Orientation for Risk Management and Internal Auditing in Energy Field

COSO Enterprise Risk Management Integrating With Strategy And Performance 2017

ISO 31000:2009 Risk Management _ A Practical Guide

ISO 31000:2009 Risk Management _ A Practical Guide

COSO Internal Control Integrated Framework 2013

International Professional Practices Framework - IPPF

Prepared By:
Eng. Ahmed Taamah.

Flow of Thoughts

About Me

What is Risk?

Enterprise Risk Management _ Definition and Benefits

Enterprise Risk Management _ Frameworks

Enterprise Risk Management Process

Tips for Practical Implementation of Risk Management

Risk Based Internal Auditing

Internal Audit Services

IA Framework and Methodology

Role of Internal Auditing in Risk Management

The IIA`s Three Lines Model

Prepared By:
Eng. Ahmed Taamah.

About Me

Internal Audit Director

Resourceful Manager with years of expertise in organizing business operations and resource management to achieve smooth flow and project operations. I've expensive knowledge of financial and operational risk. Offering sound judgment and the ability to interpret policies and controls.

SKILLS

Communication	Management
Team player	Detailed-focused
Analytical	Leadership
Critical thinking	Integrative
Interposition	Problem solving

EDUCATION

University of Leicester, UK 2014
Master of Business Administration with Merit

Yarmouk University, Jordan 2005
Electrical Power Engineering GPA 79.3

WORK EXPERIENCE

+17 years experience in **Construction** and **Energy** field:

Contract management 6 years
Project management 5.5 years
Enterprise risk management 6 years

ACHIEVEMENTS

- Successfully delivered 450,000,000 SAR package of projects (five power substations) with high profit margins and four certificates awarded by Saudi National Grid NG.
- Successfully established and managed ERM and internal auditing functions for large construction and holding companies.
- Successfully won profitable tenders in energy sector (132KV Power Substations/ Expansions/Overhead and underground transmission Tenders).

HOBBIES

Reading
Writing
Traveling

CONTACT INFO

Email: abuteamah@yahoo.com
Mobile: 00966564391976

What is Risk?

ما الأخطار؟

What is Risk? ISO 31000:2009

Effect of Uncertainty on Objectives

تأثير اللايقين على تحقيق الأهداف

Positive Consequence

If it enhances the achievement of **objectives**

Negative Consequence

If it limits or diminishes the achievement of **objectives**

Uncertainty is the **state**, even partial, of deficiency of information related to, understanding or knowledge of an **event**, its consequences or likelihood

Objectives can have different aspects (financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note: ISO (International Organization for Standardization) is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards

Prepared By:
Eng. Ahmed Taamah.

What is Risk? COSO ERM Framework

The possibility that events will occur and affect the achievement of strategy and business objectives.

احتمالية حصول أحداث تحد من تحقيق أهداف واستراتيجيات المؤسسة

It/they may/may not occur.

Those measurable steps the organization takes to achieve its strategy.

Impact of the event/s

Note: COSO is the Committee of Sponsoring Organizations of the Treadway Commission.

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

Prepared By:
Eng. Ahmed Taamah.

What is Risk?

The possibility that events will occur and affect the achievement of strategy and business objectives.

Effect of Uncertainty on Objectives

Event: An occurrence or set of occurrences. (الحدث أو مجموعة الأحداث)

Uncertainty: The state of not knowing how or if potential events may manifest. (حالة الغموض أو اللايقين فيما يتعلق بالحدث و الأثر)

Severity: A measurement of considerations such as the likelihood and impact of events or the time it takes to recover from events.
(درجة/حدة الخطورة باعتبار الحدث وأثره)

Prepared By:
Eng. Ahmed Taamah.

Two Trees Growing

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management _ Definition and Benefits

التعريف والفوائد المرجوة

Risk Management Definition

Enterprise risk management:

The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value through:

- Recognizing culture.
- Developing capabilities.
- Applying practices.
- Integrating with strategy-setting and performance.
- Managing risk to strategy and business objectives.

