



Internal Audit Manual

June 2010

Better Practice Guide



Contents

1	Introduction	10
2	Mission, Objectives, Values & Scope	12
2.1	Mission	12
2.2	Objectives	12
2.3	Values	12
2.4	Scope	12
3	Internal Audit Operating Model	14
4	Internal Audit Function Organization	15
4.1	Job Descriptions	15
5	Risk Management	17
5.1	Introduction	17
5.2	Subject Entity Level Risk Assessment	17
5.3	The Risk Management Process Overview	19
5.4	Establish The Overall Risk Management Context	21
5.5	Identify Inherent Risk	22
5.6	Analyze Risk	24
5.7	Qualitative Analysis	28
5.8	Inherent Risk Assessment	28
5.9	Identification & Assessment Of Mitigating Practices & Controls	29
5.10	Residual Risk	30
5.11	Risk Management Assurance & Monitoring	31
6	Risk Assessment And Annual Audit Plan	33
6.1	Develop Detailed Understanding Of The Key Processes	33
6.2	Risk Categories	36
6.3	Inherent Risk Description	37
6.4	Inherent Risk Rating	39
6.5	Perform Evaluation Of Controls Over Risks	40
6.6	Documentation Of Controls	40
6.7	Perform Walkthrough	44
6.8	Assessing Residual Risk	46
6.9	Gap Analysis	47
6.10	Develop High Level Testing Strategy & Annual Audit Plan	47
6.11	Resource Allocation	49



7	Planning Phase	53
7.1	Introduction	53
7.2	Validate High-Level Scope With Management	54
7.3	Develop A Preliminary Work Program For The Audit	55
7.4	Validate/Document Understanding Of The Process/Initiative/Function/Activity Being Audited	56
7.5	Develop Detailed Work Program	57
7.6	Validate That The Work Program Is Aligned With Scope	57
7.7	Budgets	58
7.8	Travel Arrangements	58
8	Execution (Fieldwork) Phase	59
8.1	Introduction	59
8.2	Detailed Work Program	59
8.3	Sampling Techniques	63
8.4	Audit Techniques	67
8.5	Identifying Information	68
8.6	Raising Internal Audit Issues	69
8.7	Co-Develop Action Plans With Management	71
8.8	Audit Supervision	72
9	Reporting Phase	74
9.1	Introduction	74
9.2	Prepare The Draft Internal Audit Report	75
9.3	Review Draft Internal Audit Report	76
9.4	Conduct Formal Closing Meeting	77
9.5	Issue Draft Report	78
9.6	Receiving Management's Feedback & Action Plans	78
9.7	Issue Final Internal Audit Report & Present Results	78
9.8	Internal Audit Reports – Summary & Guidance	79



10	Internal Audit Monitoring And Follow-Up	84
10.1	Introduction	84
10.2	Timing Of Internal Audit Monitoring & Follow-Up	84
10.3	Internal Audit Monitoring	84
10.4	Internal Audit Follow-Up	85
10.5	Implementation Schedule	85
11	Internal Audit Management Reporting	86
11.1	Reports By The Head Of Internal Audit	86
12	Internal Audit Key Performance Indicators	88
13	Corporate Governance	89
13.1	Objectives	89
13.2	Approach	89
14	Quality Assurance	90
15	Personnel Development/Training & Performance Reviews	91
15.1	Staff Profiles/Qualifications	91
15.2	Career Development & Counselling	91
15.3	Professional Development Requirements	91
15.4	Induction Program	91
15.5	Personnel Performance Review	92
16	Audit Administration And Other Matters	93
16.1	Delegations (Financial & Human Resources)	93
16.2	File Naming Convention	93
16.3	Electronic Communication & Email	93
17	Internal Audit Manual Update	95





Appendices

Appendix 1	Introduction to the IT Assurance Methodology
Appendix 2	Audit Committee Charter
Appendix 3	Internal Audit Charter
Appendix 4	Job Descriptions
Appendix 5	Gap Analysis Report Template
Appendix 6	Strategic Internal Audit Plan Template
Appendix 7	Audit Planning Letter Template
Appendix 8	Data Request Form
Appendix 9	Detailed Scope Letter Template
Appendix 10	Internal Audit Report Template
Appendix 11	Follow- Up Report Template



Glossary

The Government	Government of the Emirate of Abu Dhabi
The Executive Council	The Executive Council of the Emirate of Abu Dhabi
Subject Entity	Any Government department, agency, State Owned Entity or State Owned Subsidiaries
Senior Management	Is the highest administrative authority found in the Subject Entity (Chairman/Board of Directors, etc.)
The Audit Committee	The Committee established by the Senior Management of the Subject Entity to oversee audit operations and circumstances
Departments	Government Departments
ADAA	Abu Dhabi Accountability Authority (ADAA)
Internal Auditors	Employees of the Subject Entity's Internal Audit Function
External Auditors	Audit firms who are assigned to provide external or internal audit services
Stakeholders	Every person and / or party with an interest in the Subject Entity, e.g. staff, creditors and clients
Internal Audit	Is an independent, objective assurance and consulting activity designed to add value and improve organizations' operations. It helps organizations to evaluate and improve the effectiveness of risk management, control, and governance processes
The Internal Audit Charter	The Charter that describes the mission, independence and objectivity, scope and responsibilities, authority, accountability and standards of the Internal Audit function at the Subject Entity
The Audit Committee Charter	The Charter that describes the mission, authority, responsibilities and scope of the Audit Committee



Audit Committee report	A report prepared by the Internal Audit Function of the Subject Entity and submitted to the Audit Committee. It includes a summary of the Internal Audit Function's operations during a period of time
Risk based Audit	Risk-based audit is an audit approach that sets materiality thresholds based on risk analysis and develops audit programs that allocate a larger portion of audit resources to high-risk areas
Governance	The set of regulations, criteria and procedures that ensure institutional discipline in managing a Subject Entity with international criteria and practices by determining responsibilities and obligations of the directors and executive management, taking into consideration the protection of shareholders' rights and other stakeholders' interests
Internal control	Systems designed by the management of the Subject Entity in order to achieve objectives, safeguard assets, control and review accounting information, ensure accuracy and reliability of this information, increase the effectiveness, economy, and efficiency of operations and functions, and ensure compliance with the relevant laws and regulations
Code of Business Conduct	Set of rules outlining the responsibilities or proper practices to be applied through the Subject Entity's employees.
Operational processes	Those operations that constitute the Subject Entity's core business
Risks	The uncertainty of an event occurring that could have a negative impact on the achievement of the objectives of the Subject Entity



Risk management	Processes to identify, assess, and manage potential events or situations, to provide reasonable assurance regarding the achievements of the Subject Entity's objectives
Consulting services	Specialized tasks and missions, other than audit, to be performed by the Internal Audit Function of the Subject Entity
Independence	The freedom from conditions that threaten objectivity or the appearance of objectivity of the internal auditor
Key Performance Indicators	Indicators used by the Subject Entity to measure and evaluate the performance of various operational and financial operations.
Best practices	Those practices that have produced outstanding results in another situation and that could be used by the Subject Entity
Fraud	Any illegal acts characterized by deceit, concealment or violation of trust to achieve personal benefits
IIA Standards	Standards for the professional implementation of Internal Audit issued by the Institute of Internal Auditors
Information Technology	Computer-based information systems, particularly software applications and computer hardware applied within the Subject Entity
Conflict of interests	Inconsistency between the interests of the Subject Entity and the interests of any of its employee which arises in connection with the performance of his/her duties
Recovery plans	The process, policies and procedures of restoring operations critical to the resumption of business after a natural or human-induced disaster



1

Introduction

The purpose of this Internal Audit manual is to provide a standardized framework for Internal Audit operations and activities within the Government of Abu Dhabi, with the aim of assisting Internal Audit Functions within all Subject Entities, in addition to supporting internal auditors in executing their work by adhering to best practices such as the IIA Standards.

This manual is not designed to be an all-inclusive outline for performing audits, but rather, has the following purposes:

- To establish policies and standards for the planning, performance, and reporting of audit work
- To establish high level procedures intended to assist staff members in the discharge of their duties
- To formalize administrative and organizational policies for Internal Audit Functions within Subject Entities
- To define responsibility, authority, and accountability
- To help achieve consistency in Internal Auditing activities
- To standardize the internal audit and risk assessment approach within the Abu Dhabi Government in a manner to ensure the consistency in the application of internal audit standards
- To expedite the training of Internal Audit staff

When developing this Internal Audit manual, the Abu Dhabi Accountability Authority structured the document to include all the necessary phases for maintaining an effective audit and risk assessment activity based on a professional Internal Audit Methodology.

Thus, to ensure the proper use and the complete understanding of this manual, users should refer consistently to each of the related chapters depending on the operation or procedure intended for execution.



This manual observes the International Standards for the Professional Practice of Internal Auditing as prescribed by international bodies such as the Institute of Internal Auditors (IIA), while taking into consideration the specific features of governance within the Government of Abu Dhabi. In adopting this Internal Audit manual, the Abu Dhabi Accountability Authority has ensured that the Internal Audit Functions within Subject Entities will adopt the IIA definitions and standards in the performance of Internal Audit work. Internal Auditors at Subject Entities are required to know and understand the contents of this manual before the commencement of any internal audit engagement. This Manual includes all policies and procedures related to all Internal Audit activities.

Note: for a full fledged recap of the various screens and a more comprehensive understanding of the e-Governance portal, kindly refer to the “System User Manual” uploaded to the portal server.



2

Mission, Objectives, Values & Scope

2.1 Mission

The mission of Internal Audit is to provide independent and objective assurance and consulting services designed to assist the Subject Entity in achieving its objectives by striving to provide a positive impact on the efficiency and effectiveness of operations. Internal Audit helps the Subject Entity accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal controls, and governance processes.

2.2 Objectives

The overall objectives of Internal Audit are to provide assurance to Senior Management of the Subject Entity regarding the management of key risks and to provide independent and objective advice and counsel to Senior Management to assist them in discharging their duties and responsibilities.

2.3 Values

- **Integrity** – Internal Auditors are honest, ethical, equitable and respectful with stakeholders.
- **Accountability** – Internal Auditors are responsive and open in dealing with the needs and expectations of stakeholders.
- **Independence** – Internal Auditors provide assurance and governance services in an objective and fair manner.
- **Learning and Innovation** – Internal Auditors continually develop organizational capability through the development of individual and team knowledge and skills.

2.4 Scope

Internal Audit coverage includes all aspects of the Subject Entity's activities in accordance with the Internal Audit Charter approved by the Audit Committee. The extent and frequency of internal audits will depend upon varying circumstances such as the results of previous audits, relative risk associated with activities, materiality, the adequacy of the system of internal controls and resources available at the Internal Audit Function.

Internal Audit Functions perform various types of audits such as:

2.4.1 Compliance Audits

Compliance audit is concerned with the review of financial and/or operating activities of the Subject Entity for the purpose of determining whether they conform to specified conditions, rules, codes, laws or regulations. Internal Audit thus determines whether

the systems of internal control are adequate and effective, and whether audited activities comply with the legislative requirements and relevant regulations.

2.4.2 Performance Audits

These audits involve a systematic review of the Subject Entity's operating activities in relation to specified objectives. They can be referred to as value for money or management audits. They assess performance, identify opportunities for improvement and develop recommendations.

2.4.3 Information Technology Audits

IT Audits are designed to identify strengths and weaknesses in current IT policies, delivery methods, skills and knowledge gaps between corporate strategists and IT project managers to provide advice at all management levels on internal control, but more important, to provide assurance to balance risk and control investment in an often unpredictable IT environment.

The use of specialists and/or outsource of IT Audits would be recommended due to the relative skill set required and the low frequency of such reviews in an organization.

The "Introduction to the IT Assurance Methodology" is set out in detail in Appendix 1.



3

Internal Audit Operating Mode

The Internal Audit Function should operate under the guidance of, and report directly to the Audit Committee established by the Subject Entity, whereas the Committee plays a consultant role regarding audit and corporate governance issues to the Board of Directors of the Subject Entity. The Committee should review and approve the Annual Audit Plan and involve the Chairman/Board of Directors/Executives in the discussion of the audit findings.

From an administrative perspective, the Internal Audit Function should report to the Chairman at Government Departments and the CEO/General Manager with respect to all other Subject Entities.

Please refer to “Audit Committee Charter” in Appendix 2 for more details.

The role of the Internal Audit Function is to provide recommendations and advice in an objective manner independently of the influence of Executive Management to assist them in performing their duties and responsibilities. A full copy of the Internal Audit Charter is outlined in Appendix 3.

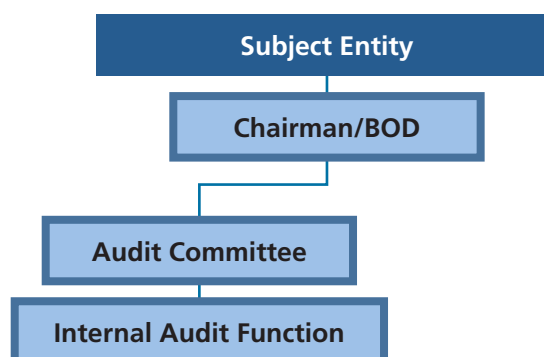
4

Internal Audit Function Organization

The proposal of an appropriate Internal Audit structure designed to perform the tasks efficiently and effectively rests with the Head of the Internal Audit Function. The approval of the Committee should be however sought prior to implementation.

The Head of the Internal Audit identifies the Function's requirements in human resources including required qualifications and skills needed to execute the work, in addition to the identification of the need to use experts from outside parties. It is mandated to obtain the approval of the Committee for all these needs and requirements.

The Internal Audit Function staffing model needs to be flexible to ensure the required skills are available to perform the work.



4.1 Job Descriptions

Job descriptions (JD) outline the roles and key responsibilities for each position. Every employee of the Internal Audit Function should have a current JD including the knowledge, skills and abilities required to perform the duties of the position. It should also reflect all the activities and expectations for that particular position.

Appendix 4 presents sample job descriptions which can be used by Subject Entities as guidance to develop JDs for the various positions of the Internal Audit Function. JDs should be approved by the Head of Internal Audit, while the latter's is approved by the Audit Committee. Ultimately, all job descriptions should be approved by the Human Resources Division within the Subject Entity.

Below is a summary of the key responsibilities for each position:

4.1.1 Head of Internal Audit

The role of the Head of Internal Audit is to direct a comprehensive program of internal audit for the Subject Entity to ensure that internal control systems to support the reliability and integrity of financial, operational and information technology are reviewed at appropriate intervals and effective recommendations are made for corrective actions as required.

Additionally, the role of the Head of Internal Audit is to develop, update and execute the implementation of the Internal Audit Charter as approved by the Committee and in line with the IIA Standards. The Head of Internal Audit establishes goals, performance standards and objectives for subordinates. The goals, performance standards, objectives and remuneration of the Head of Internal Audit are established by the Committee and/or the Board of Directors.

4.1.2 Senior Internal Auditor

The role of the Senior Internal Auditor is to plan, supervise and oversee the various audit activities being carried out by assigned Auditors. The Senior Internal Auditor identifies and evaluates risks associated with the Subject Entity's processes and prepares audit plans, including audit programs and budgets. Also, the Senior Internal Auditor performs detailed reviews of the working papers and drafts the internal audit report.

The Senior Internal Auditor ensures that duties are performed efficiently and professionally and in accordance with the Internal Audit Manual and the IIA Standards. He also performs ad hoc duties as and when requested by the Head of Internal Audit.

4.1.3 Internal Auditor

The role of the Internal Auditor is to conduct Internal Audit assignments as per the approved Annual Audit Plan.

4.1.4 Information Systems Auditor

The Information Systems Auditor facilitates the development of the IT components of the Annual Audit Plan to provide for the effective coverage of the Subject Entity's operations and processes. The Information Systems Auditor leads, conducts and manages complex Information System Audits and System Development Reviews.

4.1.5 Internal Audit Support Officer

The role of the Internal Audit Support Officer is to provide administrative support to the Internal Audit Function. He/she will act as the central point for logistical coordination of Internal Audit activities.

5

Risk Management

5.1 Introduction

This section provides an introduction to the theory of Risk Management. This section should be read in conjunction with Section 6, "Risk Assessment & Annual Audit Plan", which describes how to perform the Risk Assessment and develop the Annual Audit Plan (AAP).

Risk Management is a critical function of the Subject Entity's management. It is central to the rational allocation of resources and the choice of action in the achievement of objectives. Executive Management is responsible for the risk assessment process, control systems and risk mitigation strategies adopted by the Subject Entity.

The Internal Audit Function is accountable for conducting risk assessments and ensuring that the internal controls in place are effective. When risk assessments are not explicit or not documented, the Internal Audit team may work with management to document them.

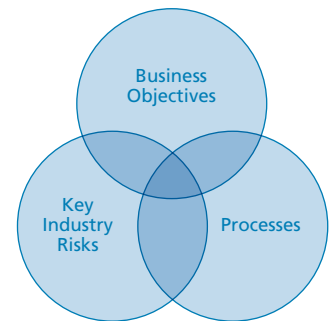
The Internal Audit Function can also assist the Subject Entity by providing advice on the design and improvement of control systems and mitigation strategies, yet management remains accountable for the selection and implementation of controls and strategies.

The Internal Audit Function has the principal responsibility for assuring that the AAP is based on reliable, complete and accurate information about the Subject Entity's operations, activities and its risk profile. Integral to this is having adequate knowledge of the risks to which the Subject Entity is exposed.

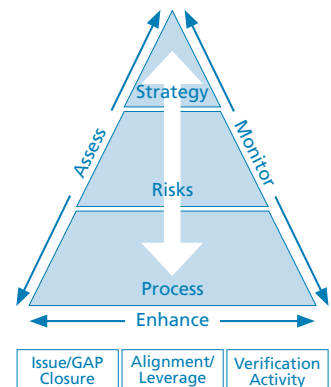
5.2 Subject Entity Level Risk Assessment

Subject Entities should constantly assess their risks. A formal, strategy-based, entity-level risk assessment can help to significantly advance the Subject Entity's ability to understand its key business risks and provides a structured process that becomes the cornerstone for prioritizing risks and focusing attention on areas meriting management review and monitoring. Moreover, this process builds knowledge and confidence as management becomes more adept at understanding the risks it takes and what it should be doing to manage these risks effectively.

How do we identify and assess risks in our organization?



How do we enhance risk coverage in our organisation?



How do we monitor risk in our organisation?

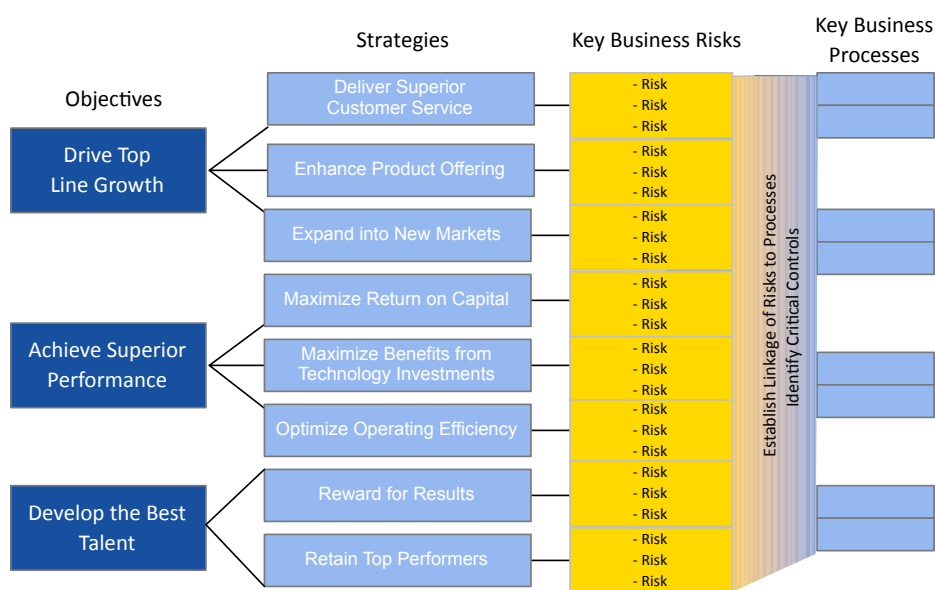


The risk assessment process involves:

- Understanding the Subject Entity's strategies and objectives
- Developing a preliminary understanding of the Subject Entity's key business risks and processes, and aligning them to strategies and objectives
- Understanding the effectiveness of entity-level controls such as the Corporate Governance framework, code of conduct, segregation of duties, business continuity, disaster recovery plans, period end financial reporting processes, fraud prevention/ detection programs, etc.
- Understanding the effectiveness of the controls over key processes that are documented in the Subject Entity's policies and procedures
- Scoping the risk assessment by obtaining input from all key stakeholders
- Assessing, prioritizing, and validating key business risks with the key stakeholders
- Reporting the results of the risk assessment in order to identify the high risk issues and processes within the Subject Entity

Key business risks result from significant events, conditions, actions, or inactions that can adversely affect the Subject Entity's ability to achieve its objectives.

The following chart depicts the relationships between a Subject Entity's business objectives, the strategies designed to help achieve those objectives, the key business risks that may affect the execution of those strategies, and the business processes that support the implementation of the strategies.



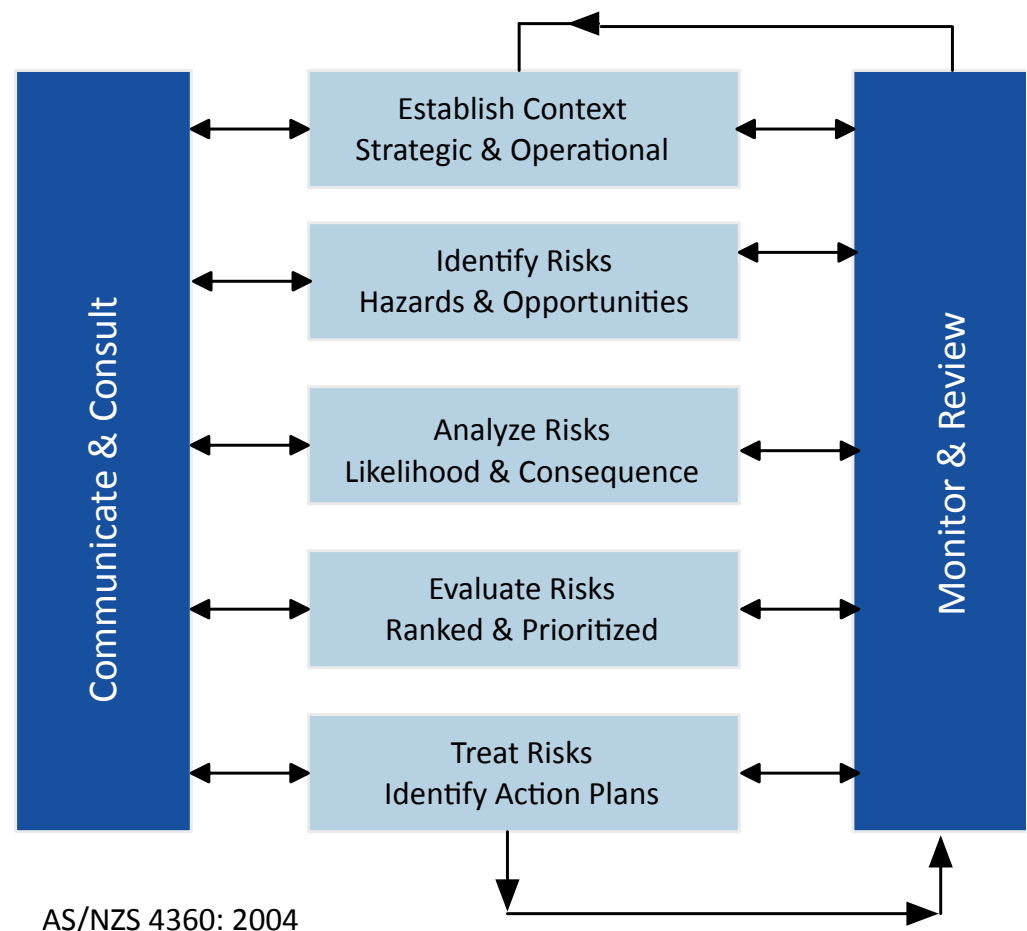
Subject Entities deploy strategies and objectives to meet stakeholder demands, to respond to environmental conditions and to capitalize on market opportunities. The multiple objectives and strategies together with the changing environment generate

risks and a continually evolving risk profile. Subject Entities should identify the processes which mitigate the key business risks identified. The Subject Entity Level Risk Assessment should be updated once a year and/or when the Subject Entity goes through major restructuring, engages in one or multiple major projects, and in the context of other similar activities.

5.3 The Risk Management Process Overview

This section provides a brief view of the risk management process. Risk management is a fundamental aspect of successful management where it is an ongoing process integrated in the practices and processes of the Subject Entity.

The risk management process includes the steps outlined in the following diagram. The risk methodology applied to maintain a register of risks is consistent with the risk management standard AS/NZS 4360:2004.



Step 1 Establish Context (SWOT analysis, strategic risk assessment, business planning)

Establishing the context requires analyzing the external and organizational environment and risk management environment, by which risks can be identified, analyzed and minimized. This analysis may cover the Subject Entity as a whole or the individual processes. The context should be agreed upon before initiating the risk management process, so as to assist in the development of the assessment standards and the risk analysis framework.

Step 2 Identify Risks

Identify what, why and how events can arise, within the Subject Entity, and which can prevent, minimize, or delay achieving objectives.

Step 3 Analyze Risks

Once risks have been identified, they will be analyzed in terms of consequence and likelihood, in the context of the existing controls. The analysis considers the range of potential consequences and how those consequences might occur (i.e. scenarios). Consequence and likelihood is combined to produce an estimate of the level of potential risk to the Subject Entity.

Step 4 Evaluate Risks

Compare estimated levels of risk against risk criteria to provide basis for management to identify risk management priorities. If the levels of risk are assessed as low, then risks may fall into acceptable tolerance levels and no further treatment may be required.

Step 5 Treat Risks

Accept and monitor low priority risks. For other risks identified, develop and implement specific management plans including the resource allocated to mitigate the risks to an acceptable level. There are several forms of risk treatment such as avoidance, transfer, or reduction to an acceptable level after taking into consideration the cost versus benefit of the risk treatment.

Step 6 Monitor & Review Risks

Monitor and review the performance of the risk management system and changes to business initiatives and other internal processes, which may affect it. This step is carried out throughout the risk management process.

Step 7 Communicate & Consult

Provide regular reports to Senior Management and the Audit Committee at each phase of the risk management process and also on the effectiveness of the processes as a whole.

