programs and management (Risk B14)	●	45		45
16. Change management	Lack of clear change management policies and procedures to implement business reorganization and integration plans (Risk A5)	●	45		45
17. Physical access control	Inadequate physical security and access control over key company assets (Risk A20)	●		Yes	
18. Business continuity & disaster recovery planning	Ineffective response systems to possible breakdowns and damages to shipping fleet (Risk B3)	●		Yes	
19. IT project management	Ineffective management and delivery of planned and ongoing key IT software projects, including cost management	●		Yes	
20. IT capacity availability and utilization	Ineffective utilisation of IT hardware and management of IT capacity needs (Risk B17)	●		Yes	
21. IT infrastructure management	Ineffective management of IT infrastructure, including integration delays (e.g. Shipnet and Oracle integration)	●		Yes	
Follow up activities on open and remediated IA recommendations			216		216
Total			1,416		1,416



8. PROPOSED IA PLAN – YEAR 2

Auditable area	Key Risk	Business Units to be audited	Number of resource days		
			In house*	Outsource	Total
1. MIS & reporting	Ineffective or impractical KPIs to track performance and productivity resulting in not reaching optimum or desired revenue, growth and incurring additional costs (Risk A7) Management may not be able to effectively interpret new management accounts and KPIs (Risk A9)		60		60
2. Customer management	Over reliance on a small number of key customers and lack of diversification strategy (Risk A2) Inadequate marketing strategy (customer targeting, after sales service, etc.) (Risk A17)		90		90
3. Human Resource: Termination & leave	Ineffective management of resource terminations, separations, voluntary leavers, sick pay, leave, time off and overtime (Risk B20)		60		60
4. Internal & external logistics management	Ineffective internal and external logistics of key inventory and equipment		90		90
5. Revenue Recognition & receivables management	Inaccurate or delayed customer invoicing (Risk B18)		90		90
6. Asset management	Ineffective management and physical tracking of assets, such as vessels, equipment, tools, etc. (Risk B9)		60		60
7. Corporate social responsibility	Ineffective corporate social responsibility programs and management (Risk B14)		45		45
8. Human Resource: Retention	Lack of HR succession planning and retention programs for senior and operational personnel (Risk A11)		45		45
9. Human Resource: Reward & Recognition	Unrealistic, misunderstood performance measurement systems for employees (Risk B1) Lack of management of employee remuneration and motivation system (Risk B4) Ineffective processing and payment of employee salaries and reimbursables (Risk B19)		75		75
10. Compliance Audit: Labour regulations	Non compliance with Qatar Labour laws (Law 14, 2004 – Labour Rights) (Risk A3)		60		60
11. Compliance Audit: environmental regulations	Non compliance with relevant Qatari and international environmental legislation		60		60

Corporate

Marine & Logistics












Trading

Capital

Offshore

Gas & Petroleum

8. PROPOSED IA PLAN – YEAR 2 (CONTD.)

Auditable area	Key Risk	Business Units to be audited	Number of resource days		
			In house	Outsource	Total
12. Fleet management	Non optimal planning and utilisation of shipping fleet		60		60
13. Corporate governance framework	Involvement of employees and suppliers in potentially fraudulent activities including misappropriation of assets (Risk A8)		60		60
14. Procurement opex	Irregular supplier selection, contracting and management fails to deliver required material at an economical cost (Risk B11)		60		60
15. Accounting	Inappropriate use of accounting policies and/ or ineffective transactional accounting process (Risk B6) Ineffective or inconsistent use of accounting policies (e.g. valuations and impairments, revenue and cost recognition) (Risk B7)		45		45
16. Fraud management	Lack of company wide fraud management and compliance framework and systems (Risk A6)		60		60
17. Employee health and safety	Potential oil product pollution, spillages and damages to health (Risk A10)		120		120
18. Segregation of duties	Inadequate segregation of duties leading to irregular transactions and process/ decision making inefficiencies (Risk A15)		60		60
19. Delegation of authority	Non optimal or effective organisational structure, reporting lines and delegation of authority			Yes	
20. Strategic planning	Planned investments into Key Non IT projects not yielding expected results (Risk B5) Planned investments into Key IT projects not resulting in cost optimisation/ other benefit to the group (Risk B8) Ineffective process for preparation of strategy and business plans (Risk B16)			Yes	
21. IT data management	Ineffective data management, back up and restoration			Yes	
22. IT management and governance	Ineffective information and technology security management (Risk A19)			Yes	
Follow up activities on open and remediated IA recommendations			216		216
Total			1,416		1,416



Q&A Time!



***Thank you** for being
a lovely audience,
learning together is
always a pleasure*

Murtuza Kachwala

Managing Director

Contact no. +91 9833 015 334

Email: murtuza.kachwala1@protivitiglobal.in