الثقافة والإمكانيات والممارسات ، المتكاملة مع الإستراتيجية والأداء، التي تعتمد عليها المؤسسات لإدارة المخاطر في إنشاء القيمة والحفاظ عليها وتحقيقها من خلال:
الاعتماد على الثقافة وتطوير القدرات وتنفيذ الممارسات والتكامل مع الإستراتيجية والأداء لإدارة المخاطر التي تحد من تحقيق الأهداف والاستراتيجية.

Risk management

Coordinated activities to direct and control an organization **with regard to risk**.

مجموعة من الأنشطة المنظمة لتوجيه المنشأة والتحكم في مخاطرها

Prepared By:
Eng. Ahmed Taamah.

Risk Management Benefits

- Increase the range of opportunities: By considering all reasonable possibilities both positive and negative aspects of risk management can identify opportunities for the entity and unique challenges associated with current and future opportunities.
- Increase positive outcomes and advantage while reducing negative surprises: Enterprise risk management allows an organization to improve its ability to identify risks and establish appropriate responses, increasing positive outcomes while reducing negative surprises and related costs or losses.
- Identify and manage entity-wide risks: Every entity faces myriad risks that can impact many parts of the entity. Sometimes a risk can originate in one part of the entity but affect a different part. Management must identify and manage these entity-wide risks to sustain and improve performance.
- Reduce performance variability: For some entities, the challenge is less about surprises and losses, and more about performance variability. Performing ahead of schedule or beyond expectations may cause as much concern as performing below expectations.
- Improve resource deployment: Obtaining robust information on risk allows management to assess overall resource needs and helps to optimize resource allocation.

- **زيادة نطاق الفرص: باعتبارالاحتمالات المنطقية، سواءً ذات الأثر الإيجابي أو السلبي، حيث يمكن لإدارة المخاطر أن تحدد الفرص المتاحة للمؤسسة في الوقت الراهن أو مستقبلًا مع ما يصحبها من تحديّات.**
- **زيادة النتائج الإيجابية والمزايا وتقليص امكانية حدوث المفاجآت السلبية: تمكّن إدارة مخاطر المؤسسة من تحسين قدرتها على تحديد المخاطر وتطوير الاستجابات المناسبة ، وزيادة النتائج الإيجابية وتقليل المفاجآت غير المتوقعة من حيث التكلفة أو الخسارة.**
- **تحديد وإدارة المخاطر على مستوى المؤسسة: لكل مؤسسة مخاطرها ذات الأثر على أقسام كثيرة منها. في بعض الأحيان يمكن أن تنشأ المخاطر في جانب من جوانب الشركة ويؤثر في الجوانب الأخرى. لذا ينبغي على الإدارة تحديد وإدارة هذه المخاطر على مستوى المؤسسة لتحسين الأداء والمحافظة عليه.**
- **التقليل من تفاوت في الأداء: تتأثر بعض المؤسسات بتفاوت الأداء أكثر من تأثرها بالأحداث غير المتوقعة والخسائر المصاحبة لها. الزيادة في الأداء فوق الحد المرغوب به قد يكون مصدر إزعاج للإدارة كالإخلال في الأداء دون المستوى المرغوب.**
- **تحسين توظيف الموارد: الحصول على معلومات دقيقة عن المخاطر يسمح للإدارة بتقييم حجم الموارد المطلوبة وهذا بدوره يحسّن من توزيعها بكفاءة.**

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management _ Frameworks

إداراة المخاطر الشاملة – الأطر المعتمدة

Enterprise Risk Management _ Frameworks

COSO ERM:
Five Components
Twenty Principles

ISO 31000:
ISO 31000 2009 a Practical Guide
ISO 31000 2018 a Practical Guide
ISO 31000 2018 Risk Management Guidelines

ISO IEC 31010: Risk Assessment Techniques

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management _ COSO ERM

Governance and Culture

Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

Strategy and Objective-Setting

Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

Performance

Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

Review and Revision

By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

Information, Communication and Reporting

Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management _ COSO ERM

1. Exercises Board Risk Oversight
The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.

2. Establishes Operating Structures
The organization establishes operating structures in the pursuit of strategy and business objectives.

3. Defines Desired Culture
The organization defines the desired behaviors that characterize the entity's desired culture.

4. Demonstrates Commitment to Core Values
The organization demonstrates a commitment to the entity's core values.

5. Attracts, Develops, and Retains Capable Individuals
The organization is committed to building human capital in alignment with the strategy and business objectives.