The key elements of the Risk Management process are detailed in the following sections.

5.4 Establish the overall Risk Management Context

5.4.1 Establish the External Context

This step defines the external environment in which the Subject Entity operates. It also defines the relationship between the Subject Entity and its external environment. This may for example include:

- The business, social, regulatory, cultural, competitive, financial and political environment
- The Subject Entity's strengths, weaknesses, opportunities and threats
- External stakeholders
- Key business drivers

It is particularly important to take into account the perceptions and values of external stakeholders and to establish policies for communication with these parties.

Establishing the external context is important to ensure that stakeholders and their objectives are considered when developing risk assessment criteria and that externally generated threats and opportunities are taken into account.

5.4.2 Establish the Internal Context

Before a risk management activity at any level is commenced, it is necessary to understand the Subject Entity. Key areas include:

- Culture
- Internal stakeholders
- Structure
- Capabilities in terms of resources such as people, systems, processes, capital
- Goals and objectives and the strategies that are in place to achieve them

Establishing the internal context is important because:

- Risk management takes place in the context of the goals and objectives of the Subject Entity
- The major risk for most organizations is the failure to achieve strategic, business or project objectives, or to be perceived by stakeholders to have failed
- Organizational policy, goals and interests help refine the Subject Entity's risk policy
- Specific objectives and criteria of a project or activity must be considered in light of the objectives of the Subject Entity

5.5 Identify Inherent Risk

5.5.1 Defining Risk

Risk may be identified in the following terms:

Examples include:



- A fraud instance damages the Subject Entity's reputation with stakeholders and the community
- The absence of policies and procedures increases the likelihood of inconsistent transactions and process flows
- Ineffective segregation of duties within accounts payable increases the likelihood of error and fraud

A risk is associated with:

- a **source** of risk – the thing which has the potential to harm or assist (e.g. a chemical spill, a fraud)
- an **event** or **incident** – something that occurs or not
- a **consequence**, **outcome** or **impact** across a range of stakeholders, assets or resources
- a **cause** (what and why) for the presence of the hazard or the event
- **controls** and their levels of effectiveness (i.e. policies, training, systems)
- **when** the risk could occur and **where** it could occur

5.5.2 Information For Identifying Risk

Good quality information is important in identifying risks. The starting point for risk identification may be historical information about the Subject Entity (or the Government of Abu Dhabi in general), followed by discussions with a wide range of stakeholders about historical, current and evolving issues. Examples include:

- local or overseas experience
- expert judgement
- structured interviews
- focus group discussions
- strategic business plans including SWOT analysis
- insurance claims reports

- post event reports
- personal experience or past organizational experience
- results and reports from audits and inspections
- surveys and questionnaires
- checklists
- historical records, incident databases and analysis of previous failures and previous risks registers if they exist.

5.5.3 Approaches To Identifying Risks

The approach used for risk identification depends on the risk management context. In selecting an approach to risk identification, the following considerations apply:

- Team-based brainstorming, for example, where facilitated workshops are a preferred approach as they build commitment, consider different perspectives and incorporate differing experiences;
- Structured techniques such as flow charting, system design review, systems analysis, hazard and operability (HAZOP) studies and operational modelling should be used where the potential consequences are catastrophic and the use of such intensive techniques are cost effective;
- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure such as 'what-if' and scenario analysis could be used;
- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements may be considered at a higher level, or a checklist may be used.

In many circumstances, multi-level risk identification is useful and efficient. In a first or preliminary scoping stage, risks may be identified at a high level and initial priorities assigned, with a detailed level identification and analysis applied to a subset of high priority areas.

The identified risks should be documented in a Risk Register (Section 6.3)



5.6 Analyze Risk

5.6.1 Introduction

Risk analysis revolves around developing an understanding of the risk. It provides input into decisions on whether risks need to be treated and subsequently the most appropriate and cost-effective treatment strategies.

Risk analysis involves the consideration of the sources of risk, their positive and negative consequences and the likelihood that those consequences may occur. Factors that affect consequences and likelihood may be identified. Risk is analyzed by combining consequences/impacts and their likelihood.

A preliminary analysis should be carried out so that similar risks are combined or low-impact risks are excluded from the assessment. Excluded risks should, where possible, be listed to demonstrate the completeness of the risk analysis.

5.6.2 Consequence/Impact Ratings

The performance of the Subject Entity must be measured in a comprehensive manner, in a way where operational activities are correlated and linked to the objectives derived from its strategy. Balanced Scorecards (BSC) can be used to measure the performance of the Subject Entity in various aspects, where Consequences / Impacts can be described in a number of ways. Risks can have Consequences / Impacts in terms of, amongst others, Financial Performance & Results, Business Continuity, Regulatory / Legal, Reputation and Image, and Human Resources. Each consequence can be rated, in terms of its severity, from 1 to 5, whereas 1 is notable, 2 is minor, 3 is moderate, 4 is major and 5 is catastrophic. Balanced Scorecards can be used by the Subject Entity to manage the negative outcome of possible events that could be faced.

A sample Consequence/Impact Criteria table based on the BSC approach is presented right:

Perspective	Definition		Objective / Driver	KPI	Target	Rating
Financial*	Government Department	Acquisition of financial resources	Delay in submitting complete budget	Delay in submitting complete budget	Less than 1 month	For example: Moderate: delay is between 1 to 2 months
			Budgets are approved and funds are received within the first quarter	Date funds are received	Before the end of the first quarter	For example: Moderate: funds received by mid 2nd Quarter
				Expenditure adherence to plan throughout the year	Variance with the plan is less than X%	For example: Moderate: Variance with the plan is less than 10%
	Other Subject Entities	Achievement of financial objectives	Dependence on Government subsidies	Increase in dependence on Government subsidies	Less than 0% increase	For example: Moderate: 10% increase in dependence on Government subsidies
			Maintain shareholder value	Reduction in return on shareholder equity	0% reduction	For example: Moderate: 5% reduction in return on shareholder equity
Customers / Stakeholders	Cooperation and coordination with stakeholders		Meet stakeholder expectations	Comprehensive SLAs exist	SLAs have been completed and communicated to stakeholders	For example: Moderate: SLA template developed but not completed
	Customer satisfaction		Maintain and improve customer satisfaction	% Customer Satisfaction	80% minimum satisfaction	For example: Moderate: 70% customer satisfaction
Internal Operations	Defined processes are in use		Ensure compliance with approved procedures	A Process Manual has been approved and is in use	Yes	For example: Moderate: processes exist within the entity but have not been grouped into one approved manual
	Proper BCM		A BCM exists and has been tested	A Business Continuity plan has been implemented and is regularly updated	Yes	For example: Moderate: individual business continuity initiatives exist at the functional level.
Learning and Growth	Work force stability		Turnover rates are maintained within industry levels	Turnover rate is less than X% where X is the industry average	X%	For example: Moderate: turnover rate is between X% and (X+0.1X)%
	Defined employee performance expectations		To provide a link between the Subject Entity's strategy and personal objectives of employees	Personal Development Plans are completed and communicated	100%	For example: Moderate: the PDPs are under development

*The Financial perspective in the table above was developed with examples for both departments and State Owned Entities

There are other approaches to measure the Consequences / Impacts which can be described in a number of ways where each consequence can be rated, in terms of its severity, from low to catastrophic. A sample Consequence / Impact Criteria table is set out below.

Rating		Financial	Business Continuity	Regulatory / Legal	Reputation & Image	Human Resources
Catastrophic	5	Financial impact in excess of AED XX	Loss of service capacity for more than X days	Significant legal, regulatory or internal policy failure (e.g. resulting in substantial criminal penalties)	Extended national adverse media coverage, and/or significant loss of confidence by stakeholders/ 3rd parties	Unplanned loss of a senior executive, or several key staff. Loss of life or permanent incapacitation
Major	4	Financial impact between AED xx and AED xx	Loss of service capacity between x and xx days	Major legal, regulatory or internal policy failure (e.g. resulting in a visit by regulators in relation to non-compliance)	Adverse national media coverage, and/or some loss of confidence by stakeholders/ 3rd parties	Unexpected loss of a key staff member with specialist knowledge without which the business is significantly affected Serious injury or incident
Moderate	3	Financial impact between AED xxx and AED xxx	Loss of service capacity between xx and xxx days	Limited legal, regulatory and internal policy failure (e.g. resulting in reportable incident(s) to regulators)	Extended local adverse media coverage and/or adverse stakeholders/ 3rd parties	Unexpected loss of a key staff member who is integral to the business with specialist knowledge. Injury or incident requiring medical attention
Minor	2	Financial impact between AED XX and AED XX	Loss of service capacity between X day and X day	Minor legal, regulatory (able to be resolved without material penalty) or internal policy failure Isolated incident	Isolated adverse local media coverage and/or adverse client or stakeholder comments or complaints	Unexpected loss of a senior staff member Minor injury or incident
Notable	1	Financial impact up to AED XX	Loss of service capacity for up to X day	Insignificant legal, regulatory or internal policy failure	Minor injury or incident. No impact or minimal impact	Unexpected loss of a single staff member Near miss incident

Note: The criteria and weights listed in the table above are not based on any assessment of the Subject Entities' risk appetite or risk tolerance levels. Before performing the risk assessment exercise, the criteria and any associated weights must be tailored to reflect the risk tolerance levels of the concerned Subject Entity. It is recommended to amend and/or add different areas of impact which may be more relevant and applicable to the Subject Entity. These areas and weights should be reviewed and approved by the Audit Committee and the Board of Directors.

5.6.3 Likelihood Rating

Analyzing risks requires an assessment of their frequency of occurrence. The following table provides broad descriptions used to support likelihood ratings.

Rating		Likelihood Of Occurrence
Almost Certain	5	The event will occur in most circumstances
Likely	4	The event will probably occur in most circumstances
Possible	3	The event should occur in some circumstances
Unlikely	2	The event could occur in some circumstances
Rare	1	The event may occur in some exceptional circumstances

Guidance:

To make an assessment of the likelihood or probability of a risk event occurring, it may be useful to consider the factors listed below. They have been expressed in the form of questions about the risk environment in order to facilitate the assessment.

Complexity – How complex is the process in terms of multiple tasks or technology? – consider the complexity of the underlying processes or environment in which the Subject Entity and / or the assessed process, function, or project operates.

Susceptibility – How susceptible or vulnerable is the Subject Entity and/or the assessed process, function, or project to the risk? – consider how new people or processes impact, the number of stakeholders involved, high level of change etc.

History – To what extent is the risk known to have occurred previously? – consider the history of error within the Subject Entity and/or across the assessed process, function, or project.



5.7 Qualitative Analysis

Qualitative Analysis is any method of analysis that uses descriptions rather than numerical means to define a level of risk. Using qualitative analysis, risk is a function of both likelihood and a measure of consequence. In its simplest form, risk can be shown as:

Risk = A function of (Consequence and Likelihood)

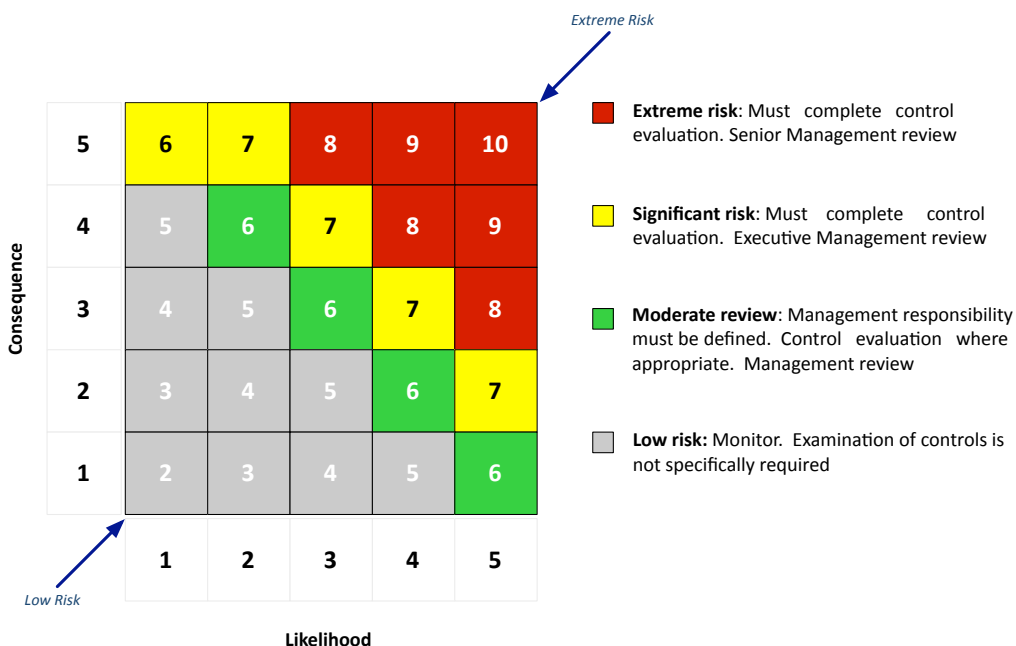
For example, using the risk matrix below, if a Consequence / Impact was assessed as Major (4) and the likelihood of that Consequence / Impact occurring was Likely (4), the risk would be rated as extreme based on its position on the matrix. Each risk identified is assessed in the same manner to produce a Risk Register. It is important to note that the risks are initially assessed without any consideration for controls.

The Subject Entity's Consequence / Impact criteria table should be documented in the "Understanding the Business Memorandum".

5.8 Inherent Risk Assessment

Inherent risk is the risk that exists in the absence of controls. Inherent risk is important to the Internal Audit process because it represents the potential impact of a breakdown in the control environment within the Subject Entity.

The combined ratings for likelihood and consequence for each risk are combined in the matrix below to determine the overall risk ranking. The legend to the right of the matrix defines each level of risk.



The Subject Entity's Inherent Risk Assessment should be documented in the Risk Register (Section 6.4).

All inherent risks ranked as "Extreme", "Significant" and "Moderate" require detailed analysis of controls to determine the residual risk rating.

Low risks may be excluded from further analysis; however the rationale for excluding these risks (and management's on-going responsibilities) should be documented to demonstrate the completeness of the analysis undertaken.

The controls existing to mitigate the risk are then considered for existence and effectiveness using the criteria shown in the controls rating table.

By rating each control as set out below, the control rating is combined with the inherent risk rating to arrive at a residual risk rating.

5.9 Identification & Assessment Of Mitigating Practices And Controls

Mitigating practices and controls include all the policies, procedures, practices and processes in place to provide reasonable assurance of the management of the Subject Entity's risks.

Where mitigating practices/controls exist but are not being followed and monitored, then adequate control does not exist, as in order for mitigating practices/controls to be effective they also must be communicated, actioned and monitored. Therefore a rating of 5 or above should be applied.

Control rating*			
Adequate	Excellent	1 or 2	Systems and processes exist to manage the risks and management accountability is assigned. The systems are well documented and regular monitoring/management review indicates high compliance to the process and that the system is effective in mitigating the risk.
	Good	3 or 4	Systems and processes exist which manage the risk. Minor improvement opportunities have been identified but not yet actioned.
Inadequate	Fair	5 or 6	Some systems and processes exist to manage the risk. Recent changes in operations require confirmation that accountabilities are in place and understood and that the risk is being actively managed.
	Poor	7 or 8	Systems and processes for managing the risk have been subject to major change or are in the process of being implemented and their effectiveness cannot be confirmed.
	Unsatisfactory	9 or 10	No systems and processes exist to manage the risk.

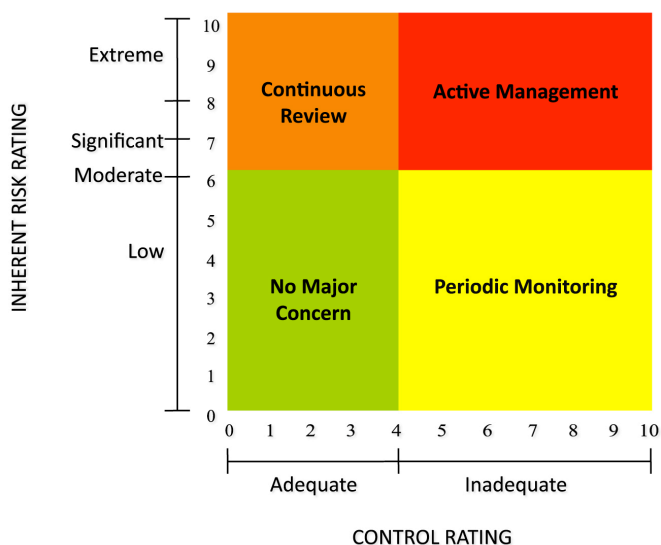
* Range of rating allows for strength of the statement to be varied.

The mitigating practices/controls relating to each risk should be documented in the risk register (Section 6.6.3) and rated according to their effectiveness in mitigating the risk from a design perspective, as the operating effectiveness of the controls will be tested during the Execution Phase.

5.10 Residual Risk

Residual risk is the level of risk that remains within the Subject Entity after consideration of all existing controls. The residual risk table below provides the Subject Entity with the required level of management attention along with the time frame when treatment plans should be developed.

The Residual Risk Rating is calculated by adding the Inherent Risk measures of Consequence/Impact and Likelihood (5.8) and combining the control rating (5.9). The management response required in relation to the Residual Risk is determined by the position of the latter on the matrix.



Active Management	Risks where current treatment options require active review and management.
Continuous Review	Control is adequate, continued monitoring of controls over time (e.g. at least quarterly) is required to confirm this.
Periodic Monitoring	Control is not strong but risk impact is not high. Options to improve control or monitor risk impact to ensure it does not increase over time.
No Major Concern	Risks where systems and processes managing the risks are adequate and subject to minimal monitoring

The grid (left) clearly demonstrates the relevance of inherent and residual risk to the Internal Audit Process.

Any breakdown in the mitigating practices/controls relating to risks in the “Continuous Review” area could have an immediate, significant impact on the Subject Entity. Risks in the “Periodic Review” area of the matrix have been assessed as having controls with a fair rating or worse; thus an increase in the level of risk could have an immediate, significant impact on the Subject Entity.

Risks in the “Active Management” area of the matrix will be brought to the attention of management (for management) and monitored closely by the Internal Audit Function during the “Active Management” period.

The Subject Entity’s Residual Risk Assessment should be documented in the Risk Register (Section 6.7).

In order to create the Residual Risk heat map in the e-Governance Portal, please follow these steps:

1. Go to Navigation -> Search -> Risk Matrices
2. Click on “Saved Searches” for the search called “Core Search”
3. Click the play icon next to “Residual Risk Ratings Report”
4. Save the Excel file to your hard disk
5. Open the file

5.11 Risk Management Assurance & Monitoring

Systems to monitor and review risks and the risk management process require careful selection, targeting and planning as they absorb scarce resources. Priority should be given to monitoring:

- (a) High risks
- (b) Credible failure of treatment strategies, especially where this would result in high or frequent consequences
- (c) Risk-related activities that feature high incidence of change
- (d) Risk tolerance criteria especially where these result in high levels of residual risk
- (e) Technological advances that may offer more effective or lower cost alternatives to current risk treatment



In general terms, monitoring and review practices will be one of three types:

- Continuous (or at least frequent) monitoring through routinely measuring or checking particular parameters
- Line management reviews of risks and their treatments (sometimes called “control self assessments”) which are often selective in scope but typically routine, regular and selected based on risk-weighted criteria
- Auditing using both internal and external audit staff. As much as possible, these audits should test systems rather than conditions. They will be more selective in scope and of a lower frequency than the above measures

6

Risk Assessment & Annual Audit Plan

6.1 Develop Detailed Understanding Of The Key Processes

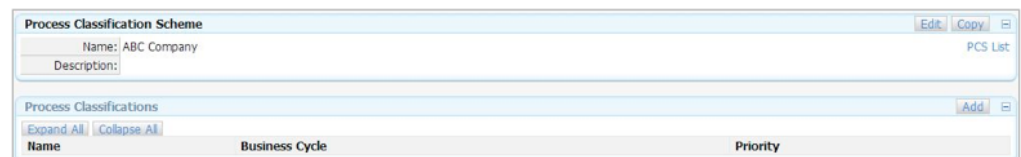
This section provides more detailed guidance on how the key risks identified at the department/function/process Level Risk Assessment (Section 5) should be documented. The objectives of the documentation are to:

- Gain detailed understanding of the mega and major processes, and when necessary, the associated sub-processes
- Analyze the process for effectiveness
- Gain an understanding of the significant flow of transactions
- Promote a comprehensive understanding of the process from beginning to end
- Identify the risks and associated controls (or lack thereof)
- Identify problem areas and improvement opportunities

For further details about using the e-Governance Portal, please refer to the Manual uploaded to your Server. (Please take into account the changes made to this Manual).

In order to create the Process Classification Scheme in the e-Governance Portal, please follow these steps:

1. Click on the link "1. Process Classification" on the homepage dashboard
2. Click [Add](#) to create a new placeholder for Processes
3. Enter a Name (e.g. ABC Company) and Description for your PCS and click [Save](#)
4. Click [Add](#) to create a process in the PCS



Process Classification Scheme		
Name: ABC Company		
Description:		
Process Classifications		
Expand All Collapse All		
Name	Business Cycle	Priority

5. Enter the name of the Process (if necessary, select the Parent Process)

Did you Know?

PCS (Process Classification Scheme): Create only 1 PCS which includes all the processes within your organization. These processes can be grouped by Function/Process/Department. For example: create the process "Finance". Then create "Accounts Payable" and "Accounts Receivable" as child processes for the process "Finance"

6. Click **Save**

In order to create the Organization Model in the e-Governance Portal, please follow these steps:

1. Click on the link "2. Organization and Process Structure" from the homepage dashboard
2. Click **Add** to create a new Organization
3. Enter the required fields on the Organization form
4. Click **Save**

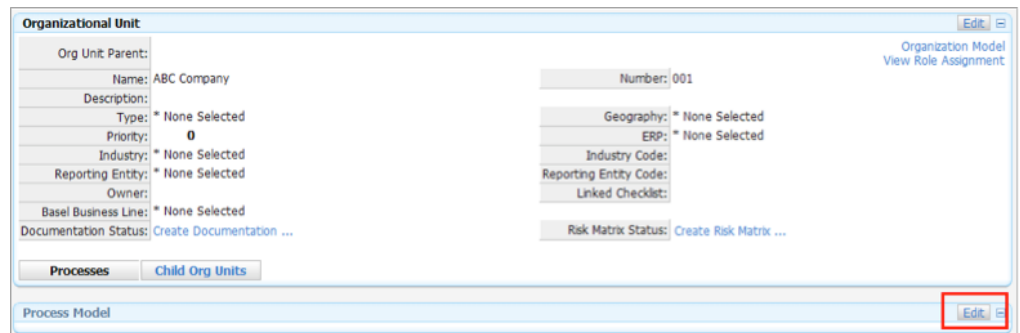
5. To create subsidiaries/branches, click on the tab Child Org Units
6. Repeat the steps from 2 to 4 to complete the creation process.

Did you Know?

Organization Model: Create a simple organization model structure that consists of only physical locations (branches/subsidiaries) of your organization. If you only have 1 location, just create 1 organization with the name of your entity. Then link the PCS (Process model), which consists of the Functions/Processes/Departments, to these organization(s). This prevents duplication between the Organization and Process model.

In order to link the PCS with the Organization Model in the e-Governance Portal, please follow these steps:

1. Click on the link "Organization and Process Structure" from the homepage dashboard
2. Click on the name of the organization to which you want to link processes
3. Click [Edit](#)



4. Select the PCS that you want to link from the dropdown menu



5. Click
6. Click (as in step 3)
7. Select the processes that you want to link to the organization
8. Click

Did you Know?

Reporting Entity: Create Reporting Entities via the homepage dashboard and tag your organizations in the organization model to these reporting entities. This can be done by clicking on the name of the organization, editing the page, and selecting the field reporting entity. This will allow you to group your subsidiaries and subsequently enable consolidated reporting.

6.2 Risk Categories

Risks are categorized at 3 levels.



Level 1: Risks at level 1 are categorized as Strategic, Operational, Financial and Compliance risks.

- Strategic Risks include risks from:
 - Subject Entity objectives and Business Strategy
 - Stakeholders
 - Governance
 - Market Structure
- Operational Risks include risks from:
 - People
 - Physical Assets
 - Information Technology
 - Process
 - Knowledge
- Financial Risks include risks from:
 - liquidity (e.g. cash flow)
 - Accounting & Reporting
 - Capital Structure

- Compliance Risks include risks from:
 - Legal and Regulatory
 - Industry Standards
 - Code of Conduct
 - Business Interruption

Once the risks at level 2 (mega processes) or level 3 (major processes) are documented in the Risk Register, the related category of Level 1 risks is documented for each.

Level 2: Risks at level 2 are categorised at the mega process level, i.e. Procurement, Human Resources etc.

Level 3: Risks at level 3 are categorised at the major-process level, i.e. Select and manage suppliers, Purchase materials and supplies (within Procurement) etc.

6.3 Inherent Risk Description

Section 5.5 provides detailed guidance on how to identify risks. A description of the inherent risk should be documented in the Risk Register. The description should be clear and concise.

The existence of each risk should be confirmed with management through a direct discussion or an arranged review. Management may disagree that a risk exists because controls are in place to prevent the risk from arising. At the current stage, the basis of the risk assessment process is to first identify the risks without consideration of controls (i.e. inherent risks).

In order to add Risks in the Subject Entity Portal, please follow these steps:

1. On the homepage dashboard, click on “Organization and Process Structure”
2. Click on the name of the Organization for whom you want to perform a Risk Assessment
3. Click on the link in the Risk Matrix Status column

Organizational Unit Edit

Org Unit Parent:
 Name: ABC Number: 001
 Description:
 Type: * None Selected
 Priority: 0
 Industry: * None Selected
 Reporting Entity: * None Selected
 Owner:
 Basel Business Line: * None Selected
 Documentation Status: Create Documentation ...
 Geography: * None Selected
 ERP: * None Selected
 Industry Code:
 Reporting Entity Code:
 Linked Checklist:
 Risk Matrix Status: Create Risk Matrix ...

[Processes](#) [Child Org Units](#)

Process Model Edit

PCS: Generic Delete All Processes
[Expand All](#) [Collapse All](#)

Process	Documentation Status	Risk Matrix Status	Checklist Summary	Priority
1 Procurement	N/A	N/A	N/A	0
1.1 Select and manage suppliers	N/A	N/A	N/A	0
1.2 Purchase materials and supplies	N/A	N/A	N/A	0
1.3 Registration	N/A	N/A	N/A	0
8 Human Resources	N/A	N/A	N/A	0
10 Financial and Physical Resources	N/A	N/A	N/A	0

- Click [Save](#) to create the risk register
- Click [+](#) in the Risks section to create a risk

Risk Register Edit Return

Entity Name: Organizational Unit: ABC Company / Process: Human Resources Template Library
 Documentation Status: Create Documentation...
 Risk Register Status:

[Analysis](#) [Review](#) [Action Plans](#) [Tasks](#) [Notes](#) [Indicators](#) [History](#)

Walkthrough Evaluation Edit

Risks Edit All Add Execute Edit Search

Risk Name	Risk Description	Risk Category	Risk - Inherent Risk Impact	Risk - Inherent Risk Likelihood	Risk - Inherent Risk Rating	Risk Rating Rationalization
+						

Controls Edit All Add Execute Edit Search

Control Name	Control Description	Control Type	Control Automation	Control Frequency
+				

Tests Execute Edit Search

- Enter a Risk name
- Click Save

6.4 Inherent Risk Rating

Risk is assessed by determining the potential consequence/ impact for the risk and the likelihood of the risk arising. To remove a degree of subjectivity and to drive consistency, the assessment is performed against the criteria highlighted in Section 5.6 above.

Inherent risks are then rated on the consequence/ impact and likelihood as highlighted in Section 5.7 above. Ratings will be either: Low Risk, Moderate Risk, Significant Risk or Extreme Risk as highlighted in Section 5.8 above. It is important to note that this assessment is made before the consideration of the extent that these risks are mitigated by controls.

In order to rate and categorize the risks in the e-Governance Portal, please follow these steps:

1. Create a risk as described above and select the values for the Risk Category, Inherent Risk Impact and the Inherent Risk Likelihood from the drop-down menu.

The screenshot shows the 'Risk Register' interface. At the top, there's a header with 'Entity Name: Organizational Unit: ABC Company / Process: Human Resources' and 'Documentation Status: Create Documentation...'. Below this is a tabbed interface with 'Analysis', 'Review', 'Action Plans', 'Tasks', 'Notes', 'Indicators', and 'History'. The 'Analysis' tab is active, showing a 'Walkthrough Evaluation' section. Below this is a table of risks. The first risk is 'Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.' The 'Risk Category' dropdown menu is open, showing a list of categories including '0001 * None Selected', '0002 * None Selected', '0002.SR - STRATEGIC RISKS', '0002.0001 SR - Department objectives and', '0002.0002 SR - Stakeholders', '0002.0003 SR - Governance', '0002.0004 SR - Market Structure', '0003 OR - OPERATIONAL RISKS', '0003.0001 OR - People', '0003.0002 OR - Physical Assets', '0003.0003 OR - Information Technology', '0003.0004 OR - Process', '0003.0005 OR - Knowledge', '0004 FR - FINANCIAL RISKS', '0004.0001 FR - Liquidity', '0004.0002 FR - Accounting and Reporting', '0004.0003 FR - Capital Structure', '0005 CR - COMPLIANCE RISKS', '0005.0001 CR - Legal and Regulatory', '0005.0002 CR - Industry standards', '0005.0003 CR - Code of Conduct', and '0005.0004 CR - Business Interruption'. The 'Risk - Inherent Risk Impact' and 'Risk - Inherent Risk Likelihood' dropdowns are also set to '*None Selected'. The 'Risk - Inherent Risk Rating' dropdown is set to '*None Selected'.

2. Enter the reasoning behind the ratings in the Risk Rating Rationalization field.
(Describe the impact from the Financial, Business Continuity, Regulatory / Legal, Reputation & Image, and Human Resources perspectives)

3. Click Save or [Save](#)

Note: The value for the Inherent Risk Rating will be automatically calculated by the system

4. Create all Risks for the Entity, then move on to adding Controls

Did you know?

Best Practice Library: Import risks and controls from the Library created and populated during the risk assessment phase.

Go to the risk register where you want to import the library contents then:

- Click Template Library
- Click on the library repository, followed by the Risk Matrix name
- Select the Risks and Controls that you want to import
- Click "Import" at the top of the screen to import the content

6.5 Perform Evaluation of Controls Over Risks

Management typically establishes and maintains a system of internal controls to help identify, monitor, and mitigate risks, and to support the achievement of the Subject Entity's objectives.

We evaluate how effective the **design** of a particular control is in mitigating the identified risk within a process. In order to perform this, the Internal Audit Function needs to identify and evaluate the controls in place and assess their **design** effectiveness in preventing or mitigating risks.

As stated above, where Inherent Risks are rated as "Low Risk", it is acceptable to focus scarce resources on higher inherent risk ratings; still, where resource availability is not a problem, the identification and evaluation of one control is sufficient.

When identifying controls, the Internal Audit team should link them directly to the risk in question. More often than not, there will be more than one control in place to mitigate a risk. The task of the Internal Audit team is to evaluate the combination of controls to determine if they are effective or, alternatively, if there may be inefficiencies created by redundant controls over less important process activities (e.g., non-value added activities). It should be noted that not all controls will be significant controls that directly mitigate a risk.

A diligent approach to link the controls to the risk is by preparing a flowchart documenting the process and the controls that are part of the process. The section below provides further details on the documentation and different types of control.

6.6 Documentation of Controls

6.6.1 Documenting Controls

Interviews or workshops are held with process owners and staff to document and confirm the understanding of the process(es). The understanding is documented in the form of structured notes or process diagrams (flow charts).

When documenting controls, the following should be clearly stated:

- Policy / procedure reference where the control is described (if applicable)
- Who performs the control, who reviews and confirms that the control is performing effectively (usually a designation is stated and not the name of the individual performing the control (documented in the "Control Description" field))
- Who is the control owner i.e. responsible for ensuring that the control is effective (again state designation)
- What is the frequency of the control i.e. transaction based, daily, weekly, monthly, quarterly, annually etc.
- Is the control a prevent or detect control
- Is the control a manual or IT control



6.6.2 Preventive & Detective Controls

Both preventive and detective controls are important. A preventive control is a control designed to prevent an error from occurring. Preventive controls are usually applied to each transaction during the normal flow of the process and are designed to prevent a risk from arising (e.g. "fire retardant carpeting").

Detective controls are devices, techniques, and procedures designed to identify and expose undesirable events that elude preventive controls. Detective controls reveal specific types of errors by comparing actual occurrences to pre-established standards. When a detective control identifies a departure from a standard, it sounds an alarm to attract attention to the problem. In reality, a Subject Entity will implement a combination of preventive and detective controls to mitigate risk. This is good practice, as an excessive number of preventive controls can make a process overly bureaucratic and unwieldy.

There is no optimal mix of preventive and detective controls within a process to mitigate risks. Certain risks will lend themselves more to one form of control than another. For example:

- In a retail environment, the risk of inappropriate cash refunds is prevented by the requirement for management to approve all refunds prior to the actual release of funds. A detective control would be too late whereas the customer would have left with the cash
- In a bank, it would not be practical to implement controls to prevent the risk of theft of cash by a bank teller during normal bank telling operations. This risk is more appropriately controlled by a detective control (i.e. reconciliation). Knowledge of the performance of such reconciliation may also deter tellers from theft, therefore helping to mitigate the risk


6.6.3 Manual & IT Controls

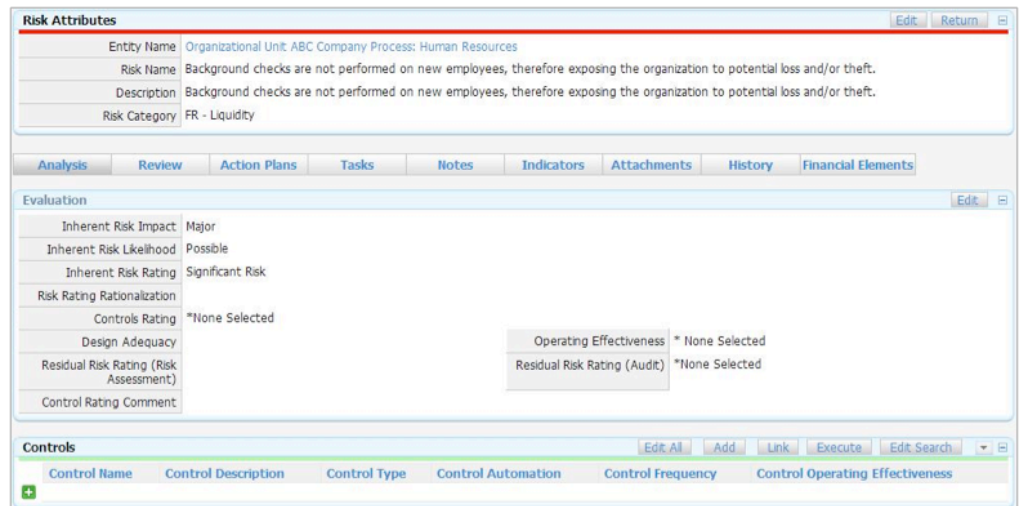
Manual controls operate outside the IT platform, such as manual approval of transactions. IT controls on the other hand are controls that are hard-coded into IT systems and will operate as designed until the program is changed.

Simply because a control is IT supported does not necessarily mean it is effective. If however it is deemed effective, we can feel greater comfort that it will continue to operate effectively.

This assumption is however subject to the adequacy of program change controls and security within the IT production environment.

In order to create controls for a certain risk in the e-Governance Portal, please follow these steps:

1. Click on the Risk Name to document the Controls for that Risk
2. Click Add  in the Controls section to create a control



Risk Attributes	
Entity Name	Organizational Unit: ABC Company Process: Human Resources
Risk Name	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.
Description	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.
Risk Category	FR - Liquidity

Evaluation	
Inherent Risk Impact	Major
Inherent Risk Likelihood	Possible
Inherent Risk Rating	Significant Risk
Risk Rating Rationalization	
Controls Rating	*None Selected
Design Adequacy	
Residual Risk Rating (Risk Assessment)	
Control Rating Comment	

Controls	
Control Name	Control Description
Control Type	Control Automation
Control Frequency	Control Operating Effectiveness

3. Enter the Control Name and Description and select the Control Type, Control Automation, and Control Frequency

Risk Attributes Edit Return

Entity Name	Organizational Unit: ABC Company Process: Human Resources
Risk Name	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.
Description	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.
Risk Category	FR - Liquidity

Analysis **Review** **Action Plans** **Tasks** **Notes** **Indicators** **Attachments** **History** **Financial Elements**

Evaluation Edit

Inherent Risk Impact	Major
Inherent Risk Likelihood	Possible
Inherent Risk Rating	Significant Risk
Risk Rating Rationalization	
Controls Rating	*None Selected
Design Adequacy	
Residual Risk Rating (Risk Assessment)	
Control Rating Comment	

Operating Effectiveness *None Selected
Residual Risk Rating (Audit) *None Selected

Controls Edit All Add Link Execute Edit Search

Control Name	Control Description	Control Type	Control Automation	Control Frequency	Control Operating Effectiveness
<input checked="" type="checkbox"/> A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll...	A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll for entry into the payroll system, receipt of policies and procedures and codes of conduct, background checks, etc.	Preventative	Manual	Daily	*None Selected
<input checked="" type="checkbox"/> Company is implementing a hiring program that will include best practice targeting, selection criteria, and post-hire assessments.	Company is implementing a hiring program that will include best practice targeting, selection criteria, and post-hire assessments.	Detective	System	Weekly	*None Selected

- Click **Save** to link the controls to the risk
- Repeat the steps above until all relevant controls have been created

Did you know?

Dependent Controls: Use dependent controls if a risk is mitigated by a control in another Process (risk register).

To link controls to risks in the e-Governance Portal, please follow these steps:

- Click on the Name of the Risk to which you want to link existing controls
- Click **Link** in the Control section of the Risk form. The pop-up screen shows the Controls that are documented within the entity

Control Linkage List Select All Deselect All Save Cancel Execute Edit Search

Selected	Control Name	Control Description	Control Type
<input type="checkbox"/>	By mid-year , the corporate HR department will begin to perform an internal audit of the various international HR departments on a periodic basis.	By mid-year , the corporate HR department will begin to perform an internal audit of the various international HR departments on a periodic basis. This will include the adherence to P&P, SOPs, safety guidelines, confidentiality and retention guidelines, and more.	*None Selected
<input type="checkbox"/>	Unless there is gross misconduct, terminations first require a verbal warning, then a written warning, a final written warning, followed	Unless there is gross misconduct, terminations first require a verbal warning, then a written warning, a final written warning, followed by a review by legal before formally terminating an employee. All written warnings are kept in the employee's file for record-keeping purposes.	*None Selected
<input type="checkbox"/>	A Compensation Board exists and meets at least once every quarter.	A Compensation Board exists and meets at least once every quarter.	*None Selected

- Select the check box next to the control that mitigates the given risk
- Click **Save** to link the controls to the risk.

At this stage, it may be possible to identify ineffective, duplicate or redundant controls which do not enhance the control environment. Any such controls should be brought to the attention of the Head of Internal Audit by the team conducting the assessment and to the attention of management in the Risk Assessment report.

Did you know?

Custom Library: Create your own library to prevent duplicating efforts of identifying risks and controls. A library can be created by following these steps:

- Go to Navigation (left side pane)
- Click on Library
- Click on "Risk Matrix Templates"
- Click "Add" for a new Library/Repository

6.7 Perform Walkthrough

The objective of the walk-through is to determine whether policies, procedures and other controls are complied with and are functioning as **designed**. The appropriateness of the control at mitigating the identified risk will be evaluated by:

- Confirming the understanding of the design of the controls and whether they have been put into operation or activated
- Assessing, based on a very limited sample, if the key controls are operating as designed.

Walk-through tests are achieved by:

- Observing the process in operation and / or
- Tracing one or two transactions through the process from beginning to end

If the walkthrough confirms that the understanding of the controls was correct, then the Internal Auditor should rate them as **adequate**. If as a result of the walkthrough however, it is noted that the controls do not perform as designed or are not applied or activated, then the Internal Auditor should rate them as **inadequate**.

In order to perform the walkthrough in the e-Governance Portal, please follow these steps:

Risk Attributes

Entity Name: Organizational Unit: ABC Company Process: Human Resources

Risk Name: Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.

Description: Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.

Risk Category: FR - Liquidity

Analysis | Review | Action Plans | Tasks | Notes | Indicators | Attachments | History | Financial Elements

Save | Cancel

Evaluation

Inherent Risk Impact: Major

Inherent Risk Likelihood: Likely

Inherent Risk Rating: Extreme Risk

Risk Rating Rationalization:

Controls Rating: *None Selected

Residual Risk Rating (Risk Assessment):

Control Rating Comment:

Operating Effectiveness: *None Selected

Residual Risk Rating (Audit): *None Selected

Save | Cancel

Controls

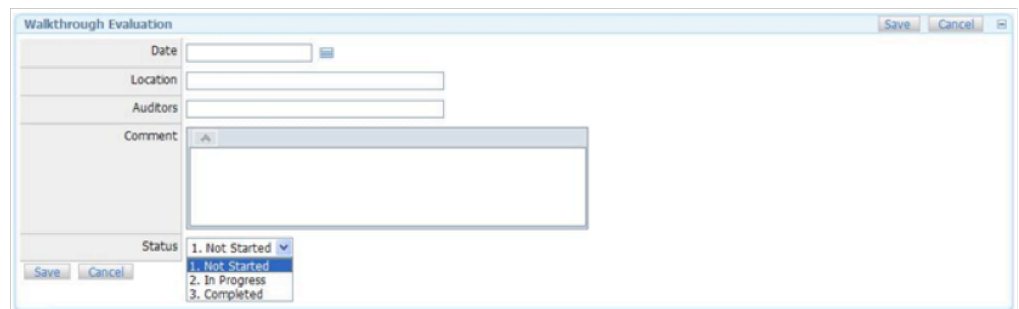
Control Name	Control Description	Control Type	Control Automation	Control Frequency	Control Operating Effectiveness
A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll...	A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll for entry into the payroll system, receipt of policies and procedures and codes of conduct, background checks, etc.	Preventative	Manual	Daily	*None Selected
Company is implementing a hiring program that will include best practice targeting, selection criteria, and post-hire assessments.	Company is implementing a hiring program that will include best practice targeting, selection criteria, and post-hire assessments.	Detective	System	Weekly	*None Selected

1. Go to the Evaluation section on the Risk form and click [Edit](#)
2. Based on the controls that are linked to the risk, rate the **Controls Rating** field on a level from 1 to 10. See section 5.9 for more information about this rating
3. Click [Save](#)

Note: Although the value for the Residual Risk Rating will be automatically calculated by the system based on both the inherent risk and controls ratings, the control rating comment field should be used to clarify the selected controls rating. Where the control(s) applied by the Subject Entity is (are) different from the formally approved policies and procedures, the Internal Auditor should consider if the control(s) applied are more effective than the documented procedures. If yes, these control(s) should be documented in the Risk Register and a note included in the Audit Report to indicate that the procedures should be amended and updated to align with the current applied procedures.

If the actual control(s) applied are less effective than the documented procedures, the approved procedures should be included in the Risk register and the matter raised in the Audit Report in terms of non compliance with the approved policies and procedures. Further testing may thus be required to be performed to assess the extent of the non compliance.

Walkthrough details should be recorded in the Risk Register or on a separate document uploaded to the portal.

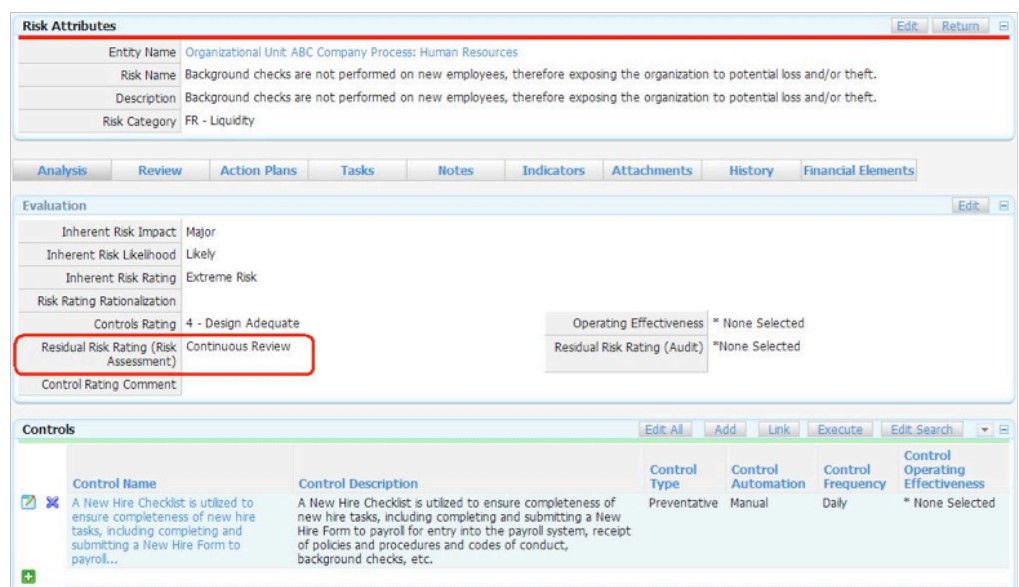


At this stage, the Internal Audit team will be able to draw conclusions about the key risks which are either not managed (as no effective controls have been identified) or are only partially managed. These reportable items can then be taken directly to either the Gap Analysis report or the Internal Audit report and recommendations developed as detailed in Section 9 below.

6.8 Assessing Residual Risk

Once the walkthrough and the controls rating stages have been successfully completed, the residual risk rating is automatically calculated by the system.

Residual risk rating will be on a scale of 1 (No Major Concern) to 4 (Active Management) as highlighted in Section 5.10 above with 1 being the lowest risk and 4 being the maximum risk.



Control Name	Control Description	Control Type	Control Automation	Control Frequency	Control Operating Effectiveness
A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll...	A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll for entry into the payroll system, receipt of policies and procedures and codes of conduct, background checks, etc.	Preventative	Manual	Daily	* None Selected

Did you know?

Saving Searches: Save your own searches to retrieve information in a format specified by yourself. After creating the search, click the dropdown arrow (next to the "Edit Search" button). Then click "Save as new search"

6.9 Gap Analysis

Once residual risks have been assessed, a "Risk Assessment and Gap Analysis Report" may be prepared and issued highlighting to Senior Management high risk areas requiring immediate action. A copy of the standard Gap Analysis Report template is presented in Appendix 5.

Note: The Gap Analysis Report can be run from the e-Governance Portal from the searches dashboard.

6.10 Develop High Level Testing Strategy & Annual Audit Plan

Based on the risk rating and the nature of the area being reviewed, a high level testing strategy should be developed. The objectives of the review should be clearly established.

The purpose of an AAP is to provide details on the testing to be performed, timing to begin and complete the testing, and assignment of audit teams with the requisite skill sets.

The selection of those risks which should be tested and the frequency of tests require considerable skill and judgement. An AAP should cover all key risks and yet should not be excessive or inefficient in terms of the amount of effort required. The Head of Internal Audit should set out criteria for the basis of selection and discuss this with the Audit Committee.

It would be normal practice that all high residual risks be selected for testing on an annual basis, it would also be usual practice that all controls be tested at least once every three years. A time estimate to perform the AAP should be developed detailing the different grades and skill sets and presented to the Audit Committee for their review and approval. A sample AAP is attached in Appendix 6.

Risk Assessment Summary and Audit Coverage									
Residual Risk Rating							Audit Priority and Coverage		
	Unrated	No Major Concern	Periodic Review	Continuous Review	Active Management	Total	Audit Priority	# of Audits	Findings
Organizations and Processes									
Reporting Entity: ABC Company	0	3	4	4	2	13	0	0	0
Business Line: Abu Dhabi Branch	0	3	4	4	2	13	0	0	0
Organization: ABC	0	3	4	4	2	13	0	0	0
Process: Procurement	0	3	2	0	1	6	0	0	0
Human Resources	0	0	2	4	1	7	0	0	0

Did you know?

Favourites: Create favourites for the searches you created to allow quick access to valuable information.

6.10.1 Scheduling Audits

The audit schedule determines the timing, template, and individuals who will be involved in the audit. Additional attributes such as estimated effort (time and budget) and actual effort will be recorded. Scheduling can be done in advance (e.g. 6 months or annual schedule) or just in time.

In order to schedule an audit assignment in the e-Governance Portal, please follow these steps:

1. From the home page, select the [Audit Schedule](#) link
2. Click [Add](#) to create a new Audit

Audit		Edit	Return
Audit Name	Select and manage suppliers	Audit Status: Pending	
Scope and Objectives	The audit covers supplier selection, which is a sub-process of the Procurement process. The controls in the process that are identified as continuous review or periodic review will be tested as part of this audit. The objective of the audit is to ensure the proper selection of bidders.	Summary of Audit Results	
Template Name	General Audit	Archive	
Origin	Risk Assessment	Auditor	
Quarter	2		
Year	2010		
Business Units expectations	We expect no inefficiencies in the process.		
Recent Development and Changes	There have been no recent changes to the process.		
Prior Audit(s) Results Summary	The previous audit on this process was conducted in June 2009. All controls were tested effective and no findings were identified.		
Areas Not Covered Due to Low Risk	All controls related to the risks that are identified as Active Management or No major concern are not included.		
Start Date	1/1/2010		
End Date	1/21/2010		
Plan Hours	0		
Actual Hours	0		
Revised Hours	0		
Budgeted Cost			
Actual Cost			
Explanation of Budget			
Key Business unit Contacts			
Key Audit Skills Needed			



3. Complete as many fields as possible including the Start Date and End Date

The fields that will show in the Audit Report are:

- Audit Name
- Scope and Objectives
- Summary of Audit Results

4. In the Template Name field, select “General Audit” for a Compliance or Performance audit, or select “IT Audit” for an IT Audit

5. After completing the relevant fields, click [Save](#)

6.11 Resource Allocation

Senior Internal Auditors should consider resource planning including human, technology and travel requirements (if applicable) for all audits they lead.

Personnel assigned to an audit should have the skills to perform the work allocated to them. During the audit, opportunities exist for both Senior Internal Auditors and Internal Auditors to identify skill gaps; such instances can then be included in the training plan, and engagement related training can be organized if considered appropriate.

When assigned to an audit requiring travel to other work locations, the Senior Internal Auditor should identify the team’s hardware and software needs; for example, access to the Subject Entity’s servers should be pre-arranged with the IT Functions.

It is incumbent upon the Senior Internal Auditor to advise the Internal Audit Support Officer to undertake the necessary travel arrangements, where applicable.

In determining the resources necessary to perform the audit, it is important to evaluate the following:

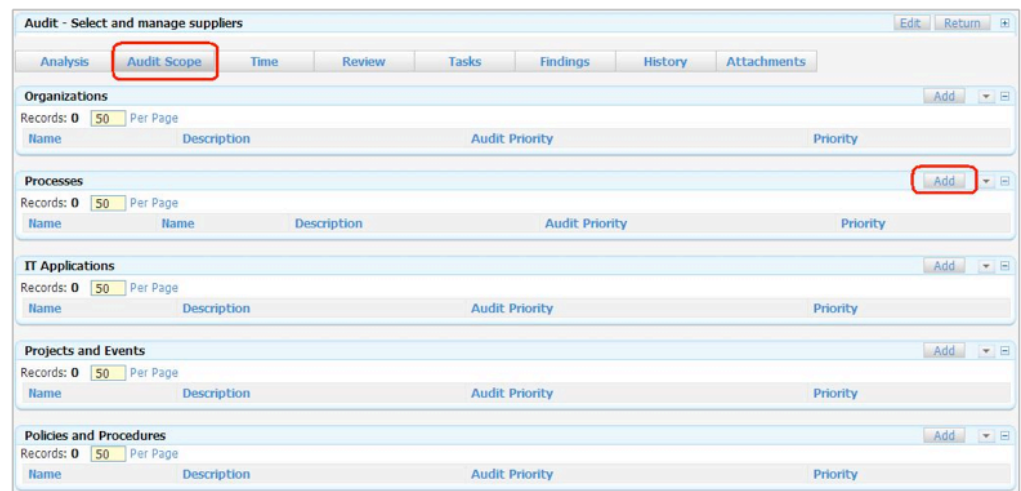
- The number and experience level of Internal Audit staff required should be based on an evaluation of the nature and complexity of the audit assignment, time constraints, and available resources
- The knowledge, skills, and other competencies of Internal Audit staff should be considered in selecting the right team for the review
- The training needs of Internal Audit staff should be considered, since each audit assignment also serves as a basis for meeting developmental needs
- The use of external resources in instances where specific unavailable knowledge, skills, and other competencies are needed.