6. Analyzes Business Context
The organization considers potential effects of business context on risk profile.

7. Defines Risk Appetite
The organization defines risk appetite in the context of creating, preserving, and realizing value

8. Evaluates Alternative Strategies
The organization evaluates alternative strategies and potential impact on risk profile

9. Formulates Business Objectives
The organization considers risk while establishing the business objectives at various levels that align and support strategy.

10. Identifies Risks
The organization identifies risk that impacts the performance of strategy and business objectives..

11. Assesses Severity of Risks
The organization assesses the severity of risk.

12. Prioritizes Risks
The organization prioritizes risks as a basis for selecting responses to risks.

13. Implements Risk Responses
The organization identifies and selects risk responses.

14. Develops Portfolio View
The organization develops and evaluates a portfolio view of risk.

15. Assesses Substantial Change
The organization identifies and assesses changes that may substantially affect strategy and business objectives.

16. Reviews Risk and Performance
The organization reviews entity performance and considers risk.

17. Pursues Improvement in Enterprise Risk Management
The organization pursues improvement of enterprise risk management.

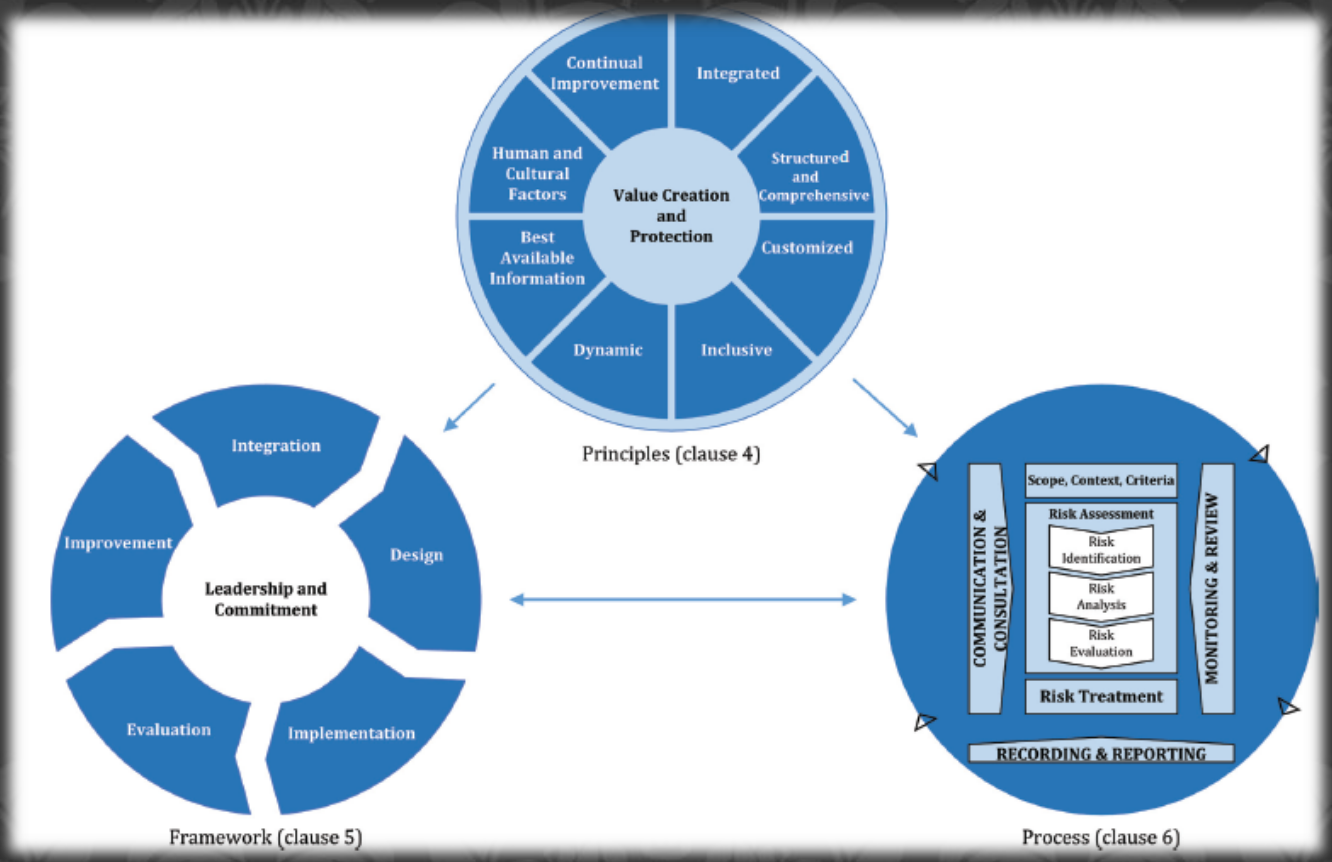
18. Leverages Information Systems
The organization leverages the entity's information and technology systems to support enterprise risk management.