In order to establish the scope of the audit in the e-Governance Portal, please follow these steps:

1. After step 5 in “Schedule an Audit (6.10.1)”, you will see the screen where you can establish the audit scope. Most likely, you will have risks and controls documented at a process level. In this case, you need to pull a process into scope. If you have

risks and controls documented at the organizational level, you need to pull an organization into scope

- Click **Add** in the Organizations or Processes section



Audit - Select and manage suppliers [Edit] [Return]

Analysis **Audit Scope** Time Review Tasks Findings History Attachments

Organizations [Add] [v] [≡]

Records: 0 50 Per Page

Name	Description	Audit Priority	Priority
------	-------------	----------------	----------

Processes [Add] [v] [≡]

Records: 0 50 Per Page

Name	Description	Audit Priority	Priority
------	-------------	----------------	----------

IT Applications [Add] [v] [≡]

Records: 0 50 Per Page

Name	Description	Audit Priority	Priority
------	-------------	----------------	----------

Projects and Events [Add] [v] [≡]

Records: 0 50 Per Page

Name	Description	Audit Priority	Priority
------	-------------	----------------	----------

Policies and Procedures [Add] [v] [≡]

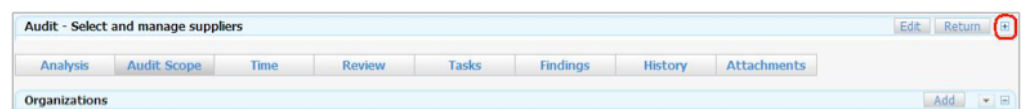
Records: 0 50 Per Page

Name	Description	Audit Priority	Priority
------	-------------	----------------	----------

- Select the processes that you want to pull into scope for the audit (see Search Functionality for details on using the search)
- Click **Save**

In order to assign auditors to the audit in the e-Governance Portal, please follow these steps:

- Click **+** in the top right corner

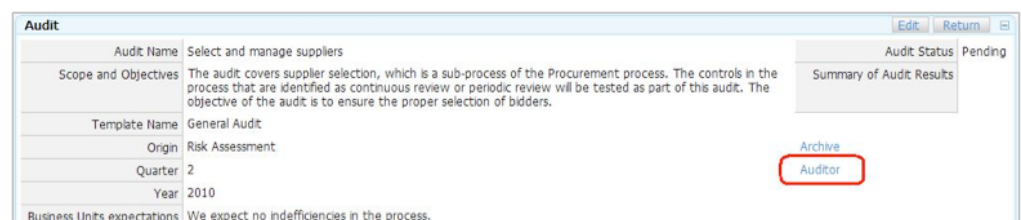


Audit - Select and manage suppliers [Edit] [Return] **+**

Analysis **Audit Scope** Time Review Tasks Findings History Attachments

Organizations [Add] [v] [≡]

- Click on link Auditor



Audit [Edit] [Return] [v]

Audit Name	Select and manage suppliers	Audit Status	Pending
Scope and Objectives	The audit covers supplier selection, which is a sub-process of the Procurement process. The controls in the process that are identified as continuous review or periodic review will be tested as part of the audit. The objective of the audit is to ensure the proper selection of bidders.		Summary of Audit Results
Template Name	General Audit		
Origin	Risk Assessment		
Quarter	2		
Year	2010		
Business Units expectations	We expect no inefficiencies in the process.		

Archive Auditor

- Click on **▼** and click Link Users, to open the list of auditors that can be linked to the audit
- Select the auditors that you want to link to the audit and click **Save**



7

Planning Phase

Step	Planning	Execution (Fieldwork)	Reporting	Monitoring
Owner	<ul style="list-style-type: none"> Audit Committee and Internal Audit Executive Management 	<ul style="list-style-type: none"> Internal Audit 	Internal Audit	<ul style="list-style-type: none"> Audit Committee and Internal Audit Executive Management
Description	<ul style="list-style-type: none"> Conduct Initial consultation with stakeholders to receive input and data. Develop the scope, objectives and approach for the audit and validate with management. Determine audit budget (time) and allocate resources Document systems and processes Develop detailed audit plan (Work Program) 	<ul style="list-style-type: none"> Conduct Audits Identify Issues Conduct Closing meeting 	<ul style="list-style-type: none"> Issue draft Internal Audit Report Obtain Management feedback Issue Final Internal Audit Report (including Management Action Plans) 	<ul style="list-style-type: none"> Monitor progress on management actions based on action plan defined in the Internal Audit Report and implementation schedule determined by the management.
Key Deliverables	<ul style="list-style-type: none"> Audit Planning Letter Audit Scope Form Detailed Work Program 	<ul style="list-style-type: none"> Issue Form 	<ul style="list-style-type: none"> Draft Internal Audit Report Management Action Plan Final Internal Audit Report 	<ul style="list-style-type: none"> Follow up Report

7.1 Introduction

The Internal Audit Function must ensure that its planning for an audit is sufficiently detailed. The key steps to be undertaken as part of the planning process include:

- Contact the concerned management to agree on matters pertaining to the audit
- Send an Audit Planning Letter (refer to "Audit Planning Letter" template in Appendix 7)
- Conduct initial consultation with management to receive data (refer to the "Data Request Form" in Appendix 8)
- Validate high-level scope with management
- Develop a preliminary work program for the audit
- Validate and agree on a detailed approach for the audit with the Internal Audit team
- Develop a budget
- Develop detailed work program
- Validate that the work program is aligned with scope

The Internal Audit Function should also seek to define and understand expectations in terms of:

- Business objectives
- Internal audit approach
- Stakeholder expectations
- Contractual requirements
- Service delivery requirements
- Key performance indicators

7.2 Validate High-Level Scope With Management

The Internal Audit Function will develop the high-level scope for the audit based on the risks identified within the auditable area during the Risk Assessment Phase.

The scope should consider:

- the nature of the audit (i.e. high-level, process-wide review, or a detailed risk and control analysis in a particular phase of the process)
- which sub processes, initiatives, functions, and / or activities are to be the focus of the audit
- particular areas of the process to be included or excluded
- the key risks that impact the process/initiative, functions and / or activity being audited
- the characteristics relevant to the process, initiative, function, and / or activity
- any analytical procedures to be performed
- third party (i.e. Abu Dhabi Accountability Authority, Department of Finance) expectations from the audit

7.2.1 Output from the high-level scope

Using the high-level understanding gained to date and the results of the Risk Assessment, the Internal Audit Function should validate with management the high-level scope and draft an "Audit Scope Letter" that details:

- Processes, initiatives, functions, and / or activities to be included in the Audit
- The inclusion of key considerations from the high-level understanding and the approach to be adopted for example, if the audit approach anticipates using analytics, make reference to the strategy to facilitate discussion on data availability, integrity, and accessibility
- The nature, timing, and extent of audit procedures – the Internal Audit Function should determine the nature of the different procedures they may carry out, including process review, control testing, transaction testing, etc
- Stakeholder-prepared documentation - during the development of the project scope, the Internal Audit team may identify certain analyses or documentation that the stakeholder needs to develop or prepare. These requirements should be discussed with the stakeholder to reach an agreement on the format and timing
- Expected outputs and/or reports from the audit - specific report expectations should be validated with management and adjusted as necessary
- Timelines, communication, and reporting protocols - for example, include the protocols to follow if management action plans are not received in a timely manner for inclusion in the monitoring and follow-up

- Internal Audit team members - this information should identify and present the Internal Audit team members. Only those team members who have the appropriate skills and competencies to perform the work should be assigned to the audit.

In order to assign access the built-in audit document templates in the e-Governance Portal, please follow these steps:

1. On the homepage dashboard, click on Audit Plan
2. Click on the name of the audit you want to work on
 - a. Click on the status link for the activity "Send Audit Planning Letter"
 - b. Click on the link [Audit Document Template](#) and then the [Audit Planning Templates](#)
 - c. You can download the templates for the Planning Letter, Data Request Form and Detailed Scope Letter here

A sample "Audit Scope Letter" is presented in Appendix 9.

Documentation Template

Name: Audit Planning Templates

Description:

Edit

Copy

Documentation Template List

Document Templates

Add

Number of Records: 3

Category	Type	Name	Description
* None Selected	* None Selected	View Audit Planning Letter	
* None Selected	* None Selected	View Data Request Form	
* None Selected	* None Selected	View Detailed Scope Letter	

The engagement team should meet during this planning phase to address:

- stakeholder expectations of the engagement and the specific audit project
- audit objectives and scope
- Internal Audit team goals and objectives

Did you know?

Audit Templates: Upload all the audit document templates (Audit Planning Letter, Data Request Form, etc) to the Portal to promptly access them during the audit. Uploading the documents can be done from: Navigation -> Library -> Internal Audit -> Document Templates

7.3 Develop A Preliminary Work Program For The Audit

An Internal Audit planning meeting will be held with the Internal Audit team members to plan the audit, agree on milestones and assign roles and responsibilities. Based on the proposed testing strategy, the discussions held during the meeting, and the scope agreed with the stakeholder, the Internal Audit team should develop a high-level preliminary work program which reflects the areas that its work will focus on. The detail(s) of the specific work steps will be added as further understanding of the process, initiative, function, and / or activity is gained / validated in meetings between the Internal Audit team and auditee personnel. The testing strategy for each risk should be documented in the Risk Register.

In order to create a preliminary test plan in the e-Governance Portal, follow the steps below:

1. Click on the status link of the activity “Develop Preliminary Work Program”

Sort	Phase	Audit Activity	Status
0001	Planning	Send audit planning letter	1. Not Started
0002	Planning	Send detailed scope letter	1. Not Started
0003	Planning	Conduct Opening Meeting	1. Not Started
0004	Planning	Conduct Internal Meeting With Audit Team	1. Not Started
0005	Planning	Develop Preliminary Work Program	1. Not Started
0006	Planning	Document Systems and Processes	1. Not Started
0007	Planning	Complete Planning Checklist	1. Not Started
0008	Planning	Make advanced information requests	1. Not Started

2. Click on the status link in the column “Audit Fieldwork”
3. Click **Add** in the Test section to create a test

Test Name	Test Results Summary	Test Results
<div> Edit All Add Execute Edit Search </div>		

4. Enter all the information about the test.
5. Click **Save**

7.3.1 Output From “Develop A Preliminary Work Program”

Internal audit documentation should contain:

- A copy of the audit scope letter and any revisions necessary to align the initially planned scope with the actual scope of the audit
- The preliminary work program.

7.4 Validate/Document Understanding Of The Process/ Initiative/Function/Activity Being Audited

In order to facilitate the development of the appropriate work program to execute the audit, the Internal Audit team should validate the understanding of the process, initiative, function, and/or activity with stakeholder personnel and management as appropriate. This may be done by sending the documentation of the team's understanding of business to concerned management for review and feedback, or by holding meetings.

7.5 Develop Detailed Work Program

Based on the proposed testing strategy, as detailed in the Risk Assessment Strategy (Refer to Section 6.10), the Internal Audit team's understanding of the process, initiative, function, and/or activity, and the agreed approach for the audit, the Internal Audit team will develop a detailed work program of procedures to be performed in executing the audit.

Efficient execution of the detailed work program is achieved only if the description of steps is explicit with respect to the nature, timing, and extent of procedures.


7.6 Validate That The Work Program Is Aligned With Scope

Before executing the detailed work program, the Internal Audit team should revisit the Audit scope letter and consider whether:

- the detailed work program is consistent with the scope of the "Audit Scope Letter"
- all expectations and coverage issues noted during the planning and risk assessment activities (or other risk assessment activities performed by management) are appropriately considered in the detailed work program

The Internal Audit team should then discuss, with the process owner, any significant changes in the scope of the audit reflected in the detailed work program and either adjust the work program to fit the original agreed-upon scope or obtain an updated "Audit Scope Letter" for the revised scope.

To validate that the work program is aligned with the audit scope in the e-Governance Portal, follow the steps below:

1. Click on the name of the audit
2. Click on the link of the activity "Complete Planning Checklist"
3. Click  in order to complete the checklist



Activity

Edit

Return

Audit Name

Human Resources Audit

Name

Complete Planning Checklist

Description

Complete Planning Checklist

Status

6. Complete

Resources

Audit Document Template

Add Comment

Recent Comment

Work Paper

Review

Tasks

Findings

Attachments

History

CheckList Items

Edit

Number of Records: 2

50

Resize

Response	Checklist Item	Comments
<input type="checkbox"/>	01. Confirm that the original agreed-upon scope of the Audit is still appropriate, if not update the Audit Schedule Form with the new scope, as well as an explanation for the revision.	1
<input type="checkbox"/>	02. Determine whether the scheduled hours for the Audit can be reduced, if the hours can be reduced, update the Audit Schedule Form with the revised hours as well as an explanation for the revision.	1

7.7 Budgets

Each audit is allocated a time budget in hours. It is the responsibility of the Head of Internal Audit and/or the Auditor In-Charge to allocate a budget for each auditor involved in the audit, including time allocated for Internal Audit management's review or quality assurance.

The Auditor In-Charge is responsible for managing the budget and for providing reasons for variations between actual and budgeted hours. Therefore it is important to note circumstances that may cause budget variations.

7.8 Travel Arrangements

This should be determined by each Subject Entity depending on their assessed requirements for travel.

8

Execution (Fieldwork) Phase

8.1 Introduction

Audit procedures, including the testing and sampling techniques to be employed, should be selected in advance where practical, and expanded or altered if circumstances warrant. The process of collecting, analyzing, interpreting, and documenting information should be supervised to provide reasonable assurance that the internal auditor's objectivity is maintained and that audit goals are met.

The Head of Internal Audit should review the composition of the Internal Audit team to ensure that the assigned team members have the appropriate skills and competencies to perform the work. He may also conduct an opening meeting with management in the area being audited to clarify the scope and approve the final protocols for the audit.

Work papers are prepared during the execution phase of the Internal Audit and generally:

- provide the principal support for the audit report
- aid in the planning, performance, and review of audit
- document whether the audit objectives were achieved
- facilitate third-party / peer review
- provide a basis for evaluating the audit activity's quality program
- demonstrate the audit compliance with professional standards.

8.2 Detailed Work Program

The Internal Audit team should execute the procedures in accordance with the detailed work program. When performing audit procedures, supporting documentation must be maintained and reviewed.

In order to execute the audit program in the e-Governance Portal, please perform the following steps.

8.2.1 Evaluate the Audit Risk Register

The Audit Risk Register allows the Internal Auditor to evaluate controls and risks from the perspective of the specific audit he/she is working on. In this context, the steps to follow are to first evaluate the tests that are created for the controls, then update the control effectiveness and finally update the Risk Rating based on the effectiveness of the related Control.

8.2.1.1 Perform Tests

In the execution phase of the Audit, the detailed Test plans are created and evaluated. Test plans have to be created to cover all (in scope) controls in the Risk Register.

To create and evaluate the detailed Test plans, complete the following steps:

1. Select the Audit Plan link from the home page
2. Select the appropriate Audit Name
3. Click on the status link for the activity “Perform Fieldwork”

Sort	Phase	Audit Activity	Status
0001	Planning	Send audit planning letter	6. Complete
0002	Planning	Send detailed scope letter	6. Complete
0003	Planning	Conduct Opening Meeting	6. Complete
0004	Planning	Conduct Internal Meeting With Audit Team	6. Complete
0005	Planning	Develop Preliminary Work Program	6. Complete
0006	Planning	Document Systems and Processes	6. Complete
0007	Planning	Complete Planning Checklist	6. Complete
0008	Planning	Make advanced information requests	6. Complete
0009	Fieldwork	Perform Fieldwork	1. Not Started
0010	Reporting	Draft IA Report	1. Not Started
0011	Reporting	Complete Audit Report Review Checklist	1. Not Started
0012	Reporting	Conduct Closing Meeting	1. Not Started
0013	Reporting	Issue Final Report	1. Not Started
0014	Quality Assurance	Complete Quality Assurance Checklist	1. Not Started

4. Click on the status link in the Audit Fieldwork column of the auditable unit (e.g. organization, process, IT application or project/event)

Activity

Audit Name: Human Resources Audit

Name: Perform Fieldwork

Description: Perform Fieldwork

Status: 1. Not Started

Resources: Audit Document Template

Add Comment

Recent Comment

Work Paper | Review | Tasks | Findings | Attachments | History

Risk Control Matrix(RCM) Audit Form

Records: 1 | 50 | Per Page


Entity Name	Entity Type	Audit Fieldwork	Risk Register
001.001 Human Resources (ABC Company)	Process	1. Not Started	3. Completed

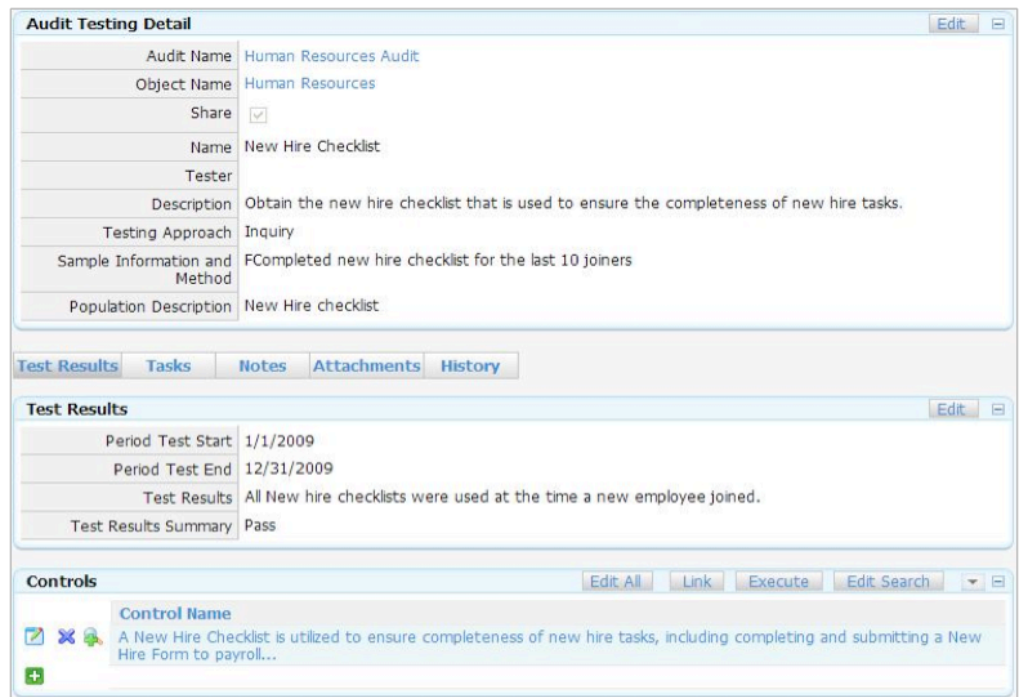
5. Click on any of the tests created during the phase “Develop Preliminary Audit Program” or create new tests as described in section 7.3
6. Click on the Name of the test
7. Click [Link](#) in the Controls Section
8. Select the Controls to which the Test should be linked and click [Save](#)


The detailed work program should be reviewed with all team members and signed off by the Head of Internal Audit.

To perform the tests in the e-Governance Portal, follow the steps below:

1. Go to the Audit Risk register
2. Click on the name of the test that you performed
3. Click [Edit](#) in the Test Results section


4. Enter the testing period and results
5. Click 







Audit Testing Detail 




Audit Name	Human Resources Audit
Object Name	Human Resources
Share	<input checked="" type="checkbox"/>
Name	New Hire Checklist
Tester	
Description	Obtain the new hire checklist that is used to ensure the completeness of new hire tasks.
Testing Approach	Inquiry
Sample Information and Method	Completed new hire checklist for the last 10 joiners
Population Description	New Hire checklist

[Test Results](#) | [Tasks](#) | [Notes](#) | [Attachments](#) | [History](#)

Test Results 



Period Test Start	1/1/2009
Period Test End	12/31/2009
Test Results	All New hire checklists were used at the time a new employee joined.
Test Results Summary	Pass

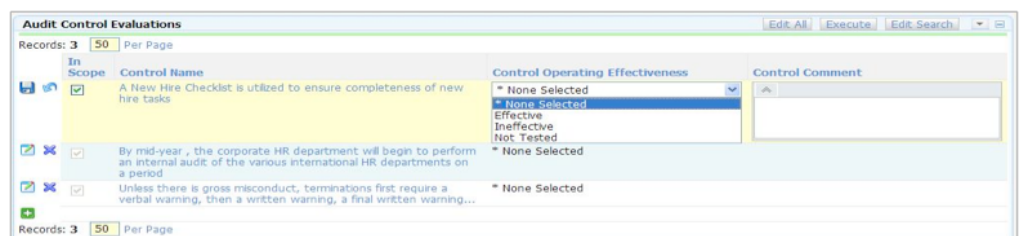
Controls    




Control Name
   A New Hire Checklist is utilized to ensure completeness of new hire tasks, including completing and submitting a New Hire Form to payroll...

Note: Attachments related to the test can be uploaded under the Attachments tab on the Test form


8.2.1.2 Evaluate Controls

1. Based on the test evaluation, update the control effectiveness by clicking  next to the control that you wish to evaluate (or click  to evaluate all controls at once)




Audit Control Evaluations   

Records: 3 | 50 | Per Page

In Scope	Control Name	Control Operating Effectiveness	Control Comment
<input checked="" type="checkbox"/>	A New Hire Checklist is utilized to ensure completeness of new hire tasks	 * None Selected * None Selected Effective Ineffective Not Tested	
<input checked="" type="checkbox"/>	By mid-year, the corporate HR department will begin to perform an internal audit of the various international HR departments on a period	* None Selected	
<input checked="" type="checkbox"/>	Unless there is gross misconduct, terminations first require a verbal warning, then a written warning, a final written warning...	* None Selected	

Records: 3 | 50 | Per Page

Note: To see what tests were performed for the control, click on the control name and scroll down to the Tests section in the pop-up window)

2. Select "Effective", "Ineffective", or "Not Tested" from the dropdown list.
3. Click 

8.2.1.3 Evaluate Risks

1. Based on the Control evaluation, update the Risk field “Operating Effectiveness” by clicking Edit next to the Risk that you wish to evaluate
2. Select one of the Operating Effectiveness values from the dropdown menu

In Scope	Risk Name	Risk Description	Risk - Controls Rating	Risk - Operating Effectiveness	Risk - Residual Risk Rating (Audit)
<input checked="" type="checkbox"/>	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.	4 - Design Adequate	* None Selected * None Selected Well Controlled Adequately Controlled Inadequately Controlled None Selected	*None Selected
<input checked="" type="checkbox"/>	Confidentiality of employees' personal information is not safeguarded.	Confidentiality of employees' personal information is not safeguarded. Employee personnel files are not maintained in accordance with applicable retention requirements.	8 - Design Inadequate		*None Selected

3. Click **Save**

Note: To see the effectiveness of the controls that are linked to the risk, click on the risk name and scroll down to the controls section in the pop-up window.

Did you know?

Control over the audit work: by clicking on the “History” tab of audit working papers, risks, controls or tests, you can track the changes made to the work documents with all the relevant details (names, dates, previous field values, etc).

The screen shot below presents the layout of a completed Audit field work phase:

Audit Risk Control Matrix Evaluation

Audit Name: Accounts Payable Template Library Link

Entity Name: Accounts Payable

Status: Complete

Documentation Status: Create Documentation...

Analysis Findings History

Audit Testing Details Evaluation

Records: 3 50 Per Page

Test Name	Test Results Summary	Test Results
Validate vendor master file is restricted	Pass	
AP Policy is clearly communicated across process	Pass	
Management review and approval	Fail	

Audit Control Evaluations

Records: 3 50 Per Page

In Scope	Control Name	Control Operating Effectiveness	Control Comment
<input checked="" type="checkbox"/>	A/P access to vendor master file is restricted to select data fields (address, phone, terms)	Effective	No Comment
<input checked="" type="checkbox"/>	Receiving enters all receipts only against an open Purchase Order in the system.	Effective	No Comment
<input checked="" type="checkbox"/>	Restrict access to accounts payable files and supplies to the employees in the payables area.	Ineffective	No Comment

Audit Risk Evaluations

Records: 3 50 Per Page

In Scope	Risk Name	Risk Description	Risk - Controls Rating	Risk - Operating Effectiveness	Risk - Residual Risk Rating (Audit)
<input checked="" type="checkbox"/>	Misappropriations or fraudulent payments	Misappropriations or fraudulent payments	4 - Design Adequate	Inadequately Controlled	Periodic Review
<input checked="" type="checkbox"/>	Unauthorized access to accounts payable records and stored	Unauthorized access to accounts payable records and stored	1 - Design Adequate	Adequately Controlled	Continuous Review
<input checked="" type="checkbox"/>	Unintentional or deliberate errors on supplier invoices	Unintentional or deliberate errors on supplier invoices	8 - Design Inadequate	Well Controlled	Continuous Review

8.3 Sampling Techniques

During the fieldwork, the Internal Audit Function may rely on sampling to arrive at meaningful inferences about the population under examination. The question that must always be answered prior to commencing fieldwork is one of scope and, more specifically, how much evidence should be gathered to satisfy a particular audit objective or support a conclusion.

Both judgmental and statistical sampling methods are based on the premise that all evidence in support of a particular assertion need not be examined to confirm the assertion's validity. The type of sampling methodology used is a matter of judgment and thus this decision should be made by the more experienced members of the engagement team, i.e. the team leader and / or the Head of Internal Audit.

Obviously, the more critical the results are, the higher the requirement for more extensive testing. With the increasing use of information technology, the Internal Audit Function must decide whether sampling is the most efficient and effective way to obtain evidence. This increase in the use of information technology raises the fact that there may also be situations where the entire population can be examined by using file interrogation software, data mining, data warehouses or other information retrieval approaches. Furthermore, sampling in auditing can be defined as the process of selecting and examining a portion of a group of related items for the purpose of obtaining information or evaluating some characteristic about the group as a whole. The entire set of data from which the sample is selected is called the **population**, and the individual items that constitute the populations (and are available for selection) are called **sampling units**.

The Internal Audit Function realizes that by sampling, Internal Audit personnel accept the risk that the sample selected does not truly represent the population. To further explain, the audit risk in sampling relates to the possibility that a materially incorrect inference about a population may be reached as a result of sampling. This risk has two components:

- Sampling error
- Non sampling error.

8.3.1 Sampling Error

In every sample, there is a possibility that the sample will provide information that is not representative of the population. The aspect of this possibility caused purely by random chance in sample selection is the risk of "**Sampling Error**". The sampling error risk is available in every sample, regardless of how the sample is selected. The Internal Audit Function realizes that the control to reduce the risk is by applying professional judgment and following the appropriate procedures in choosing the Internal Audit samples.