19. Communicates Risk Information
The organization uses communication channels to support enterprise risk management.

20. Reports on Risk, Culture, and Performance
The organization reports on risk, culture, and performance at multiple levels and across the entity.

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management _ ISO 31000



Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management Process

عملية إدارة المخاطر

Enterprise Risk Management Process

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management Process _ Establish the Context

Risk Management Process

The Context

Prepared By:
Eng. Ahmed Taamah.

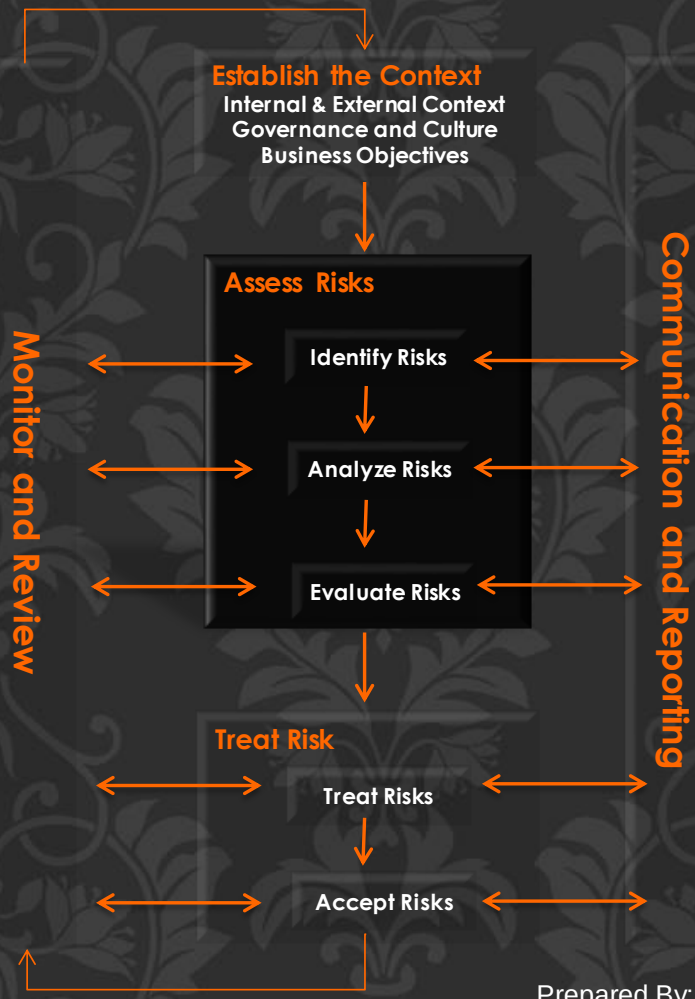
Enterprise Risk Management Process _ Assess Risks

Risk Management Process

Assess Risks

The process that sets out how to identify, analyze and evaluate risks

تقييم المخاطر هي العملية الشاملة لتحديد المخاطر وتحليلها وتقديرها.



Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management Process _ Identify Risks

تحديد "معرفة"المخاطر

Risk Management Process

Assess Risks

Identify Risks

Identify what, why, and how events can arise and prevent minimize or delay achieving objectives

- **Categorize the Objectives**
  - Budget, Scope, Schedule, etc.
  - Customer Satisfaction.
  - Operation, Reporting, Compliance, etc.
- **Identify, new, emerging and changing risks**
  - Change in Business context objectives, strategy and regulation.
  - Not previously identified in the same business context.
  - Were previously identified but require change in severity.
  - Emerging Technology, Labor shortage, Big data analysis.
- **Identification Approaches**
  - Brainstorming Workshops
  - Structured Interviews, Process Analysis
  - Data Analysis, SWOT Analysis, Surveys, Learned Lessons.