8.3.2 Non sampling Error

Similarly to the sampling error risk, every sample is subject to the risk of non-sampling error. Non sampling errors can affect the representativeness of the sample, but they also can relate to all other aspects of the sample. They include the use of inappropriate sampling techniques, improper definition of the population, mistakes in selecting the sample, etc.

In other words, the risk of non sampling error encompasses all possible mistakes, oversights and misjudgments that may produce and incorrect inference from the sample.

To mitigate or minimize that risk, the Internal Audit Function should accentuate the importance of adequate planning, supervision and the proper execution of the audit plan.

8.3.3 Sample Size

Whether designed to test attributes or amounts, all samples follow either a statistical or judgmental (non-statistical) approach. There is no difference between statistical sampling and judgmental sampling in the execution of a sampling plan, nor does the approach affect the competence of the evidence obtained or the Internal Audit Function's response to detected errors. Selection between statistical or judgmental sampling should be made after careful evaluation of both the pros and cons of each.

The sections below further describe both sampling methods.

8.3.4 Statistical Sampling

Statistical sampling is an objective method of determining the sample size and selecting items to be examined. Unlike judgmental sampling, it provides a means of quantitatively assessing precision or allowance for sampling risk (how closely the sample represents the population) and reliability or confidence level (the probability the sample will represent the population). Furthermore, statistical sampling provides a specific estimate of an occurrence rate or of a monetary amount.

The advantage of this approach is that the reliability of the results is determined through the use of the probability theory. That is by following prescribed procedures for selecting the sample and calculating the results, the Internal Audit Function can use a statistical model to measure risk of sampling error.

8.3.5 Judgmental Sampling

Judgmental sampling is a subjective approach to determining the sample size and sample selection. This subjectivity is not always a weakness. Internal Audit personnel, based on other work, may be able to test most material and risky transactions and to emphasize the types of transactions subject to high control risk. In judgmental sampling or non-statistical sampling, the Internal Audit Function relies solely on judgment to assess the risk of sampling error and evaluate the population. Although the risk of sampling error cannot be measured in a judgmental sample, the Internal Audit Function can attempt to control it by following certain guidelines and procedures.

8.3.6 Taking the Sample

When defining the sample to be used to provide evidence during the audit engagements, the Internal Audit Function may adopt the following principles of selection to guide its Internal Audit personnel:

- Know your population because audit conclusions may be based only on the sample taken from that population
- Define the sampling unit in terms of the audit objectives
- Let every sampling unit in the population have an equal chance of being selected.

8.3.7 Sample Selection Techniques

Sample selection techniques include the following:

- Random Selection
- Systematic Selection
- Cluster Selection
- Haphazard Selection
- Judgmental Selection

Random, Systematic and Cluster Selection are broadly referred to as random - based selection techniques. These techniques provide reasonable assurance that each sampling unit has a predetermined probability of being selected, and prevent unintentional bias in the selection. Haphazard and judgmental selections are considered as non-random selection techniques. The random-based selection techniques must be used in statistical sampling. These techniques are further described below.

8.3.8 Random Selection

Random selection eliminates subjective factors from the selection process, including any conscious or unconscious bias that might affect the likelihood of certain sampling units being selected or not. Although there is always some risk that a sample will not be representative of the population, random selection, by eliminating bias, entails less sampling error risk than other selection techniques. It therefore should be considered whenever the risk is of significant concern.

There are many ways of selecting random samples, including:

- Random selection software routines, which are selection routines in audit software that can extract random samples from the auditee's records
- Computerized random number generators which can provide lists of random numbers from the selected population.

8.3.9 Systematic Selection

Systematic selection is the selection of sampling units at fixed intervals within the population. This technique usually produces a close approximation of a random selection

technique. In this technique, a sampling interval is calculated by dividing the desired sample size into the number of sampling units in the population. Starting at the front of the population, a group of items equal in number to the interval is determined and one item is randomly selected for the sample from the group. Beginning with the next item, the sampling interval is applied regularly throughout the rest of the population and the last item in each interval is selected; e.g. to obtain a sample of 200 from a population of 10,000, an item is drawn from the first 50 items and every 50th item is selected thereafter.

Systematic selection, while it could be widely used, is not as conceptually sound as random selection because of the possibility that a systematically drawn sample might be biased due to the manner in which the sampling units are arranged.

8.3.10 Cluster Selection

Cluster samples are used when a population is so dispersed that systematic selection would be burdensome. Cluster sampling is the method of sampling whereby the population is formed into groups or “clusters” of items. The first step is to make a random selection of clusters to include in the sample, then the items within the selected clusters may be randomly selected and sampled. This is called Multi-Stage Sampling. Cluster Sampling is commonly used to get the most precise results from a fixed budget for example, yet it is not as precise as Random selection.

8.3.11 Haphazard Selection

Haphazard selection is the selection of a sample without following any organized or structured approach. Further, haphazard selection involves selecting items that are readily at hand taking the easy approach rather than the reasoned approach; e.g. the haphazard sampling of purchase orders would include choosing a sample of purchase orders that are readily available not taking into account such factors such as the items on the purchase order, the amount of the purchase order, the date of the purchase order, etc.

The objective is to obtain an approximation of a random based sample. Its advantage is that it may be easier to apply than other techniques, especially if audit software is not available and sampling units are not numbered or ordered in a way that facilitates random-based selection. When using this technique, the Internal Audit team should be careful not to consciously introduce bias into the selection such as the unconscious avoidance of the first or last page of a document / register / list.

8.3.12 Judgmental Selection

In applying judgmental selection, the Internal Audit team would select the audit samples based on their personal judgment and reasoning. Judgmental selection could be used to support the Internal Audit testing as defined below:

- To select examples of deficiencies to support the Internal Auditors’ contention that the system is weak
- The judgmental selection can be used where it is known that the population has no variability, e.g. in an information system where each item is treated the same way by the system.

8.4 Audit Techniques

There exist numerous techniques from various disciplines which can be used to perform the field work in terms of data selection and analysis. The techniques adopted by the Internal Audit team should be those most suitable for the needs and circumstances of the particular audit in question.

Some of the techniques auditors can use to obtain audit evidence and to analyze performance data include:

- Surveys;
- Examination;
- Benchmarking;
- Work Study;
- Flow Charting;
- Questionnaires;
- Interviewing;
- Focus Groups;
- Statistical Analysis;
- Computer Assisted Audit Techniques (CAATs)

With regard to information technology audits, the techniques and types of data interrogation with modern audit software are almost unlimited. Thus, audit software presents numerous commands that support the Internal Auditor's requirement to review transactions for fraud such as the existence of duplicate transactions, missing transactions, and anomalies. Examples of these commands include:

- comparing employee addresses with vendor addresses to identify employees who are also vendors;
- searching for duplicate cheque numbers;
- analyzing the sequence of all transactions to identify missing cheques or invoices;
- identifying vendors with more than one vendor code and/or more than one mailing address;
- finding several vendors with the same mailing address;
- sorting payments by amount to identify transactions that fall just under or above a particular threshold limit to test compliance with authority delegations.
- CAATs may also be used in performing various audit procedures including:
- tests of transactions and balances such as recalculating interest;
- analytical review procedures such as identifying inconsistencies or significant fluctuations;
- compliance tests of general controls such as testing the set-up or configuration of the operating system or procedures to the program libraries;



- sampling programs to extract data for audit testing;
- compliance tests of application controls such as testing the functioning of a programmed control.

8.5 Identifying Information

Internal Auditors should identify sufficient, reliable, relevant, and useful information to achieve the audit's objectives. Internal Auditors should thus identify the following:

- The information to be collected on all matters related to the audit objectives and scope of work.
- The analytical auditing procedures to be used when identifying and examining information.

The information should be sufficient, reliable, relevant, and useful to provide a sound basis for audit observations and recommendations.

Sufficient - when the evidence is factual and persuasive enough that a prudent, informed person would reach the same conclusion.

Reliable - when the evidence can be verified by others and has been gained through competent and appropriate audit procedures.

Relevant - when the evidence collected relates directly to the areas being tested.

Useful - when the evidence collected allows the Internal Auditors to form a view on whether the Subject Entity is meeting its goals and objectives and accomplishing the desired result.

8.5.1 Analysis & Evaluation

Internal Auditors should base conclusions and audit results on appropriate analyses and evaluations. Audit procedures should be used during the audit to examine and evaluate information to support audit results.

Internal Auditors should consider the factors listed below in determining the extent to which analytical auditing procedures should be used:

- Significance of the area being examined
- Adequacy of the system of internal control
- Availability and reliability of information
- Precision with which the results of analytical auditing procedures can be predicted
- Availability and comparability of information
- Extent to which other audit procedures provide support for results.

After evaluating these factors, internal auditors should consider and use additional auditing procedures, as necessary, to achieve the audit objective.

8.5.2 Recording Information

Internal Audit documentation should support execution of the work program and related findings/issues noted, including the following as applicable:

- Understanding of business process(es) and/or transactions
- Evaluation of the system of control design
- Results of testing
- Issues summaries
- Walk-through documentation

Internal Auditors should record relevant information to support the conclusions and audit results. Audit documentation should be prepared by the Internal Auditor and reviewed by the Senior Internal Auditor or the Head of Internal Audit.

The documentation should include the information obtained and the analyses made, and should support the basis for the observations and recommendations to be reported.

8.6 Raising Internal Audit Issues


When issues and/or exceptions are identified as a result of the procedures carried out, the Internal Audit team should consider them first in the context of the purpose of the audit, then in the context of the potential impact on the process, initiative, function, activity, and/or Subject Entity as a whole.

For example, if the work program consists of procedures to test accounts payable reconciliations, the Internal Audit team should consider individual exceptions for the purposes of recommending to management steps to correct the errors; the Internal Audit team should also consider the exceptions in light of the entire accounts payable process to raise with management any potential overall process issues.

The Internal Audit team should meet with Subject Entity personnel and management to review the overall results of the Audit. The Internal Audit team should focus on reviewing the issues and/or exceptions identified during the assignment with management and obtaining additional insight from them as to root cause (if applicable), and information related to the issues and/or exceptions that the team may want to include in the audit report. This communicates a cooperative spirit with management by advising them early on about issues and recommendations.

The Internal Audit team is also encouraged to work with management to identify possible connections between individual issues and/or exceptions which may affect any action plans that will be co-developed.

In order to create a finding in the e-Governance Portal, please follow these steps:

1. Select the Audit Plan link from the home page
2. Click on the name of the Audit
3. Click on the status link of the activity 'Perform Fieldwork'
4. Click on the status link in the Audit Fieldwork column of the auditable unit (e.g., organization, process, IT application or project/event)
5. Click Add Findings  next to the Risk that is related to the finding
6. Fill the Audit Finding template (see below).

Audit Risk Evaluations					
Records: 10 50 Per Page					
In Scope	Risk Name	Risk Description	Risk - Controls Rating	Risk - Operating Effectiveness	Risk - Residual Risk Rating (Audit)
<input checked="" type="checkbox"/>	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.	4 - Design Adequate	Inadequately Controlled	Active Management

Audit Finding		Return	Save	Save As	Delete	Cancel
Notification	Notification					
Auto Email	<input type="checkbox"/>					
Audit Name	Human Resources Audit					
Workpaper Name	Develop Preliminary Work Program					
Object Name	Background checks are not performed on new employees, therefore exposing the organization to potential loss and/or theft.					
Name	Background checks are not performed on new					
Observation/Process Enhancements	<div> </div> <p>Our observation pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue. Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat. Maecenas purus erat, mollis vitae, au.</p>					
Criticality	* None Selected					
Type	* None Selected					
Recommendation	<div> </div> <p>Our recommendation is to massa non nisl. Aliquam erat volutpat. Maecenas purus erat, mollis vitae, auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit.</p>					
Auditor Assigned	Vincent Degens					
Management Owner	Ahmed M.					
Management Response Due Date	5/31/2010					
Management Response Status	* None Selected					
Remediation Date						
Reminder Days	7					
Review Status						
<div>Save Save As Delete Cancel</div>						

7. Click 

Did you know?

Email Notification: Use email notification to notify management owners of findings identified during the audit. When email notification is enabled, the person responsible for the finding will receive an email containing a link to the section of the finding where he/she can respond by entering an action plan and comments. This will allow an efficient management of the audit findings and allows to keep track of the status of all the findings related to the audit. Contact your IT administrator to enable the email notification functionality in the Portal.

8.7 Co-Develop Action Plans With Management

The Internal Audit team should work with management to co-develop action plans to address the issues and/or exceptions that were identified during the course of the audit. The action plans, at a minimum, should cover the following elements:

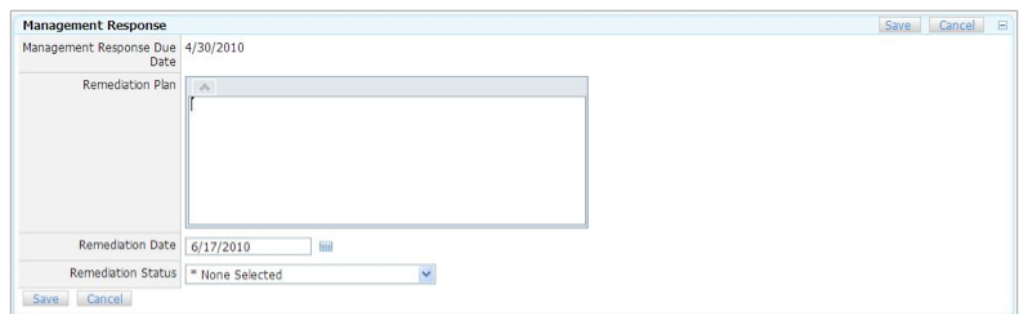
- What is (are) the action(s)?
- Who is responsible for implementing the action(s)?
- When will the action(s) be started and completed?


The Internal Audit team may consider the use of facilitated sessions to co-develop the action plans with management. The use of facilitated sessions to finalize action plan development and ownership provides the benefit of being able to obtain real-time consensus from all those present during the session.

The finalization of action plans, the assignment of action plan ownership, and the communication to action plan owners are all the responsibility of management.

In order to create the management action plans in the e-Governance Portal, please follow the following steps:

1. The business owner will receive an email with a link to the finding in the e-Governance Portal
2. Click **Edit** in the Management Owner Section of the finding (only accessible by the management owner assigned to the finding)



3. Complete the Remediation Plan section and select the Remediation Date
4. Click 

8.8 Audit Supervision

Audits should be properly supervised to ensure objectives are achieved, quality is assured, and staff are developed. Supervision begins with planning and continues throughout the examination, evaluation, communicating and follow-up phases of the audit.

Supervision includes:

- ensuring that the Internal auditors assigned to the engagement possess the requisite knowledge, skills and other competencies to perform the audit;
- providing appropriate instructions during the planning of the audit and approving the audit program;
- ensuring that the approved audit program is carried out as approved unless changes are both justified and authorized;
- determining that audit working papers adequately support the audit observations, conclusions, and recommendations;
- ensuring that the audit report is accurate, objective, clear, concise, constructive and timely;
- ensuring that audit objectives are met;
- Providing opportunities for developing auditors' knowledge, skills and other competencies.

Appropriate evidence of supervision should be documented and retained. The extent of supervision required will depend on the proficiency and experience of the assigned auditors and the complexity of the audit.

Appropriate supervision also allows for resolution of differences in professional judgment over significant issues relating to the audit. Further it allows for the documentation and disposition of differing viewpoints in the audit working papers. The objectives of documenting the supervision work are to:

- provide evidence of supervisory review. This would consist of the reviewer initialling and dating each working paper after it is reviewed;
- ensure that working papers and conclusions properly support the audit report and that all necessary audit procedures have been performed;
- reflect any other review techniques that provide evidence of supervisory review including completing an audit working paper review checklist and/or preparing a memorandum specifying the nature, extent, and results of the review.

Reviewers may develop a written record (review notes) of questions arising from the review process. When clearing review notes, care should be taken to ensure that the documentation provides adequate evidence that questions raised during the review have been resolved.

In order to document the supervision work in the e-Governance Portal, please follow these steps.

1. Click on the name of the audit
2. Click on the status link of the activity you want to review

Audit Activity				
Records: 14		50	Per Page	
Sort	Phase	Audit Activity	Status	
	0001	Planning	Send audit planning letter	4. Request for Manager Review
	0002	Planning	Send detailed scope letter	1. Not Started
	0003	Planning	Conduct Opening Meeting	1. Not Started
	0004	Planning	Conduct Internal Meeting With Audit Team	1. Not Started
	0005	Planning	Develop Preliminary Work Program	1. Not Started
	0006	Planning	Document Systems and Processes	1. Not Started
	0007	Planning	Complete Planning Checklist	1. Not Started
	0008	Planning	Make advanced information requests	1. Not Started
	0009	Fieldwork	Perform Fieldwork	1. Not Started
	0010	Reporting	Draft IA Report	1. Not Started
	0011	Reporting	Complete Audit Report Review Checklist	1. Not Started
	0012	Reporting	Conduct Closing Meeting	1. Not Started
	0013	Reporting	Issue Final Report	1. Not Started
	0014	Quality Assurance	Complete Quality Assurance Checklist	1. Not Started

3. Change the status of the activity to Review Comments or Completed and add a Comment in the Add Comment box

Activity		Return	Save	Cancel
Audit Name	Human Resources Audit			
Name	Send audit planning letter			
Description	Send audit planning letter			
Status	4. Request for Manager Review			
Resources	1. Not Started			
Add Comment	2. In Progress 3. Request for Team Leader Review 4. Request for Manager Review 5. Review Comments 6. Complete Not Applicable			
Recent Comment				
Save	Cancel			

4. Click **Save**

Did you know?

Review Status Search: Create and save your own search to show the status of the audit work papers and other relevant information from the work paper, such as Activity Name, Auditor(s)' comments, etc. To create a search, go to:

- Navigation (left side pane) -> Search -> Internal Audit
- Click on the "Core Audit Search" link
- Click "Edit Search" and select the columns to display

9

Reporting Phase

9.1 Introduction

The Head of Internal Audit is responsible for communicating the results of the audit/review to the appropriate levels of management who can ensure that results are given due consideration.

Internal Audit reports must be accurate, objective, clear, concise, constructive and timely. The final Internal Audit report:

- Includes the agreed upon Internal Audit scope and objectives
- Contains the Internal Audit Function's overall opinion and / or conclusions
- Indicates satisfactory performance or control strengths noted in the audit/review.

During audits, risk management, control and governance issues may be identified. Whenever these issues are significant to the Subject Entity, they should be communicated to Senior Management and the Audit Committee if they are not directly linked to the scope of the Internal Audit assignment.

Reports (whether draft or final) should be issued following a formal protocol communicated to the auditee. Thus, such communication may include the time frame for holding the exit meeting following the conclusion of the fieldwork, the time frame for issuing the draft report following the exit meeting, the time frame for receiving management's replies following the issuance of the draft report, etc.

A summary of the audit results should be entered in the e-Governance Portal and will be displayed in the audit report.

To add a summary of the audit results in the e-Governance Portal, follow the steps below:

1. Click on Audit Plan on the homepage dashboard
2. Click on the name of the audit
3. Click [Edit](#) in the top right corner

Audit - Human Resources Audit					Edit	Return
Analysis Audit Scope Time Review Tasks Findings History Attachments						
Audit Activity					Add	
Records: 14 50 Per Page						
Sort	Phase	Audit Activity			Status	
0001	Planning	Send audit planning letter			4, Request for Manager Review	

4. Enter an overview of the audit results in the section 'Summary of Audit Results'

5. Click [Save](#)

9.2 Prepare the Draft Internal Audit Report

During the planning process, decisions were typically made about:

- the use of ratings for individual findings and/or the report
- the distribution of the report to executive management and to the Audit Committee.

In preparing the draft report, the Internal Audit team should perform the following steps:


- gather and review audit findings for reportable items
- coordinate the comments of the Internal Audit team members
- prioritize issues and/or the report
- Discuss the report with the process owner to validate its contents.

The Internal Audit Function should use a standard report template to record its findings following the performance of an audit. A copy of the standard report template is presented in Appendix 10.

In order to create the draft internal audit report in the e-Governance Portal, please follow these steps.

1. Click Audit Plan on the home page
2. Click on the Audit Name
3. Click on the [Status](#) link for the [Draft IA Report](#) or [Issue Final Report](#) activity




4. Click **Quick Reports**
5. Click **Internal Audit Report**
6. Apply a filter based on the audit name to narrow the data that is collected for the report
7. Click **Execute** to create the report
8. Click **Export**  in the top left corner of the report and select **Microsoft Word (RTF)** from the drop down list to download the report to Word
9. Click **OK** and then **Open** to view the document
10. Edit the Word document if needed

9.3 Review Draft Internal Audit Report

The draft report should be reviewed by the Head of Internal Audit and signed off by the latter as proof of the review. The completion of this process documents the approval of the Head of Internal Audit and reflects that detailed and second-level reviews were completed.

The Audit Report Review Checklist provides the considerations to be taken when preparing and reviewing the draft Internal Audit Report.

In order to complete this checklist in the e-Governance Portal, please complete the following steps:

1. Access the audit you are working on
2. Click on the Audit Activity link **Complete Audit Report Review Checklist**
3. Click **Edit**  to answer the checklist items

Activity

Audit Name

Select and manage suppliers

Name

Complete Audit Report Review Checklist

Number

0003.0001

Description

Complete Audit Report Review Checklist

Work Paper Type

Checklist

Status

* None Selected

Resources

Audit Document Template

Edit

Return

Work Paper

Review

Tasks

Findings

Attachments

History

Checklist Items

Edit

Number of Records: 13

50

Resize

Checklist Item	Response	Comments
01. Is the date on the cover of the report consistent with the date fieldwork was substantially completed or as planned with business unit?	2. Yes	
02. Is the index (if applicable) consistent with the order of the report?	4. Not Applicable	
03. Is the report addressed to the appropriate individual?	2. Yes	
04. Is the subject line of the report consistent with the nature of the report?	2. Yes	
05. Are the appropriate business unit personnel sent a copy of the report and executive summary, including external auditors (compare distribution to organization chart)?	2. Yes	
06. Are the business unit personnel's names spelled correctly?	2. Yes	
07. Are the appropriate individuals sent a copy of the executive summary?	2. Yes	
08. Is the report paginated?	2. Yes	
09. Do items included in the executive summary make sense considering your understanding of the items noted during the project?	2. Yes	
10. Are the recommendations presented in the report reasonably grouped from most important to least important?	2. Yes	
11. Are proper names defined only once in each report and abbreviated thereafter?	2. Yes	
12. Does the cover sheet of each report include the correct name of the business unit audited?	2. Yes	
13. Does the report contain the background, objectives, and scope of the project and our findings and recommendations and/or management action plans?	2. Yes	

9.4 Conduct Formal Closing Meeting

The Internal Audit team should meet with stakeholder personnel and management to discuss the findings identified at the conclusion of the field work and **before** sending the draft Internal Audit Report to obtain alignment with its components. Specifically, the meeting provides an opportunity to:

- Present the findings, discuss their components, and solicit management's action plans with a holistic view of improving the process, initiative, function, and/or activity;
- resolve any misunderstandings;
- demonstrate the benefits of the services the Internal Audit Function has provided;
- agree on follow-up activities, aligned with protocols established in the planning activities.

A key win from holding the exit meeting prior to sending the official Internal Audit draft report is to ensure that all and any findings, information, and analysis are valid and correct. Thus, while management may disagree with a component of a finding (e.g. effect), there should be consensus on the existence and condition of the finding itself. In other words, the Internal Audit Function should ensure that upon issuing the Internal Audit report, its content, source of data, and conclusions reached cannot be challenged for validity.

The Internal Audit team should maintain detailed minutes as evidence of management's response to the issues raised and the report as a whole.

In order to document the minutes of the closing meeting in the e-Governance Portal, perform the following steps:

1. Access the audit you are working on
2. Click on the status link for the activity [Conduct Closing Meeting](#)
3. Click edit to document the details in the work paper

The screenshot displays the 'Activity' section of the e-Governance Portal. It includes a table with the following data:

Field	Value
Audit Name	Select and manage suppliers
Name	Conduct Closing Meeting
Number	0003.0003
Description	Conduct Closing Meeting
Work Paper Type	Meeting and Interview
Status	* None Selected
Resources	Audit Document Template

Below the table are tabs for 'Work Paper', 'Review', 'Tasks', 'Findings', 'Attachments', and 'History'. The 'Work Paper' tab is selected, showing the 'Meeting and Interview Audit Form'. This form includes fields for Name, Purpose, Description, Interviewee, Date, Time, Place, Attendees, and Summary of Interview. The 'Meeting and Interview Attendees' section is also visible, showing a table with columns for Name, Email, First Name, Last Name, Title, NT Account, Phone1, Phone2, and Roles. The table currently shows 0 records.

9.5 Issue Draft Report

After all required report reviews have been completed and following the formal exit meeting with auditee management, the Internal Audit Function should issue the draft Internal Audit Report of detailed findings and recommendations in line with protocols agreed upon with the stakeholder. The distribution of the draft Internal Audit Report is typically limited in nature and may include stakeholder personnel and possibly certain members of management for their replies and action plans.

9.6 Receiving Management Feedback & Action Plans

The feedback from management may vary in substance and/or form. The Internal Audit Function should use professional judgment to decide whether further additional follow-up work and/or meetings are required to address management feedback. If management feedback is not aligned with the recommendations, these recommendations should be further discussed and revised, if possible.

Where concerned management insists on its feedback and/or refuses to develop action plans, the Head of Internal Audit should report this case to the Executive Management, then to Senior Management and finally to the Audit Committee.

9.7 Issue Final Internal Audit Report & Present Results

The Internal Audit Function will issue the final audit report when satisfactory feedback is received. The issuance of the Final Internal Audit Report represents the closure of the Internal Audit assignment.

The Final Internal Audit Report distribution includes Executive and Senior Management, in addition to the Audit Committee.

Refer to the section on creating the draft internal audit report (Section 9.2) for guidance on creating the Final Internal Audit report.

9.8 Internal Audit Reports – Summary & Guidance

Internal Audit reports should include the audit objectives and scope as well as applicable conclusions, recommendations and action plans.

Although the format and content of the audit report may vary by division or type of audit, they should contain, at a minimum, the purpose, scope and results of the audit.

The Internal Audit Function may include background information and summaries. The background information identifies the organizational unit(s) and activity(ies) reviewed and provides relevant explanatory information. It may also include the status of observations, conclusions, and recommendations from prior reports in addition to an indication as to whether the report covers a scheduled audit or is responding to a specific request. Summaries, if included, should be balanced representations of the audit content.

Purpose statements should describe the audit objectives and may, where necessary, inform the reader why the audit was conducted and what it was expected to achieve.

Scope statements should identify the audited activities and include, where appropriate, supportive information such as time period reviewed. Related activities not reviewed should be identified to delineate the boundaries of the audit. The nature and extent of audit work performed also should be described.

Results should include:

- Risk
- Observation
- Action plans
- Due date
- Control rating table.

9.8.1 Observations in Internal Audit Reports

Observations are pertinent statements of fact. Those observations necessary to support Internal Audit conclusions or prevent misunderstandings of those conclusions should be included in the final audit communications. Less significant observations may be communicated informally.

Audit observations emerge by a process of comparing what should be with what is. Where there is a difference, the Internal Audit team has a foundation on which to build the report. However, when conditions meet the criteria, acknowledgment in the audit communications of satisfactory performance may be appropriate.

Observations should be based on:

- **Criteria** - the standards, measures, or expectations used in making an evaluation and/or verification (what should exist);
- **Condition** - the factual evidence that the Internal Audit team found in the course of the examination (what does exist);
- **Cause** - the reason for the difference between the expected and actual conditions (why the difference exists);

Did you know?

Attach final report: attach the final audit report to the work paper "Final Report" to have a complete register of all completed reports in the portal.

- **Effect** - the risk or exposure to the process, function, department and/or the Subject Entity as a whole because the condition is not consistent with the criteria (the impact of the difference).

In determining the degree of risk or exposure, Internal Auditors should consider the effect their audit observations may have on the Subject Entity's operations and financial statements.

Observations may also include management's accomplishments, related issues and supportive information if not included elsewhere.

The following table shows the system for classifying the observations according to their importance in Internal Audit Reports:

Finding Criticality Rating	Definition
<ul style="list-style-type: none"> High 	The finding is critical and deserves immediate attention by the Process Manager. Management's action plan and related corrective action should be implemented as a matter of urgency. The finding is also reported to the Audit Committee at least quarterly.
<ul style="list-style-type: none"> Medium 	The finding impacts the accomplishment of process objectives. Management's action plan and related corrective action should be implemented as a matter of priority. If not resolved, the finding could result in an inefficient use of entity resources and or potentially disrupt business processes.
<ul style="list-style-type: none"> Low 	The finding is reported to the Process Manager but is of a minor risk to the Subject Entity. Management action should be taken to address the weakness within a reasonable agreed time-frame. The finding will not be reported to the Audit Committee unless the finding remains open after the follow up audit.

It should be noted that at this stage, the Internal Audit team is testing and reporting on the operating effectiveness of mitigating controls identified during the Risk Assessment Phase and during the Planning Phase for this review. The table below illustrates the rating system used:

Rating	Definition
<ul style="list-style-type: none"> No Major Concern 	Controls are operating effectively and in accordance with management's control objectives. No control weaknesses were noted.
<ul style="list-style-type: none"> Adequately Controlled 	Certain controls require improvement to ensure that the overall control structure will continue to operate effectively. Few control weaknesses were noted, if any.
<ul style="list-style-type: none"> Inadequately Controlled 	Significant control weaknesses were noted in a number of components or less significant weaknesses exist over the entire control environment.



9.8.2 Conclusions in Internal Audit Reports

Conclusions (opinions) are Internal Auditors' evaluations of the effects of the observations on the activities reviewed. The Internal Audit team should usually put the observations and management action plans in perspective based on their overall implications. Audit conclusions, if included in the report, should be clearly identified as such.

Conclusions may encompass the entire scope of an audit or specific aspects, acknowledgements of satisfactory performance and corrective actions.

9.8.3 Confidential Information in Internal Audit Reports

Certain information may not be appropriate for disclosure to all report recipients because it is privileged, proprietary, or related to improper or illegal acts. Such information may be disclosed in a separate report.

9.8.4 Interim Internal Audit Reports

Interim Internal Audit Reports may be written or verbal and may be transmitted formally or informally. Interim reports may be used either to communicate information that requires immediate attention, to communicate a change in audit scope for the activity under review, or to keep management informed of audit progress when audits extend over a long period. The use of interim reports does not however diminish or eliminate the need for a final report.

Interim Internal Audit Reports may be appropriate for levels of management higher than process management. They may be issued separately from or in conjunction with the final report.

9.8.5 Quality of Audit Reports and Communications

Audit reports and communications should be accurate, objective, clear, concise, constructive, complete and timely.

Accurate communications are free from errors and distortions and are faithful to the underlying facts. The manner in which the data and evidence is gathered, evaluated and summarized for presentation should be done with care and precision.

Objective reports are fair, impartial and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Observations, conclusions and recommendations should be derived and expressed without prejudice, partisanship, personal interests, and the undue influence of others.

Clear reports are easily understood and logical. Clarity can be improved by avoiding unnecessary technical language and providing all significant and relevant information.

Concise reports are to the point and avoid unnecessary elaboration, superfluous detail, redundancy and wordiness. They are created by a persistent practice of revising and editing a statement. The goal is for each thought to be meaningful yet succinct.

Constructive reports are helpful to the stakeholder and the Subject Entity and lead to improvements where needed. The contents and tone of the presentation should be useful, positive, well-meaning and contribute to the objectives of the Subject Entity.

Complete reports lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions.

9.8.6 Errors and Omissions in Audit reports

An error is defined as an unintentional misstatement or omission of significant information.

If it is determined that an Internal Audit Report contained a significant error or omission, the Head of Internal Audit should consider the need to issue an amended report which identifies the information being corrected. The amended audit communication should be distributed to all parties who received the initial audit communication subject to correction.

9.8.7 Legal Considerations in Audit Reports

Internal Auditors are required to gather evidence, make analytical judgments, report their results and ensure corrective action is taken. Internal Auditors should exercise caution when including such results and issuing opinions in Internal Audit Reports, communications and working papers regarding regulatory violations and other related issues. Established policies and procedures regarding the handling of these matters and a close working relationship with other appropriate areas (Legal) are strongly encouraged.

10

Internal Audit Monitoring & Follow-Up

10.1 Introduction

The Head of Internal Audit should develop a mechanism to follow-up with the process owners on the implementation of the action plans and periodically report on the results of the follow-up reviews.

Internal Audit Reports and Management Action Plans are monitored through:

- a time-frame within which management's response to the audit observations is required;
- an evaluation of management's response;
- a verification of the response (if appropriate);
- a follow-up audit (if appropriate);
- a communication procedure that escalates unsatisfactory responses/actions, including the assumption of risk, to the appropriate levels of management;
- the issuance of periodic reports to the Audit Committee on the level of implementation of management's action plans.

Did you know?

Identical Audit: When conducting an audit on a process that has been audited before, create a new audit in the application and bring the same process in scope. In the audit fieldwork, you will see the risks and controls that were identified before, while allowing you to create new tests.

10.2 Timing of Internal Audit Monitoring & Follow-up

Certain reported observations and management action plans may be so significant that they require immediate action by management. These conditions should be continuously monitored by the Internal Audit team until corrected because of the effect they may have.

Did you know?

Archiving: through archiving, you take a snapshot of the risk register at a certain moment in time, and store it in the Portal (read-only). An archived risk register can be accessed from the "History" tab in the risk register.

Archive the risk register(s) in the scope of your audit after completing the audit. This will allow you to change the ratings of the risks and controls in future audits while allowing you to retain visibility in the ratings given in previous audits.

10.3 Internal Audit Monitoring

Techniques used to effectively monitor progress include:

- addressing audit observations and management action plans to the appropriate levels of management responsible for taking corrective action;
- receiving and evaluating management responses to audit observations and management action plans during the audit or within a reasonable time period after the results are communicated;
- receiving periodic updates from management in order to evaluate the status of management's efforts to correct conditions.

Responses are more useful if they include sufficient information to allow an evaluation of the adequacy and timeliness of corrective action. For each of the activities above, the concerned Internal Audit team should prepare the necessary working paper.

10.4 Internal Audit Follow-up

The Internal Audit Follow-Up report should include supporting documentation substantiating the implementation process.

The process and mechanism to document all follow-ups made with management are recorded in the "Implementation Schedule" described below.

10.5 Implementation schedule

Management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations. The Head of Internal Audit is responsible for assessing management actions in terms of their relevance to addressing the impact of the issue(s) and the timely resolution of matters reported as observations and the related recommendations.

The Internal Audit Function should utilise an implementation schedule as a mechanism to establish and monitor the disposition of results communicated to management.

The "Implementation Schedule" is therefore significant in deciding the extent of follow-up and whether additional verification procedures are necessary.

In the event management has decided to assume the risk of not correcting the reported condition because of cost or other considerations, the Head of Internal Audit should inform the Audit Committee of management's decisions on all significant observations.

A copy of the standard Follow-Up Report template is presented in Appendix 11.

11

Internal Audit Management Reporting

This section deals with Internal Audit's role and responsibility for monitoring events or meetings with management and reporting to the stakeholders (Audit Committee, Senior Management, etc.)

Internal Audit reporting to management encompasses an audit follow-up process to monitor whether significant audit concerns for which corrective actions are recommended have been adequately addressed by management.

In addition, the Internal Audit team should maintain a calendar of events that includes key dates for:

- Audit Committee meetings;
- Senior Management / Head of Internal Audit meetings;
- Audit Committee / Head of Internal Audit meetings;
- Senior Management / Abu Dhabi Accountability Authority / Head of Internal Audit meetings;
- Abu Dhabi Accountability Authority / Head of Internal Audit / other Subject Entities Heads of Internal Audit meetings.

11.1 Reports by the Head of Internal Audit

11.1.1 Monthly Reports to Senior Management

The Head of Internal Audit may provide an administrative report and briefing during a monthly meeting with Senior Management.

11.1.2 Quarterly reports to the Audit Committee

The Head of Internal Audit presents at quarterly Audit Committee meetings an overview of the activities of the Internal Audit Function in addition to a detailed status of audits / projects in progress with an update on the status of progress against the Annual Audit Plan and the financial budget.



11.1.3 Internal Audit Function Contribution to Subject Entity's Annual Report

Leading practices encourage Subject Entities to prepare an Annual Report to transparently disclose details of their operations and progress against strategy. Internal Audit Functions normally provide input into the Annual Report disclosing details of the Annual Audit Plan and their progress against the plan, in addition to details of their contribution to risk management and corporate governance initiatives.

The contribution of Internal Audit Functions to the Annual Report generally includes:

- Role of Internal Audit
- Internal Audit Coverage
- Reporting and Consultative Relationships
- Values
- Critical Value Drivers
- Key Strategies for Performance
- Assurance Services
- Achievements
- Professional Staff Qualifications and Expertise
- Future Priorities
- Key Performance Indicators



12

Internal Audit Key Performance Indicators

Leading practices require that indicators used for measuring Internal Audit performance be linked to the Subject Entity's mission and objectives. This will ensure that the Internal Audit Function provides a value added service relevant to the needs of the Subject Entity. Therefore, the Internal Audit Function should develop and implement a system of performance indicators to measure its own performance; such measures should be linked to the audit mission and objectives and should be based on outcomes, not just the measurement of inputs.

KPIs include:

- Service Delivery Benchmarks:
 - The percentage of Internal Audits actually completed as per the original audit plan for the period
 - The number of recommendations implemented as a percentage of the total number of recommendations made in Internal Audit reports, presented both as an accumulated total, for example for the last 2 years, and as a current figure for the period under review
 - The average number of days between the date of the conclusion of the fieldwork and the date of issuing the final internal audit report
- Cost Control Benchmarks:
 - The actual costs of the Internal Audit Function as percentage of the total budgeted costs for the Internal Audit Function for the period
 - The number of direct hours spent on Internal Auditing (excluding hours spent on administrative matters) as a percentage of total hours available
 - Percentage of individual audit projects completed on time and budget

13

Corporate Governance

13.1 Objectives

A key objective of the Internal Audit Function is to provide assurance to the Chairman/ Audit Committee/Board of Directors on the Subject Entity's compliance with leading governance practices and any related regulations (such as Resolution # 13 of 2008 related to Government Departments in Abu Dhabi which was issued by the Chairman of the Executive Council).

The objective of an effective Corporate Governance structure is to create an effective and transparent business environment within the Subject Entity that takes into consideration the interest of the Emirate of Abu Dhabi. Its scope includes both compliance with regulations and procedures and the establishment of a structure that encourages the principles of good governance.

13.2 Approach

As part of its overall risk assessment, the Internal Audit Function should identify the risks of non-compliance with leading governance practices (and the aforementioned resolution where applicable) and the controls and processes established by the Subject Entity to mitigate such risks. This review will include among other items the following:

- Senior Management's responsibilities for the overall performance of the Subject Entity.
- Subject Entity's responsibilities for the execution of its strategic plan.
- Executive Directors' responsibilities for achieving the Subject Entity's objectives.
- Establishment of the various governance committees such as the Executive Committee, Audit Committee, Human Resources Committee and Tendering and Bidding Committee.
- Execution of the above committees of their tasks in line with their approved charters.



14

Quality Assurance

As part of Internal Audit's continuous improvement philosophy, ADAA has undertaken the performance of quality assessments and ongoing monitoring of Internal Audit Functions at Subject Entities. This exercise aims to assist Internal Audit Functions to improve their delivery model, which in turn would reflect on the operations of Subject Entities in terms of a more comprehensive coverage, in addition to providing assurance that the Internal Audit Function is in conformity with the related Standard on Quality Assurance (Attribute Standard 1300).

15

Personnel Development/Training and Performance Reviews

15.1 Staff Profiles/Qualifications

The profiles and qualifications of the employees of the Internal Audit Function should be available to Subject Entity staff.

Note: Internal Audit Functions in many jurisdictions have a dedicated page on their organisations website. This is normally where stakeholders can access the profiles of auditors and other details relating to Internal Audit activities.

15.2 Career Development & Counselling

It is the responsibility of each senior team member to assist in the career development of other team members by leading, mentoring and advising on a professional basis where possible and appropriate.

15.3 Professional Development Requirements

Standard 1230: Continuing Professional Development states the following:

“Internal auditors should enhance their knowledge, skills and other competencies through continuing professional development”.

As part of the Achievement and Personal Development Plan process, the Head of Internal Audit should develop a comprehensive policy governing continuing professional development for Internal Audit personnel including, but not limited to, the required Continuing Professional Education to maintain the certificates held by the employees of the Internal Audit Function.

15.4 Induction Program

Staff joining the Internal Audit Function should attend a formal briefing by the Head of Internal Audit on issues including, but not limited to:

- the Strategic Plan
- the Subject Entity's Code of Conduct
- the Internal Audit Charter
- the Audit Committee
- the Organisational Chart
- the Annual Audit Plan
- Working Hours
- Time Sheets (if applicable)
- Staff Meetings



- Internet
- Gift Policy
- ADAA and External Audit Reports
- Training
- Professional Behaviour
- Professional Development
- Expectations
- Management Style
- Team
- Mentorship
- Types of Audits

15.5 Personnel Performance Review

The employees of the Subject Entity, including Internal Audit staff, should participate in the Performance Review Process. Details of the Performance Review process are obtained from the Internal Audit Function or from the Human Resources Division. All internal audit staff are required to complete an "Achievement and Personal Development Plan" that focuses on the planning and review of individual performance. Quarterly reviews allow consultative discussions between staff and management regarding past performance, planned performance and the identification of any training needs.

16

Audit Administration and Other Matters

16.1 Delegations (Financial & Human Resources)

The Head of Internal Audit, in his capacity as Senior Executive, should be assigned the relevant delegations which relate to the operations of Internal Audit. Therefore expenditures, leaves and any other related activity must be approved by the Head of Internal Audit.

All requests for expenditure, including procurement of consumables, IT software and hardware as well as all Internal Audit related expenditure are to be submitted to the Head of Internal Audit for approval before they are forwarded to the Procurement Division. Leave applications should also be submitted to the Head of Internal Audit for approval before they are forwarded to the Human Resources Division. Wherever possible, requests for leave must be provided in advance.

16.2 File Naming Convention

The purpose of file naming conventions within the Internal Audit Function is to achieve consistency and accuracy in the presentation of files and reports.

A file naming convention should be established by each Subject Entity depending on the document management systems in use. This protocol should be established for the following reasons:

- To prevent replication conflicts
- To manage version control efficiently
- For easy identification of the most recent documents
- To identify the creator or previous editor of a particular document.

16.3 Electronic Communication & Email

The Internal Audit Function should make use of the Subject Entity's electronic memo templates for inter-departmental correspondence.

In general, Internal Audit staff should ensure that emails have a meaningful subject line. Blank subject lines should be avoided. The subject should be an accurate description of the email document or an action statement.

Use of language which is likely to be unfamiliar to the recipient should be avoided.

E-mails should not include material that:

- is inappropriate due to its nature or content;
- may expose the Internal Audit Function and / or the Subject Entity to legal action;



- is subject to copyright or intellectual property rights infringements;
- relates to privileged or confidential information.

Transmission of official e-mails to external parties needs to be undertaken with due care.

A detailed signature and salutation block should be included. Details should include name, title, organizational unit, phone, fax and address. This will add valuable contextual information to the message.

Note: Disclaimer notices are normally added to e-mail messages leaving most organizations. Internal Audit Functions often incorporate an additional disclaimer due to the nature of the work they perform.

17

Internal Audit Manual Update

ADAA is responsible for reviewing this manual on a regular basis - at least once every year - in order to make sure it reflects the better practices applied in the field of internal audit as a profession and the needs of Internal Audit Functions at Subject Entities.





Appendix 1

An Overview of the IT Assurance Methodology



1. Introduction

The purpose of this Appendix is to provide an overview of the IT Assurance Methodology developed by ADAA.

The “IT Assurance Methodology” is designed to identify strengths and weaknesses in current IT policies, delivery methods, skills and knowledge gaps between corporate strategists and IT project managers to provide advice to all management levels on internal control; more important, it is designed to provide assurance to balance risk and control investment in an often unpredictable IT environment.

The goal of the “IT Assurance Methodology” is to have an ideal model of understanding IT assurance controls and the importance of IT assurance controls in a consistent and structured IT environment with auditable interfaces to elements (operational, technical and systems) of an Enterprise Architecture (EA) and EA-related tasks and activities.

2. General IT Assurance Framework

The IT Assurance Framework uses the COBIT Methodology (Control Objectives for Information and related Information Technology – IT Governance Institute) as the base and builds on it by incorporating the three elements of performance (efficiency, integrity and reliability), as well as organizational requirements for transformation (priorities and innovation), as these are critical components of a value adding IT system.

This approach aims to link organizational goals and objectives to IT performance allowing for a systematic evaluation of the “IT Results Chain.” The IT results chain approach provides discipline for aligning performance expectations and measures at all levels. In short, the framework allows providing assurance on:

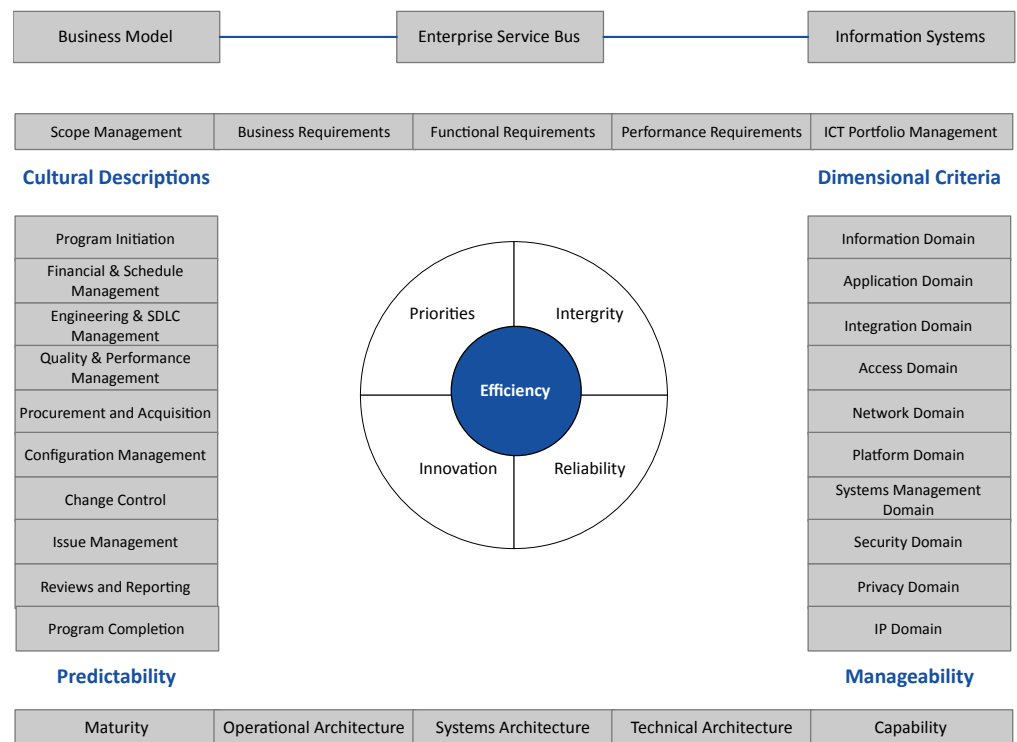
- Information Management
- Information Systems
- Information Technology

3. IT Assurance Model

The IT Assurance Model uses a top-down methodology where it examines the overview controls before evaluating detailed system and application controls. Internal Audit resources are thus targeted and individual test packages are available for each discrete component. This permits testing target components based on the Risk Assessments undertaken in consultation with management and ensuring that high-risk areas are given precedence. The benefit to management is that it allows them to provide an independent assurance on components that are of interest to management.

Further, the component approach permits independent reviewers to provide assurance on the component which is evaluated without auditing the whole system.

To ensure that both the validity of the Risk Assessment and the focus of the Internal Audit activity are directed to critical areas, a global and system level health check is required to be performed as part of the Risk Assessment Phase.



To maximize the results of IT assurance services, the methodology provides tests that IT programs align with and directly support high-level organizational missions, goals and objectives. This approach links organizational goals and objectives with information assets (systems and applications).

4. The IT fieldwork

The IT fieldwork phase comprises 3 additional steps:

Audit - * IT Audit

Edit

Return

Analysis

Audit Scope

Time

Review

Tasks

Findings

History

Attachments

Audit Activity

Add

Records: 19

50

Per Page

Sort	Phase	Audit Activity	Status
<div><div></div><div></div></div> 0001	Planning	<u>Complete Planning Phase:</u>	* None Selected
<div><div></div><div></div></div> 0001.0001	Planning	Complete Planning Checklist	* None Selected
<div><div></div><div></div></div> 0001.0002	Planning	Send audit planning letter	* None Selected
<div><div></div><div></div></div> 0001.0003	Planning	Send detailed scope letter	* None Selected
<div><div></div><div></div></div> 0001.0004	Planning	Conduct Opening Meeting	* None Selected
<div><div></div><div></div></div> 0001.0005	Planning	Develop detailed audit plan	* None Selected
<div><div></div><div></div></div> 0001.0006	Planning	Make advanced information requests	* None Selected
<div><div></div><div></div></div> 0002	Fieldwork	<u>Complete Fieldwork Phase:</u>	* None Selected
<div><div></div><div></div></div> 0002.0001	Fieldwork	Complete Inform. System Assurance Questionnaire	* None Selected
<div><div></div><div></div></div> 0002.0002	Fieldwork	Complete IT Environment Questionnaire	* None Selected
<div><div></div><div></div></div> 0002.0003	Fieldwork	Complete Security over Hardware Checklist	* None Selected
<div><div></div><div></div></div> 0002.0004	Fieldwork	Document Systems and Processes	* None Selected
<div><div></div><div></div></div> 0002.0005	Fieldwork	Perform Fieldwork	* None Selected
<div><div></div><div></div></div> 0003	Reporting	<u>Complete Reporting Phase:</u>	* None Selected
<div><div></div><div></div></div> 0003.0001	Reporting	Complete Audit Report Review Checklist	* None Selected
<div><div></div><div></div></div> 0003.0002	Reporting	Draft IA Report	* None Selected
<div><div></div><div></div></div> 0003.0003	Reporting	Conduct Closing Meeting	* None Selected
<div><div></div><div></div></div> 0003.0004	Reporting	Issue Final Report	* None Selected
<div><div></div><div></div></div> 0004	Quality Assurance	<u>Complete Quality Assurance Checklist</u>	* None Selected

Records: 19

50

Per Page

1. Complete an Information System Assurance Questionnaire
2. Complete an IT Environment Questionnaire

Activity			Edit	Return	
Audit Name	* IT Audit				
Name	Complete IT Environment Questionnaire				
Description	Complete IT Environment Questionnaire				
Status	* None Selected				
Resources	Audit Document Template				
Add Comment					
Recent Comment					

Work Paper	Review	Tasks	Findings	Attachments	History
------------	--------	-------	----------	-------------	---------

CheckList Items			Edit	
Number of Records: 31			50	Resize
CheckList Item	Response	Comments		
1. Does the client have an anti virus system? If yes, answer the following questions:	1. Not Answered			
1.1 Does the anti virus system get updated regularly?	1. Not Answered			
1.2 Does it get updated on all workstations?	1. Not Answered			
1.3 Does the system administrator enforce the anti virus updating process?	1. Not Answered			
2. Does the client have an ongoing IT project? If yes, document in the Portal a list of all ongoing/future projects and ensure that a proper project management methodology is consistently followed	1. Not Answered			
3. Does the client have a quality plan? If yes, check its adequacy.	1. Not Answered			
4. Does the client have a risk assessment framework? If yes, check its adequacy (i.e. identifies critical systems and assesses its impact on the business).	1. Not Answered			
5. Check if the client has service level agreements? If yes, check its adequacy.	1. Not Answered			
6. Check whether the client has a contract with third party to provide IT services? If yes, ensure that this contract is adequately managed.	1. Not Answered			
7. Does the client have operational procedures that cover the IT processes (Planning and organisation,	1. Not			

3. Complete "Security over Hardware" Checklist

Activity		Edit	Return
Audit Name	* IT Audit		
Name	Complete Security over Hardware Checklist		
Description	Complete Security over Hardware Checklist		
Status	* None Selected		
Resources	Audit Document Template		
Add Comment			
Recent Comment			

Work Paper	Review	Tasks	Findings	Attachments	History
<div>Checklist Items</div> <div>1</div> <div> Checklist Item </div> <div> Existence of both automatic and manual fire alarms placed at strategic location Existence of automatic fire extinguisher placed at strategic locations and dispence appropriate suppressant Existence of appropriate types of maual fire extinguishers Existence of control panel shows the place of the alarm Fire extinguishers are marked clearly and can be accessed easily Existence of adequate drainage system Existence of alarms at strategic locations Existence of protective fabric coverage for hardware when it is not in use Hardware is located in raised flooring Existence of voltage regulators and circuit breakers Existence of Uninterruptible Power Supply system (UPS) Existence of dust collection rugs placed at entrances Dust generating activities are carried out away from dust sensitive equipments Existence of security devices at doors to prevent intruders </div> <div>1</div>					





Appendix 2

Audit Committee Charter



Contents

Article 1 Glossary	2
Article 2 Organization	3
Article 3 Purpose	3
Article 4 Composition	6
Article 5 Meetings	6
Article 6 Minutes	6
Article 7 Duties, Authorities & Responsibilities	6





1. Glossary

XXX	XXXX Company
The Committee	The Audit Committee formed by the Board of Directors to oversee audit operations and circumstances
The Charter	The Charter that governs the operation of the Audit Committee
Board of Directors	XXX's Board of Directors
CEO	Chief Executive Officer
HolA	Head of Internal Audit
Internal auditors	Employees of XXX's Internal Audit Function
External auditors	Audit firms who are assigned to provide external or internal audit services
Stakeholders	Every person or entity with an interest in XXX, e.g. shareholders, creditors, staff, and clients
Internal control	Management functions of acting to ensure that objectives are achieved, including effectiveness, economy, efficiency, compliance, policies, procedures, statutory, safeguarding assets, integrity and reliability of management information
Internal Audit Charter	Describes the mission, independence and objectivity, scope and responsibilities, authority, accountability and standards of the Internal Audit Function
IFRS	International Financial Reporting Standards
Governance	The set of regulations, criteria and procedures that ensure institutional discipline in managing XXX with international criteria and practices by determining responsibilities and obligations of the directors and executive management, taking into consideration the protection of shareholders' rights and other stakeholders' interests
Information Technology	Computer-based information systems, particularly software applications and computer hardware applied within XXX
Recovery plans	The process, policies and procedures of restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (incoming, outgoing, toll-free, fax, etc.), workspace, and other business processes after a natural or human-induced disaster
Risk	The uncertainty of an event occurring that could have a negative impact on the achievement of objectives
Fraud	Any illegal acts characterized by deceit, concealment or violation of trust

Conflict of interests	Inconsistency between the interests of an employee of XXX which arises in connection with the performance of his duties
Financial statements	A written report which quantitatively describes the financial health of a company. This includes a statement of comprehensive income and a statement of financial position, a statement of change in equity, and often also includes a cash flow statement
Code of Business Conduct	Set of rules outlining the responsibilities of or proper practices to be applied through XXX's employees
Operational processes	Processes that constitute the core business and create the primary value stream
Risk management	Processes to identify, assess, manage and control potential events or situations, to provide reasonable assurance regarding the achievements of XXX's objectives

2. Organization

This Charter governs the operations of the Committee of XXX.