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Assess Risks

How to write Risk Statement?

Risk statement provides an accurate picture of the risk

- Events and impacts should be relevant to organization objectives.
- Negation of control is not a risk statement (Avoid the use of “lack of, absence of”).
- Risk statement should be clear and concise.

Examples:

- Loss of skilled employees may affect the quality of services and the business unit`s ability to achieve its objectives.
  - فقدان الموظف الجيد قد يؤثر في جودة العمل
- Unclear scope may result in inaccurate cost estimate.
  - نطاق العمل المبهم قد يؤدي الى احتساب التكلفة بشكل غير دقيق

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management Process _ Analyze Risks

تحليل المخاطر

Risk Management Process

Assess Risks

Analyze Risks

Analyze Risks:

The method of assessing the severity of consequences and the likelihood of the risk on the business objectives based on a definite criteria.

- Define assessment criterion.
- Define likelihood criterion
- Apply the defined criteria to agree on risk score/rating.

The output of risk analysis is the level of inherent risk.

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Assess Risks

Impact Criteria

Setting impact dimensions to measure the severity of the risk if it took place.

Impact value	Impact Description	Impact Criteria				
		Financial	Operational	Regulatory legal	Customer Stakeholders	Business Growth
5	Extreme					
4	High					
3	Moderate					
2	Low					
1	Insignificant					

Impact value	Impact Description	Impact Criteria				
		Financial	Business Continuity	Regulatory legal	Reputation	Human Resource
5	Extreme					
4	High					
3	Moderate					
2	Low					
1	Insignificant					

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Assess Risks

Likelihood Criteria Example

Setting likelihood dimensions to measure the possibility of risk occurrence.

Likelihood value	Likelihood Description	Likelihood Criteria
5	Almost certain	Event is expected to occur once or more per year Or is almost certain to occur i.e. probability > 50%
4	Likely	Event is expected to occur once or more within the next 1 to 5 years Or is expected to occur in most circumstances i.e. probability > 30% and <=50%
3	Possible	Event is expected to occur once or more within the next 5 to 10 years Or is expected to occur i.e. probability > 20% and <=30%
2	Unlikely	Event is expected to occur once or more within the next 10 to 20 years Or is unlikely to occur i.e. probability > 10% and <=20%
1	Rare	Event may occur once in the next 20 years Or may occur in exceptional circumstances i.e. probability <=10%

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Assess Risks

Risk Score

Risk Score = Impact + Likelihood

Risk Score	Risk Category
2	Low
3	Low
4	Medium
5	Medium
6	High
7	High
8	Extreme
9	Extreme
10	Extreme

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Assess Risks

Inherent Risk

The result of the risk analysis is the **inherent** risk rating

is the risk to an entity (organization) in the absence of any direct or focused actions (Controls/Mitigations) by management to alter its severity (rating).

الخطر المتأصل

هو درجة أو حدة الخطر في ظل غياب أي من الضوابط الرقابية أو أي إجراء من قِبل الإدارة المعنية.

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management Process _ Evaluate Risks

Risk Management Process

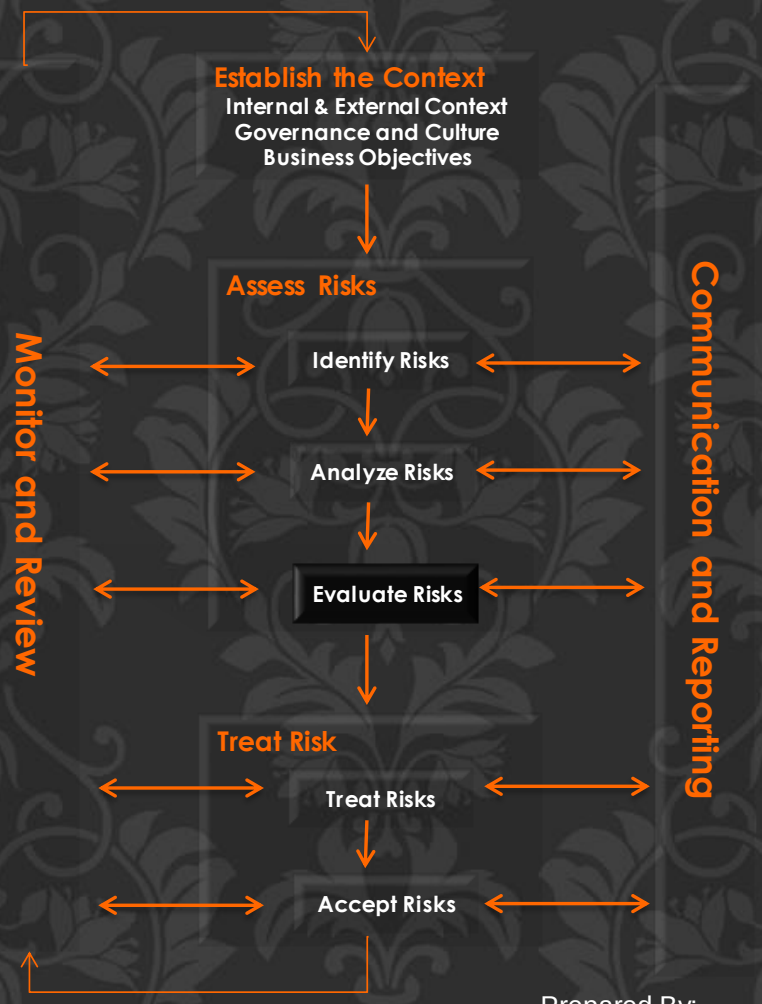
Assess Risks

Evaluate Risks

After being analyzed, risks need to be evaluated, therefore, management should decide whether to accept, mitigate, tolerate, run away from the risk.

Successful Risk Evaluation depends on:

- Defining risk criteria.
- Identifying and assessing controls in place.
- Defining target and actual residual risk level.



Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Asses Risks

Risk Criteria

To identify the need of any required action/response to risk/controls against each risk identified and analyzed, risk criteria must be defined as follows:

Score	Inherent Risk Level	Required Action
2,3	Low	Rational for not evaluating mitigating controls in place should be documented. Executive Manager review is required.
4,5	Medium	Primary mitigating controls in place should be evaluated to determine residual risk level. General Manager review is mandatory.
6,7	High	All mitigating controls in place must be evaluated to determine residual risk level. The President/VP review is mandatory.
8,9,10	Extreme	All mitigating controls in place must be evaluated to determine residual risk level. The President/VP review is mandatory.

Prepared By:
Eng. Ahmed Taamah.