The Board of Directors will establish the Committee. The Committee shall be guided by this Charter.

3. Purpose

The purpose of the Committee is to:

- Assist the Board of Directors and management in fulfilling their oversight responsibilities to the stakeholders, and others relating to the (1) XXX's financial statements and financial reporting process, (2) the systems of internal accounting and financial controls, (3) the Internal Audit Function, (4) the annual external audit of XXX's financial statements, and (5) the legal compliance including all agreements and the Code of Business Conduct ("CBC"), as established by the management and the Board of Directors
- Prepare an "Audit Committee Annual Report" summarizing the results of its work, its conclusion and recommendations to be issued to the Board of Directors
- Maintain free and open communication between the Committee, internal auditors, external auditors, and management of XXX
- Investigate any matter brought to its attention with full access to all books, records, facilities, and personnel of XXX and with the power to retain outside counsel, or other experts for this purpose



4. Composition

The Committee will consist of at least three and no more than five members who will be appointed by the Board of Directors. The Committee shall include:

- Two members of the Board of Directors
- One independent member

The Committee shall appoint a Secretary who shall be the HoIA at XXX.

Each Committee member shall be independent from XXX's management and shall be financially literate, or shall become financially literate within a reasonable period of time after the appointment of the Committee; at least one member shall have accounting or related financial management and/or business expertise as determined by the Board of Directors.

5. Meetings

The Committee shall meet at least four times each year or more frequently as circumstances dictates. During meetings, the Committee shall discuss such audit matters as the Committee deems appropriate with XXX's internal and the external auditors or any member of management. Meeting agendas will be prepared and provided to members in advance.

6. Minutes

Decisions of the Committee shall be evidenced by resolutions passed at the meeting of the Committee and recorded in the minutes of such meeting or by an instrument in writing signed by all the members of the Committee and such resolution shall constitute authority for appropriate action by management.

A copy of the minutes of each meeting of the Committee or a copy of any instruments in writing evidencing decisions of the Committee shall be transmitted promptly by the secretary of the Committee to each member of the Committee, copied to CEO and to whom the Committee deems appropriate.

7. Duties, Authorities & Responsibilities

The Committee shall understand XXX's structure, controls, and types of transactions in order to adequately assess the significant risks faced by XXX in the current environment, and shall perform the following:

7.1 Financial Statements

- Review significant accounting and reporting issues, including changes in accounting policies, significant adjustments resulting from the audit, complex or unusual transactions and highly judgmental areas, and recent professional and regulatory pronouncements, and understand their impact on the financial statements
- Review with management and the external auditors the results of the audit, including any difficulties encountered
- Review the annual financial statements, and consider whether they are complete, consistent with information known to Committee members, and comply with appropriate accounting principles and standards
- Review with management and the external auditors all matters required to be communicated to the Committee under general accepted auditing standards

7.2 Internal Control

- Consider the effectiveness of XXX's internal control system, including information technology security and control
- Understand the scope of internal and external auditors' review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with management's responses
- Review the adequacy of accounting and business policies, approving and ensuring appropriate application of new policies, and revisions to existing policies, as required
- Ensure the adequacy of the systems of internal control through independent review of operational processes
- Ensuring the existence of an adequate framework for identification and management of risks including facilitation of business risk assessments
- Developing and maintaining an effective risk mitigation strategy including monitoring and supervision of mitigation controls
- Ensuring the existence of an adequate framework that could be reasonably expected to prevent and detect material fraud

7.3 External Audit

- Consider the appointment of the auditors to XXX, their fees, and any questions relating to their resignation or removal and review the extent of non-audit services provided by the auditors in relation to the objectivity and independence needed in the conduct of the audit, and make such recommendations on these matters to the Board of Directors as the Committee sees fit
- Review with XXX's external auditors any audit problems and difficulties and management response, including: (1) any restrictions on the scope of the external auditors activities, (2) any restrictions on the external auditor access to requested materials, (3) any significant disagreements with management, (4) any material



audit differences that the external auditor noted or proposed but for which XXX's financial statements were not adjusted

- Be responsible for the compensation and oversight of the work of the external auditor for the purpose of preparing or issuing an audit report or related work. The external auditor will formally report directly to the Board of Directors
- Evaluate on annual basis the external auditor qualifications, performance and independence
- Have the authority to review all services to be performed by the external auditor. The Committee may delegate this authority to sub-committees consisting of one or more members when appropriate provided that recommendations of such sub-committee presented to the full Committee at its next scheduled meeting

7.4 Internal Audit

- Review with management and the HoIA the internal audit charter, plans, activities, staffing, and organizational structure of the Internal Audit Function
- Review the appointment and replacement of the HoIA and approve the annual internal audit work plan
- Review all reports submitted to the Committee by the HoIA and management's responses to such reports
- Evaluate the performance of the HoIA, or if applicable, the independent public accounting firm, providing internal audit services to XXX

7.5 Compliance

- Review (a) the status of XXX's compliance with applicable laws, regulation and agreements (b) major legislative and regulatory developments which could materially impact XXX, and (c) management's efforts to monitor compliance with the XXX CBC
- Review and investigate any matters pertaining to the integrity of senior management including conflict of interest or adherence to standards of conduct as required by XXX's policy

7.6 Other Duties, Authorities & Responsibilities

- Have Ownership of the process for receipt, retention and treatment of complaints received by XXX regarding accounting, internal accounting controls or auditing matters, and the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters
- Have the authority to retain independent legal, accounting or other advisors. XXX will provide appropriate funding as determined by the Committee, for payment of compensation to any advisors employed by the Committee
- Assess whether XXX has appropriate up to date contingency and recovery plans
- Exercise all the duties, authorities and responsibilities above in respect of all companies or subsidiaries that XXX controls



Appendix 3 Internal Audit Charter



Contents

Article 1 Glossary	4
Article 2 Organization	5
Article 3 Mission	5
Article 4 Scope Of Work	5
Article 5 Authority	6
Article 6 Accountability	7
Article 7 Independence	7
Article 8 Responsibility	7





1. Glossary

XXX	XXX Company
The Committee	The Audit Committee established by the Board of Directors to oversee audit operations and circumstances
Board of Directors	Board of Directors of XXX
Internal auditors	Employees of XXX's Internal Audit Function
External auditors	Audit firms assigned to provide external or internal audit services
Internal audit	Is an independent, objective assurance and consulting activity designed to add value and improve organizations' operations. It helps organizations to evaluate and improve the effectiveness of risk management, control, and governance processes
The Charter	The Internal Audit Charter that describes the mission, independence and objectivity, scope and responsibilities, authority, accountability and standards of the Internal Audit Function
Audit Committee report	A report prepared by the Internal Audit Function which includes a summary of the Function's operations and is submitted to the Audit Committee
Risk based Audit	Risk-based audit is an audit approach that sets materiality thresholds based on audit risk, analysis and develops audit programs that allocate a larger portion of audit resources to high-risk areas
Governance	The set of regulations, criteria and procedures that ensure institutional discipline in managing XXX with international criteria and practices by determining responsibilities and obligations of the directors and executive management, taking into consideration the protection of shareholders' rights and other stakeholders' interests
Internal control	Management's actions to ensure that objectives are achieved, including effectiveness, economy, efficiency, compliance (policies, procedures, statutory), safeguarding of assets, integrity and reliability of management information.
Code of Business Conduct	Set of rules outlining the responsibilities of or proper practices to be applied through XXX by its employees
Operational processes	The operations that constitute XXX's core business

Risk management	Processes to identify, assess, manage and control potential events or situations, to provide reasonable assurance regarding the achievement of XXX's objectives
Risk	The uncertainty of an event occurring that could have a negative impact on the achievement of objectives
Specialized services	Tasks and missions other than audit to be performed by the Internal Audit Function
Independence	The freedom from conditions that threaten objectivity or the appearance of objectivity of the Internal Auditor
Key Performance Indicators	Formally documented and approved measurements of operational and financial performance
Best practices	Those practices that have produced outstanding results in another situation and that could be used by XXX
Fraud	Any illegal acts characterized by deceit, concealment or violation of trust

2. Organization

This Charter governs the activities and operations of the Internal Audit Function of XXX. The Audit Committee will approve the Charter.

3. Mission

- The mission of the Internal Audit Function is to provide independent, objective assurance and consulting services designed to assist XXX in achieving its objectives by striving to provide a positive impact on the efficiency and effectiveness of the operations.
- Internal Audit helps XXX accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal controls, and governance processes.

4. Scope of Work

The scope of work of the Internal Audit Function is to determine whether XXX's systems of risk management, internal controls, and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed
- Interaction with the various governance groups occurs as needed



- Significant financial, managerial, and operating information is accurate, reliable, and timely
- Employees' actions are in compliance with policies, standards, procedures, code of ethics and applicable laws and regulations
- Resources are acquired economically, used efficiently, and adequately protected.
- Programs, plans, and objectives are achieved
- Quality and continuous improvement are fostered in XXX's control process
- Significant legislative or regulatory issues impacting XXX are complied with and addressed appropriately
- Opportunities for improving management control, output, and XXX's image may be identified during audits. They will be communicated to the appropriate level of management

5. Authority

The staff of the Internal Audit Function is authorized to:

- Have unrestricted access to all functions, records, property, and personnel.
- Have full and free access to the Committee
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives
- Obtain the necessary assistance from XXX personnel where they perform audits, as well as other specialized services from within or outside XXX in line with the approved budget

The detailed "Annual Audit Plan" will be approved by the Committee. The "Annual Audit Plan" will include an allocation of time and budget for activities and reviews that may be requested by the Committee.

The "Audit Committee Report" will be presented to the Committee periodically by the Head of Internal Audit.

The Committee reviews the authority, scope of work and resources of the Internal Audit Function on a regular basis to confirm these remain appropriate. Changes to the Charter are to be approved by the Committee.

The staff of the Internal Audit Function shall not:

- Perform any operational duties for XXX or its affiliates
- Initiate or approve accounting transactions external to the Internal Audit Function
- Direct the activities of any XXX employee not employed by the Internal Audit Function, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors

6. Accountability

The Head of Internal Audit, in the discharge of his/her duties, shall be accountable to the Committee to:

- Provide annually an assessment on the adequacy and effectiveness of XXX's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work
- Report significant issues related to the processes for controlling the activities of XXX and its affiliates, including potential improvements to those processes, and provide information concerning such issues through resolution
- Periodically provide information on the status and results of the "Annual Audit Plan" and the sufficiency of resources
- Coordinate with and provide oversight of other control and monitoring functions (risk management, compliance, security, legal, ethics, environmental, external audit and Code of Business Conduct)

7. Independence

To provide for the independence of the Internal Audit Function, its personnel shall report to the Committee and in a manner outlined in the above section on accountability. Thus, the Head of Internal Audit will report administratively to the CEO/GM/Chairman and functionally to the Audit Committee.

8. Responsibility

The Head of Internal Audit has the responsibility to:

- Develop a flexible "Annual Audit Plan" using an appropriate risk-based methodology, including any risks or control concerns identified by management, and submit that plan to the Committee for review and approval as well as quarterly updates
- Implement the "Annual Audit Plan", as approved, including as appropriate any special tasks or projects requested by the Committee
- Maintain a professional audit staff with sufficient knowledge, skills, experience, and professional certifications or outsource the needed skills and capabilities to meet the requirements of this Charter
- Evaluate and assess significant merging/consolidating functions and new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion
- Issue "Internal Audit Reports" to management at the conclusion of each audit after



full discussion with the management of the area audited. The report will be copied to the Committee. The report will include the following:

- Scope and objectives
- Description of the audit process
- Summary of results
- Assessments of each individual risk / control
- Detailed observations / process enhancements
- Management action plans along with due dates for implementation
- Definitions of risks / controls ratings
- Issue “Follow-up Audit Reports” to the Committee on a semi-annual basis on outstanding management action plans
- Develop Key Performance Indicators (KPIs) for the Internal Audit Function and report these to the Committee quarterly
- Keep the Committee informed of emerging trends and best practices in internal auditing
- Assist in the investigation of significant suspected fraudulent activities within XXX and notify management and the Committee of the results.
- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to XXX at a reasonable overall cost



Appendix 4 Job Descriptions



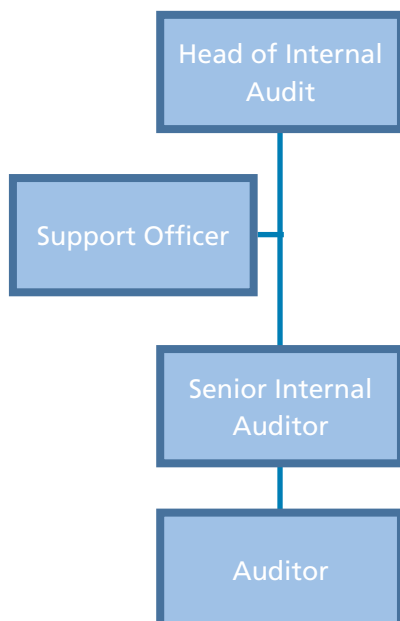
Job Title: Head of Internal Audit
Reports to: Audit Committee
Division:
Department: Internal Audit
Section:
Location: Abu Dhabi
Position No.:
Grade:

1. Job Summary Scope

The role of the Head of Internal Audit is to direct a comprehensive program of Internal Audit for the Subject Entity to ensure that internal control systems for reliability and integrity of financial, operational and information technology are reviewed at appropriate intervals and effective recommendations are made for corrective actions as required.

Additionally, the role of the Head of Internal Audit is to develop, update and implement the Internal Audit Function Charter in accordance with the Standards from the Institute of Internal Auditors (IIA).

2. Organisation Chart



3. Principal Responsibilities

Internal Audit Charter

- Develop, implement and maintain the Internal Audit Charter and champion the Internal Audit Function throughout the Subject Entity

Strategic Audit Plan

- Develop the strategic audit plan for 3 to 5 years. This will define the audit assignments to be done on a yearly basis.
- Submit the Strategic Audit Plan to the Audit Committee for approval.
- Review the Strategic Audit Plan at the beginning of each year to reconfirm the status and nature of risks, and to validate whether changes to the systems have affected the risk assessment results
- Obtain the Audit Committee approval on the changes to the Strategic Audit Plan

Annual Audit Plan (AAP)

- Develop and present the AAP for the year. This includes operational audits, performance audits, compliance audits, financial audits and information technology audits.
- Monitor the implementation of the AAP and suggest changes to the plan when required and approve the changes accordingly
- Develop and present the risk assessment table for the Subject Entity

Audit Team Management & Development

- Lead the preparation of financial and manpower budgets of the Internal Audit Function for the year
- Coordinate the Internal Audit recruitment process
- Prepare, update and maintain the Internal Audit Manual
- Ensure Internal Audit teams comply with the Internal Audit Charter and follow the procedures listed in the Internal Audit Manual
- Support proper professional development for Internal Audit staff, including proper training, counselling and implementation of a transparent appraisal system.
- Agree with staff on the set targets and the professional development plan for measuring performance
- Provide the technical expertise on any related assigned duties, and have responsibility for the update of the knowledge base and skills required for the execution of the Internal Audit assignments
- Allocate the assignments under the AAP to seniors

Audit Committee reporting

- Obtain approval for the AAP from the Audit Committee
- Present the Internal Audit findings to the Chairman and to the Audit Committee on a quarterly basis
- Submit the Annual Report recapping the performance of the Internal Audit Function during the year

External Liaison

- Coordinate with the Statutory Auditors and the Abu Dhabi Accountability Authority (ADAA).

Special Projects

- Plan the execution of special investigations requested by the Audit Committee

Follow - up Reports

- Plan follow-up assignments for audits completed during the year. This will include the follow-up on the implementation of the actions agreed with the management based on the recommendations raised
- Report to the Audit Committee the status of the follow-ups

4. Audit Planning

Co-develop the Expectation

- Meet with the Internal Audit team and set the expectation for the audit assignment as per the AAP
- Co-develop the risk assessment with the team and client and communicate risks to the Audit Committee
- Agree the communication protocol with the team and the Auditee management and identify the Internal Audit Liaison within the Auditee Function

Planning Meetings

- Attend the opening planning meetings with the Auditee management and obtain commitment to the audit assignment
- Review and approve the minutes of audit planning meetings prepared by the Senior Auditor

Resources Planning

- Identify and ensure the availability of the resources required and the special skills needed to execute the specific audit plan. This is dependent on the nature and complexity of the audit assignment

- Review and approve the allocation of the resources available to each phase of the audit assignment and the internal timetable schedule and budget for completing the audit assignment.
- Identify if external resources are required to execute the audit assignment.

Understanding the Business & Testing Strategy

- Review and sign off the documentation prepared for understanding the business of the Department / Section / Function under review
- Review and sign off the understanding of the business process to be audited
- Review and approve the risks identified, nature, impact and likelihood on the Department / Section / Function under review and the controls identified to mitigate those risks
- Review and approve the audit plan to address the risks identified along with the testing strategy
- Review and agree the degree of testing to achieve the objectives of the audit assignment and the related nature and extent of testing (substantive testing vs detailed analytical review)
- Review and approve the detailed scope letter to be communicated to the Head of the Department / Section / Function under review
- Agree on use of computer software that aide in performing tests (Audit Command Language (ACL))
- Review and approve the internal audit program developed by the senior auditor. This includes the sampling techniques to be used

5. Audit Execution

Post Planning Event

- Meet the audit team and discuss the internal audit plan for the audit assignment to ensure resources are allocated, original risk assessment and testing strategy are properly developed based on the information provided during the planning phase

Working Papers File Review

- Review the testing of internal controls identified during the planning phase. Agree with the conclusion on the internal controls design effectiveness.
- Monitor the execution of the internal audit plan through conducting regular meetings with the audit team
- Perform on the job review of the working papers as and when an audit section is completed and reviewed by the senior auditor



- Review the issues raised and the management response and agree if the issue is to be included or excluded from the final report and the reasons why.
- Review and sign off key working papers (to be identified, ie Planning Documents, Risk Assessment and the extent of testing, Final Report).

6. Audit Reporting

Review

- Review the internal audit report and ensure that issues raised and documented in the working paper file are properly excluded or included in the report
- Review the changes to the internal audit report. This continues to evolve and change over the course of the audit as new information and new perspectives are revealed
- Review the wording of the report to avoid any use of inappropriate language
- Review the proper rating and prioritization of the points raised

Report & Attending Closing Meetings

- Issue the draft report for the Head of the Department / Section / Function under review and comments
- Review of the management comments obtained and typed in the report
- Attend the closing meeting with the Head of the Department / Section / Function under review to discuss the issues raised, recommendations suggested and management responses
- Issue the final report to the Audit Committee along with a copy to the Chairman BOD and prepare to present the findings to the Audit Committee when requested
- Plan for a follow up assignments to confirm implementation of the corrective actions agreed in the final report

7. Supervision Of Staff

- Ensure that the team assigned possess the requisite knowledge, skills and other competencies required to complete the audit assignment
- Provide appropriate instructions and guidelines during the execution of the audit assignment to achieve the audit objectives

8. Professional Conduct & Development

Training & Counselling

- Develop and approve a training program for internal audit staff
- Ensure that internal audit staff enrolled in the training program
- Conduct regular counselling sessions with the employees and provide regular feedback about the performance and how to improve on the area of weaknesses
- Ensure proper induction and training for newly recruited staff before starting any audit assignment
- Ensure that all internal audit staff sign the Government code of conduct

Professional Development & Appraisals

- Participate in details in producing a professional development plan for each employee. This will include the professional certification to be obtained which is relevant to the assignments done
- Review and sign off the completed staff appraisal for each audit assignment and discuss it with the staff and agree on development measures



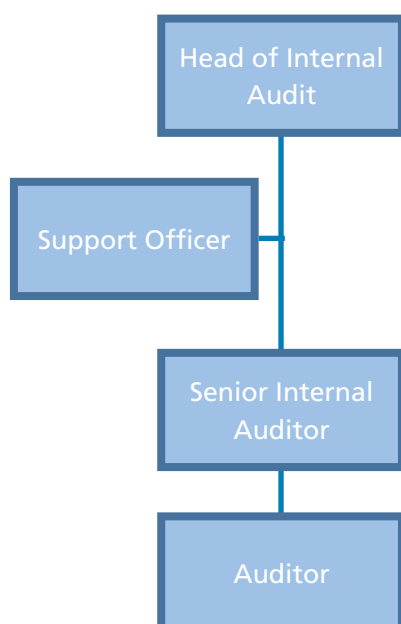
Job Title: Internal Audit Senior
Reports to: Head of Internal Audit
Division:
Department: Internal Audit
Section:
Location: Abu Dhabi
Position No.:
Grade:

1. Job Summary Scope

The role of the Senior Auditor is to plan, supervise and oversee the various audit activities being carried out by assigned Auditors. The Senior Auditor identifies and evaluates risks associated with the Department's processes and prepares audit plans, including audit programs and budgets. The Senior Auditor performs detailed reviews of the working papers and drafts the internal audit report.

The Senior Auditor establishes goals, performance standards and objectives for self and other subordinates. He ensures that duties are being carried efficiently and professionally and in accordance with the Internal Audit Manual and the International Internal Audit Standards. He performs ad hoc duties as and when requested by the Audit Manager.

2. Organisation Chart



3. Principal Responsibilities

Internal Audit Charter:

- Implement Internal Audit Charter

Strategic Audit plan:

- Participate in the development of the strategic audit plan for the 3 to 5 years. This will define the audit assignments to be done on yearly basis
- Participate in the review of the Strategic Audit Plan at the beginning of each year to reconfirm the risks remain the same and that there have been no changes in the systems that might affect the risk assessment

Annual Operational Audit Plan (AAP):

- Participate in the development of the AAP for financial, operational, compliance, performance and information technology, detailing assignments, timeframes and resources required and submit to the Head of Internal Audit for review and approval
- Identify significant process, develop audit objectives and prepare the risk assessment process for each audit assignment and present to the Head of Internal Audit for review and approval

Audit Team Management & Development:

- Participate in the internal audit staff recruitment process
- Participate in the development of proper professional development for subordinate and monitor the performance of subordinates
- Participate in setting individual staff targets and a professional development plan for measuring performance
- Allocate the assignments under the internal audit plan to respective auditors and staff
- Prepare the budget for each audit assignment and present it to the Head of Internal Audit for review and approval
- Provide the technical expertise on any related assigned duties responsible for updating knowledge base and skills required for the execution of the internal audit assignments on regular basis

Special Projects:

- Execute special investigation requested by the Chairman / BOD or the Audit Committee as directed by the Head of Internal Audit

Reporting to the Head of Internal Audit:

- Present the findings of the internal audit assignment to the Head of Internal Audit.
- Provide regular feedback to the Head of Internal Audit for the status of each audit assignment
- Conduct follow up assignments and report to the Head of Internal Audit the findings on the status of implementation of the recommendations raised in the final report

4. Audit Planning

Co-develop the Expectation:

- Plan and arrange the internal audit team planning meeting, and agree with the Audit Manager the audit approach setting the expectations for the audit assignment as per the Internal Audit Plan
- Plan and attend the opening planning meetings with the Head of the Department / Section / Function under review and obtain his / her commitment to the audit assignment
- Prepare the minutes of audit planning meetings

Risk Assessment & Testing Strategy:

- Prepare the preliminary risk assessment and discuss it with the team
- Prepare the testing strategy for the degree of testing to achieve the objectives of audit assignment and the related nature and extent of testing (substantive testing vs detailed analytical review)
- Prepare the detailed scope letter to be communicated to the Head of the Department / Section / Function under review
- Plan and direct the use of computer software that aide in performing tests (Audit Command Language (ACL))
- After completing the planning of the audit assignments, prepare a detailed risks identified, nature, impact and likelihood on the Head of the Department / Section / Function under review and the controls identified that mitigate those risks and update the audit plan and the testing strategy if required
- Prepare the internal audit program including the sampling techniques to be used

Audit Team Management & Development:

- Plan the resources required and the special skills needed to execute the specific audit plan. This is dependent on the nature and complexity of the audit assignment
- Prepare the allocation of the resources available to each phase of the audit assignment and the internal timetable schedule and budget for completing the audit assignment and submit to the Head of Internal Audit for his review and approval

Establishing of Communication Protocol:

- Agree the communication protocol with the Head of Internal Audit and the Head of the Department / Section / Function under review and identify the Internal Audit Liaison within the Department / Section / Function under review

5. Audit Execution

Post Planning Event:

- Agree the final risk assessment with the Head of Internal Audit and the Head of the Department / Section / Function under review
- Revisit the internal audit plan for the audit assignment to ensure proper resources are allocated, original risk assessment and testing strategy are properly developed based on the information provided during the planning phase
- Ensure that sufficient testing is done for the internal controls identified during the planning phase. Confirm the conclusion on the internal controls design effectiveness

Audit Team Management & Development:

- Supervise the execution of the internal audit plan through daily visits and discussion with the audit team

Working Papers File Review:

- Ensure that sufficient documentation is complete and filed in order to understand the business of the Department / Section / Function under review
- Ensure that sufficient documentation is complete and filed in order to understand of the business process to be audited
- Perform on the job detailed review of the working papers as and when an audit section is completed
- Perform the detailed review and confirmation of the issues raised and the management response and recommend if the issue is to be included or excluded from the final report and the reasons why
- Review and sign off the working papers

6. Audit Reporting

Reporting:

- Prepare the draft internal audit report and ensure that issues raised and documented in the working paper file are properly excluded or included in the report
- Identify gaps between actual and expected performance. While all differences are noted, only significant differences are identified in the reporting phase



- Ensure the proper wording of the report to avoid any use of inappropriate language.
- Prepare the rating and prioritization of the points raised
- Obtain and document the management comments in the report
- Closing Meetings and Final Report:
 - Attend the closing meeting with the Head of the Department / Section / Function under review to discuss the issues raised and recommendations suggested
 - Prepare issuance of the final report to the Head of the Department / Section / Function under review of Internal Audit

Follow up assignments:

- Conduct follow up assignments with the Head of the Department / Section / Function under review to ensure proper implementation of the corrective actions agreed in the report

7. Supervision Of Staff

- Review the work allocation to ensure that the team assigned possess the requisite knowledge, skills and other competencies required to complete the audit assignment
- Provide appropriate instructions and guidelines during the execution of the audit assignment to achieve the audit objectives
- Resolves issues with the Department / Section / Function under review under audit

8. Professional Conduct & Development

Training and Counselling:

- Participate in the development of a training program for internal audit staff
- Ensure proper on job training is given to the staff

Professional Development & Appraisals:

- Participate in the development of a professional development plan for subordinate
- Submit regular feedback to the Audit Manager regarding the performance of his subordinate and how to improve on the area of weaknesses

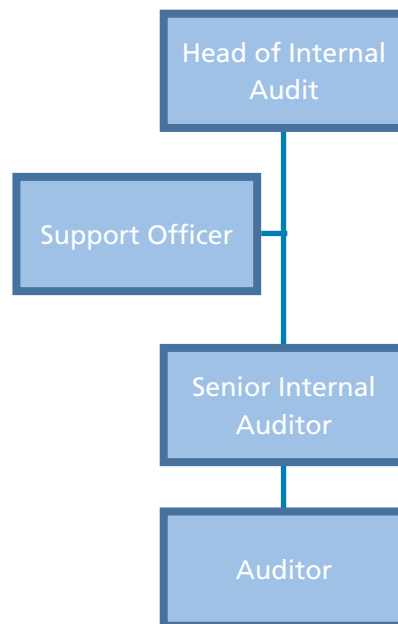
Complete the staff appraisal for each audit assignment and discuss it with the staff and agree on development measures.

Job Title: Auditor
Reports to: Internal Audit Senior
Division:
Department: Internal Audit
Section:
Location: Abu Dhabi
Position No.:
Grade:

1. Job Summary Scope

- The role of the Auditor is to conduct internal audit assignments in line with the approved Internal Audit work program.

2. Organisation Chart





3. Principal Responsibilities

Audit Assignment:

- Provide regular feedback to the Senior Auditor on the status of audit assignments

Special Projects:

- Participate in special assignments directed

4. Audit Planning

Co-develop the Expectation:

- Attend the Internal Audit team planning meetings
- Attend the opening planning meetings with the Head of the Department / Section / Function under review

Risk Assessment & Testing Strategy:

- Participate in the risk assessment process
- Participate in the preparation of the detailed risk register(s) including the nature, impact and likelihood on the Department / Section / Function under review and the controls identified that mitigate those risks
- Participate in the preparation of the detailed internal audit work program to address the risks identified along with the testing strategy

5. Audit Execution

Implementation of Testing Strategy:

- Implement the testing strategy to achieve the objectives of audit assignment
- Perform testing of internal controls identified during the planning phase to the extent documented in the risk assessment. Conclude on the internal controls effectiveness
- Use computer software that aids in performing analytical tests (CAATS)

Working Papers File & Information Gathered:

- Identify sufficient, factual, reliable, relevant and useful information to support test results
- Document the work done during the understanding of the business of the Department / Section / Function under review
- Document and confirm the issues raised and the management response
- Sign off all the working papers

6. Audit Reporting

Audit Report:

- Prepare the Internal Audit Control exception sheet
- Participate in the drafting of the Internal Audit report

Closing Meetings:

- Attend the closing meeting with the Head of the Department / Section / Function under review to discuss the issues raised and the proposed recommendations

Follow up Assignments:

- Participate in conducting the follow up assignments to ensure the proper implementation of the corrective actions agreed in the report

7. Supervision Of Staff

- None

8. Professional Conduct & Development

Training and Counselling:

- Follow up on the individual training program and ensure registration to the communicated training courses

Professional Development & Appraisals:

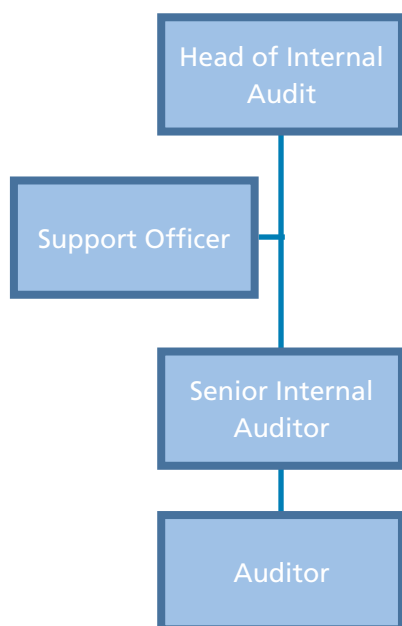
- Prepare the individual professional development plan
- Obtain regular feedback from the Senior Auditor regarding his / her performance and how to improve
- Initiate the staff appraisal following each audit assignment and discuss it with the Senior Auditor and agree on development measures

Job Title: Support Officer
Reports to: Head of Internal Audit
Division:
Department: Internal Audit
Section:
Location: Abu Dhabi
Position No.:
Grade:

1. Job Summary Scope

- The role of the Support Officer is to provide administrative support to the Internal Audit Function. The Support Officer will act as the central point for coordination of Internal Audit activities.

2. Organisation Chart



3. Principal Responsibilities

Administrative Matters:

- Coordinate and manage the Head of Internal Audit's calendars, appointments and meetings
- Make travel arrangements for Internal Audit staff
- Open and direct distribution of incoming mail to Internal Audit staff
- Compose letters and memos as directed by the Head of Internal Audit

Office Matters:

- Communicate with the Abu Dhabi Accountability Authority, independent consultants and other external vendors as directed by the Head of Internal Audit
- Monitor, order and maintain the office supplies inventory
- Track Internal Audit Function correspondence, noting due dates for action and follow up as required
- Edit draft and final audit reports as requested by the Head of Internal Audit and / or Senior Auditors
- Provide backup support to other administrative support staff as needed (vacation, illness, work overflow)

Audit Matters:

- Facilitate the Internal Audit team's communication through the effective use of conference calls, e-mails, audit team meetings and other communication means
- Act as a point of contact (though not the primary one) for the Internal Audit Function in order to assist with coordination of engagements, meetings and events
- Prepare the "Auditee Satisfaction" questionnaires and ensure that they are sent out the Heads of the Departments / Sections / Functions reviewed after audits are completed, then collate and communicate the results to the Head of Internal Audit
- Conduct research for information relevant to the audit assignments as directed by the Internal Audit team
- Update the key auditee personnel contacts databases
- Assist in preparation of presentations for the Head of Internal Audit
- Prepare and / or maintain reports and analyses as directed by the Head of Internal Audit



4. Professional Conduct & Development

- Prepare the individual professional development plan
- Initiate the staff appraisal process and discuss it with the Head of Internal Audit and agree on development measures

5. Personal Qualities

- Professional, confident and outgoing
- Top tier interpersonal skills – able to influence at all levels combining diplomacy with a firm manner
- Ability to function as part of a team
- Organized and self-disciplined
- Calm and capable – able to juggle conflicting demands on time and priorities effectively
- Excellent communication skills in Arabic and English both written and verbal



Appendix 5 Gap Analysis Report

Gap Analysis Report

Reporting Entity	Organization	Process	Risk	Inherent Risk Rating	Risk Rating Rationalization	Design Adequacy	Control Rating Comment	Residual Risk Rating (Risk Assessment)
Abu Dhabi	ABC Company	Accounts Payable	Cash may be disbursed for goods and services never received or in advance of receipt.	Extreme Risk	Donec placerat massa non nisi. Aliquam erat volutpat. Maecenas purus erat, mollis vitae, auctor vitae	Inadequate	No controls in place to mitigate this risk	Active Management
			Payable and related accounts may be misstated because of incorrect adjustments or incorrect reclassifications of distributed amounts.	Extreme Risk	Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat	Inadequate	No preventative controls to mollis at, sem. Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare	Active Management
			Short pays are resolved in favor of the supplier even though goods may not have been received	Significant Risk	Nunc vulputate sapien vitae augue. Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem	Inadequate	Additional controls sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque	Active Management
			Unintentional or deliberate errors on supplier invoices	Significant Risk	Maecenas purus erat, mollis vitae, auctor vitae, mollis at, sem.	Inadequate	Donec placerat massa non nisi. Aliquam erat volutpat. Maecenas purus erat, mollis vitae, auctor vitae, mollis at, sem	Active Management



Appendix 6 Internal Audit Plan



Introduction	4
Approach	4
Risk & Audit Universe	4
Basis of Selection	4
Budget & Resource Allocation	4
Internal Audit Plan	4
Project Timing	5
Appendix 1	6
Appendix 2	6



1. Introduction

The Entity Name Strategic Internal Audit Plan for (time period) (“the Plan”) relates to the provision of Internal Audit activities for the period (time period).

This document outlines the approach employed by the Internal Audit Function to develop the Plan for (year) and indicative projects for (year). The (year) projects will be agreed in early (year).

Add as you see fit.

2. Approach

The approach taken to develop the Plan for (year) is demonstrated in the diagram below / or as follows:

3. Risk & Audit Universe

4. Basis of Selection

Explain the strategy and the methodology used for the identification and selection of audit projects for the (year) and what would be the benefits derived from such audits i.e. value.

5. Budget & Resource Allocation

6. Internal Audit Plan – (insert year(s))

The table below outlines the Internal Audit projects proposed to be included in the Plan for (year) and anticipated projects for (year). An estimated number of days required to complete the fieldwork is also provided. A brief description of each Internal Audit project is provided in Appendix 1. The exact scope of each project will be agreed with management and documented in detail prior to commencement of our fieldwork.

Projects for (year) will be revised and agreed in early (year) to ensure continuing relevance within Entity Name changing risk environment.

[illegible]

Appendix 1: Project Descriptions

No.	Project Title	Est. Days	Year/s
1.	(insert project description)	#	(year)
2.	(insert project description)	#	(year)
3.	(insert project description)	#	(year)
4.	(insert project description)	#	(year)
5.	(insert project description)	#	(year)
6.	(insert project description)	#	(year)
7.	(insert project description)	#	(year)

Appendix 2: Personnel Consulted

We would like to extend our appreciation to the following individuals who participated and provided information during this Internal Audit planning exercise

[illegible]



Appendix 7

Audit Planning Letter Template



Date

To: *(Insert Name—Unit/Division Head)*

From: *(Head of Internal Audit)*

Internal Audit Review

In line with *(Subject Entity)'s (period)* Internal Audit plan (approved by the Audit Committee), we have scheduled Internal Audit procedures related to *(name(s) of process(es))* at *(Function's location)*.

This review is scheduled to commence during the week of *(date)*. *(name of Internal Auditor)*, a member of the Internal Audit team will contact you directly to set up a time to agree the scope of the project.

If you have any questions or concerns, please contact *(first name of Internal Auditor)* at *(phone number)*.

It is vital that you work closely with Internal Audit to identify risks and opportunities inherent in the process(es) being reviewed. Our goal is to ultimately identify areas where internal control improvement and efficiencies can be realized. We recommend that you be closely involved in the Internal Audit process to ensure that issues are resolved on a timely basis.

Signed

Head of Internal Audit

cc: *(Executive sponsors i.e. CEO, etc.....)*



Appendix 8 Data Request Form



Date: (date)

To: (business unit name)

From: (your name)

Subject: Request for Electronic Data File

As part of our (Date [annual, quarterly etc.]) procedures at (business unit name), we would like to obtain the following information in an electronic format in order to perform procedures in the area of (name the area, e.g., Payroll, AP).

The information we are requesting is found in (report or file name), and we have enclosed a copy of the file format with this request. We will need the data to cover the period/or as of (date), and the control totals for this data should agree to (state amount, if known). The fields needed are listed at the end of this letter.

Summary of Our Processing Capabilities

- We can receive the file in ASCII or EBCDIC on Zip Disk, CD, or via email.
- If possible or applicable, we would like the data file requested to be in dBase format (*.dbf). If this is not possible, we can also process the following data types:
 - Text (*.csv, *.txt)
 - Excel (*.xlsx)
 - Lotus (*.wks)
 - MS DataBase (*.mdb)
 - ASCII (*.asc)
 - EBCDIC (including packed and binary fields)
 - Data Interchange File (*.dif)
 - Print Image File (*.prn, *.rpt., *.dat)

In summary, we need you to assist us as follows:

- We would like to receive the data described above by (request date) so we may complete our procedures in a timely and efficient manner.
- Complete and return with the data file(s), the documentation which includes the data file layout, record and block length specifications, and record count and control totals.

If you have any questions or concerns regarding this request, please contact me at (phone number). Thank you for your assistance with this matter, and I will contact you shortly to ensure that you are not having any problems with this request.

Please provide the following information for each data file:

Business unit Name: Audit No.: Audit Title:	Ref.: Prepared By: Date : Reviewed By: Date :
---	---

Field Names	Starting Position	Length	Data Type N-Numeric; C-Character	Decimal Positions
Field1	1	10	C	
Field 2	11	6	N	2

Total Record Count	
Control Totals (With Source)	
Record Length in Bytes	
Block Length in Bytes	





Appendix 9

Detailed Scope Letter Template



(Date)

(name of process owner (i.e. Division Head))
(title)

Dear *(name of process owner (Division Head))*:

This letter is to confirm our plans to conduct the audit procedures beginning on *(Start Date)* and ending on *(End Date)* and to provide you with an overview of our objectives, scope, nature of our work, communication protocols and the team members for the project. We are excited about the opportunity to work with you and your staff and look forward to getting started.

Objectives and Scope

The objectives of our audit are to:

- Gain an understanding of your significant business processes
- Perform a risk assessment within the processes
- Identify and evaluate controls over these risks
- Test controls over the most significant risks
- Agree action plans to improve control effectiveness and, where appropriate, to improve process performance

The process understanding, risks and controls will be developed with respect to the *(Detail Internal Audit Focus)* as agreed with *(Name or Group from Planning activities)*.

The scope of the audit project will include the following business processes:

- Detail specific major processes and associated sub-processes included in the audit
- ...

If appropriate, detail any processes or areas specifically excluded from the audit scope.

Nature of Our Work

Our audit process is highly dependent on co-developing each element of our audit (process understanding, risk assessment, control evaluation) with respective process owners. This is achieved through interviews to both develop and confirm each element of the audit.

Communications and Reports

In order to ensure a mutual understanding and agreement on each finding identified, we will hold an exit meeting following the completion of the field work.

The closing meeting will serve as an opportunity to finalize any management action plans required to address Internal Audit findings, and discuss any additional issues or concerns related to the current and future audits.

Key Contacts

The Audit team will be led by [Name] who will be assisted by [Names]. If you have any questions or comments, please do not hesitate to contact [Audit Team leader] at [phone number] or myself at [phone number].

Signed
Head of Internal Audit





Appendix 10

Internal Audit Report Template

Internal Audit Report

Accounts Payable Audit

CONFIDENTIAL

TABLE OF CONTENTS

Scope and Objectives

Audit Process

Summary of Results

Detailed Results

Appendix 1 - Definitions of Control ratings and Finding Criticality

Entity Logo/ Name

Scope and Objectives

The scope is the accounts payable process in the Abu Dhabi branch of ABC Company. The objectives are to ensure that the risks in the accounts payable process are mitigated by the controls in place. All adequately designed controls are in scope for this audit.

Audit Process

We have assessed the specific risks identified within each area of scope, evaluated the associated mitigating controls, and commented on the results of our audit procedures. The Risk, Observation/Process Enhancement and Management Action columns on the following pages are intended to improve existing controls over risks and to improve the efficiency of current operating procedures.

The period under review was primarily from [date] to [date]. See Appendix 1 for definitions of control ratings.

This report is intended solely for the information and use of management of (the Department) only and is not to be used or relied upon by others for any purpose.

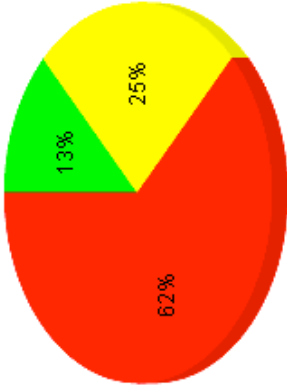
Date: 4/12/2010

Summary of Results:

Curabitur nonummy velit. Nullam a dolor vehicula lectus volutpat convallis. Sed imperdiet, dui at rutrum molestie, mauris libero tincidunt quam, et scelerisque enim neque vitae est. Nullam non quam quis urna consectetuer elementum. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.

Cras volutpat lacinia lacus. Ut viverra tincidunt dolor. Quisque vel sapien vel nisi tempus vestibulum. Fusce placerat odio et felis eleifend ullamcorper. Etiam rhoncus dictum diam. Aliquam erat volutpat. Vivamus dolor. Nam fermentum metus in ante.

Operating Effectiveness



1 Risks were assessed as *Well Controlled*
2 Risks were assessed as *Adequately Controlled*
4 Risks were assessed as *Inadequately Controlled*

Set of Control Rating	Definition
<div>●</div> Well Controlled	Controls are operating effectively and in accordance with management’s control objectives. No control weaknesses were noted.
<div>●</div> Adequately Controlled	Certain controls require improvement to ensure that the overall control structure will continue to operate effectively. Few control weaknesses were noted, if any.
<div>●</div> Inadequately Controlled	Significant control weaknesses were noted in a number of components or less significant weaknesses exist over the entire control environment.

We note below the findings related to areas in scope of this audit.

Accounts Payable

High

- Duplicate Payments
- Unauthorized access to payment file
- Detail activity may be incorrectly posted in the subsidiary ledger

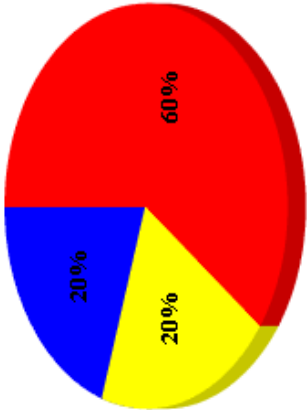
Medium

- Fraudulent payments detected

Low

- Errors on supplier invoices

% of Findings by Rating



Finding Rating	Definition
High	Finding is serious and deserves immediate attention by the Process Manager. The finding is reported to the Audit Committee quarterly.
Medium	Finding impacts the accomplishment of the Process objectives. Corrective action is required by management. If not resolved, finding could result in inefficient use of entity resources and or potentially disrupt business processes.
Low	Finding to be reported to Management but is of a minor risk to the entity. Findings will not be reported to the Audit Committee unless the finding remains open after the follow up audit.

Entity Logo/ Name

Finding Name (Criticality)	Risk (Operating Effectiveness)	Observation/Process Enhancements	Recommendation	Due Date Remediation Plan
<div> <div></div> <div>High</div> </div> <p>Duplicate Payments</p>	<p>● Inadequately Controlled</p> <p>Vendors are added as approved vendors without proper research and authorization</p>	<p>We noted that Pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue. Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat.</p> <p>Vendors are added as approved vendors without proper research and authorization</p>	<p>We recommend pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue. Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat. Maecenas purus erat, mollis vitae, auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis.</p>	<p>04/29/2010</p> <p>Suspendisse quis lorem sit amet mauris interdum tempus. Sed et enim ut lacus semper tempor. Aliquam vulputate adipiscing risus. Suspendisse id lectus. Ut neque felis, pharetra in, varius id, pretium non, orci. Phasellus urna magna, placerat</p>
<div> <div></div> <div>High</div> </div> <p>Unauthorized access to payment file</p>	<p>● Inadequately Controlled</p> <p>Vendor setup/update is not centrally located; therefore, access to system is not properly supervised and maintained.</p>	<p>We noted that Pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue. Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat. Vendors are added as approved vendors without proper research and authorization</p>	<p>We recommend pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue. Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat.</p>	<p>04/29/2010</p> <p>hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat. Vendors are added as</p>

Entity Logo/ Name

Finding Name (Criticality)	Risk (Operating Effectiveness)	Observation/Process Enhancements	Recommendation	Due Date Remediation Plan
<div><div>■ Low</div><div>Errors on supplier invoices</div></div>	<div><div>● Well Controlled</div><div>Vendor file not purged or kept current on a periodic basis which results in authorized payees who may no longer be.</div></div>	<div><div>We noted that Pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue.</div><div>Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem.</div><div>Donec placerat massa non nisl. Aliquam erat volutpat. Vendors are added as approved vendors without proper research and authorization</div></div>	<div><div>We recommend pellentesque fringilla ante in leo. Nunc vulputate sapien vitae augue.:</div><div><ul style="list-style-type: none">Fusce lacus purus, dictum eu, mattis vel, hendrerit eget, lorem. Donec placerat massa non nisl. Aliquam erat volutpat.Maecenas purus erat, mollis vitae, auctor vitae, mollis at, sem.Quisque non nulla tincidunt odio blandit mattis</div></div>	<div><div>04/30/2010</div><div>Suspendisse quis lorem sit amet mauris interdum tempus:</div><div><ol style="list-style-type: none">Sed et enim ut lacus semper tempor.Aliquam vulputate adipiscing risus.Suspendisse id lectus.Ut neque felis, pharetra in, varius id, pretium non, orci.Phasellus urna magna, placerat</div></div>
<div><div>No Finding</div></div>	<div><div>● Inadequately Controlled</div><div>Inaccurate or incomplete vendor information entered into the system causing error in payments to that vendor.</div></div>			

Entity Logo/ Name

Finding Name (Criticality)	Risk (Operating Effectiveness)	Observation/Process Enhancements	Recommendation	Due Date Remediation Plan
No Finding	<div><div></div>Adequately Controlled Management reports are inaccurate</div>			
No Finding	<div><div></div>Inadequately Controlled Unauthorized vendor accounts established.</div>			



Appendix 11 Follow Up Report

Follow Up report

Audit	Finding	Observation and Recommendation	Remediation	Due Date	Review
Accounts Payable Audit	Criticality: High Vitae consequat dui neque eu risus. Phasellus ac lacus in erat	Observation: We noted that auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare, sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque. Aliquam Recommendation: We recommend auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis.	Management Owner: Mohammed K. Status: Complete Remediation Plan: Suspendisse quis lorem sit amet mauris interdum tempus. Sed et enim ut lacus semper tempor. Aliquam vulputate adipiscing risus. Suspendisse id lectus. Ut neque felis, pharetra in, varius id, pretium non, orci. Phasellus una magna, placerat	1-Jun-10	Review Status: 4. Approved Review Comment: Suspendisse quis lorem sit amet mauris interdum tempus.
	Criticality: Low Unauthorized access to accounts payable records	Observation: We noted that auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare, sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque. Aliquam Recommendation: We recommend phasellus ac lacus in erat egestas scelerisque. Aliquam	Management Owner: Mohammed K. Status: Complete Remediation Plan: Sed et enim ut lacus semper tempor. Aliquam vulputate adipiscing risus. Suspendisse id lectus. Ut neque felis, pharetra in, varius id, pretium non, orci. Phasellus una magna, placerat	28-May-10	Review Status: 4. Approved Review Comment: Suspendisse quis lorem sit amet mauris interdum tempus. Sed et enim ut lacus semper tempor. Aliquam vulputate adipiscing risus. Suspendisse id lectus. Ut neque felis, pharetra in, varius id, pretium non, orci. Phasellus una magna, placerat
	Criticality: Medium fraudulent payments detected	Observation: We noted that auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare, sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque. Aliquam Recommendation: We recommend quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare, sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque. Aliquam	Management Owner: Ahmed M. Status: In Progress Remediation Plan: Ut neque felis, pharetra in, varius id, pretium non, orci. Phasellus una magna, placerat Suspendisse quis lorem sit amet mauris interdum tempus. Sed et enim ut lacus semper tempor. Aliquam vulputate adipiscing risus. Suspendisse id lectus.	20-Apr-10	Review Status: 3. Review Comments Review Comment: eget, lorem. Donec placerat massa non nisi. Aliquam erat volutpat. Maecenas purus erat, mollis vitae, auctor vitae, mollis at, sem
Human Resources Audit (Example)	Criticality: High Vitae consequat dui neque eu risus. Phasellus ac lacus in erat	Observation: We noted that auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare, sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque. Aliquam Recommendation: We recommend auctor vitae, mollis at, sem. Quisque non nulla tincidunt odio blandit mattis. Quisque vestibulum, arcu vitae placerat ornare, sem est porttitor lacus, vitae consequat dui neque eu risus. Phasellus ac lacus in erat egestas scelerisque. Aliquam	Management Owner: Ahmed M. Status: In Progress Remediation Plan: Suspendisse quis lorem sit amet mauris interdum tempus. Sed et enim ut lacus semper tempor. Aliquam vulputate adipiscing risus. Suspendisse id lectus. Ut neque felis, pharetra in, varius id, pretium non, orci. Phasellus una magna, placerat	20-Apr-10	Review Status: 3. Review Comments Review Comment: Suspendisse quis lorem sit amet mauris interdum tempus.