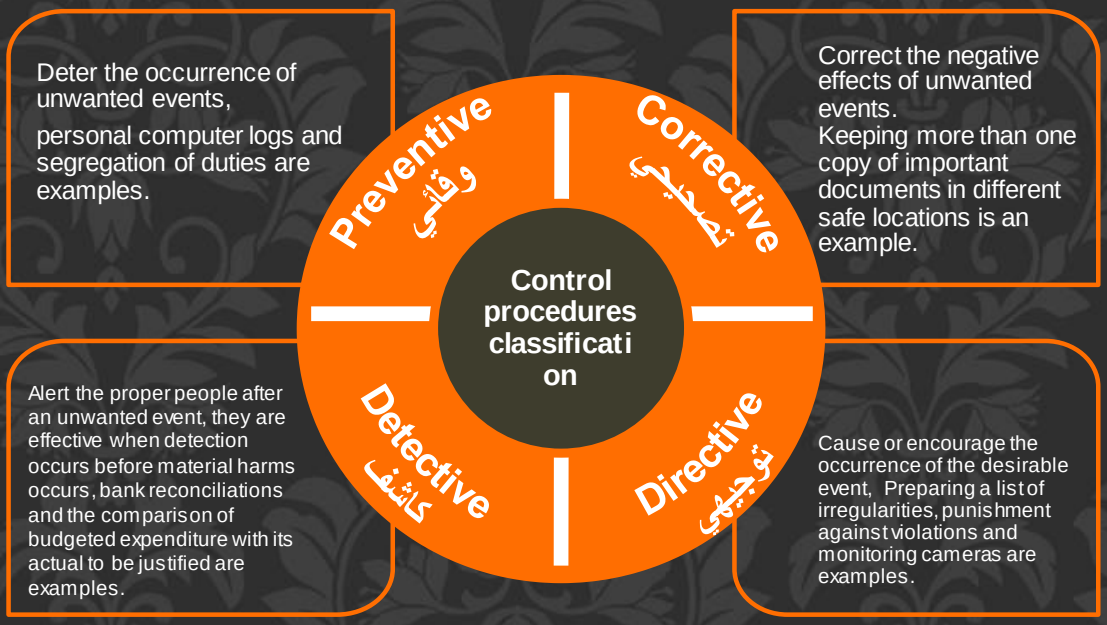
Risk Management Process

Assess Risks

Existing Controls

A Process effected by an entity`s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

الضابط الرقابي هو أي إجراء أو ممارسات – منبثقة من مجلس الإدارة أو إدارة المؤسسة أو فريق العمل – بغرض تأكيد تحقيق الأهداف المتعلقة بالتشغيل وإعداد التقارير والامتثال.



Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Evaluate Risks

Residual Risk

Actual Residual Risk الخطر المتبقي فعليا

is the risk remaining after management has taken action to alter its severity.

هي المخاطر المتبقية بعد أن تتخذ الإدارة إجراءً لتغيير حدتها

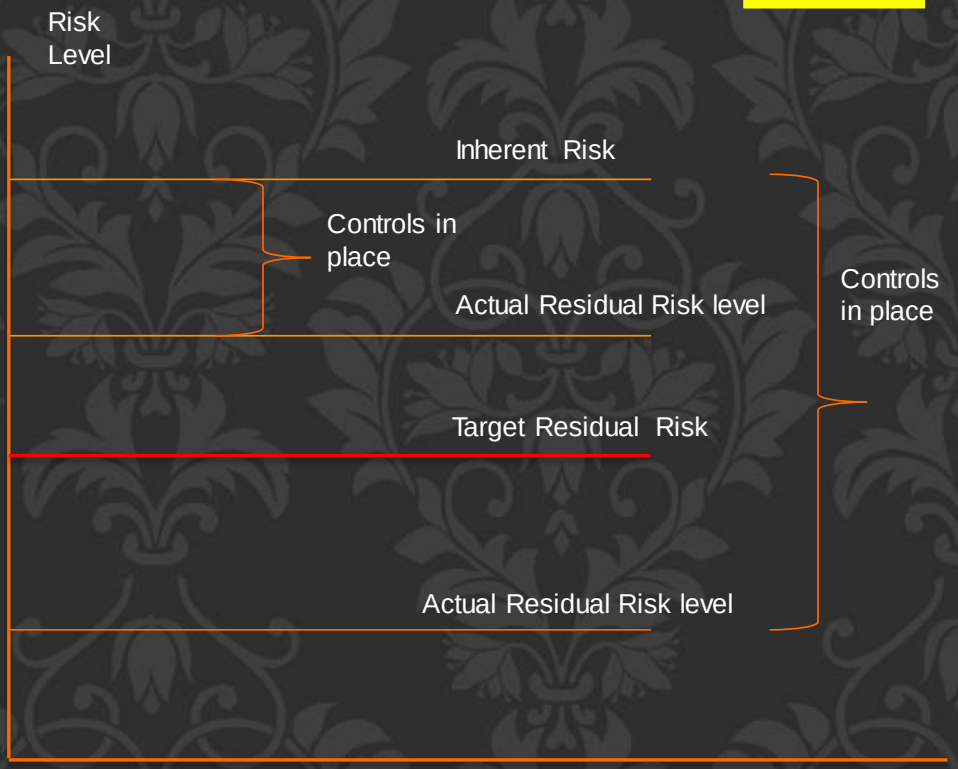
Actual residual risk should be equal to or less than the target residual risk. Where actual residual risk exceeds target risk, additional actions should be identified that allow management to alter risk severity further.

Target Residual Risk حد الخطر المتبقي

is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.

هو مقدار الخطر الذي تفضل المؤسسة تحمله في السعي لتحقيق استراتيجيته والأهداف.

Real Example



Prepared By:
Eng. Ahmed Taamah.

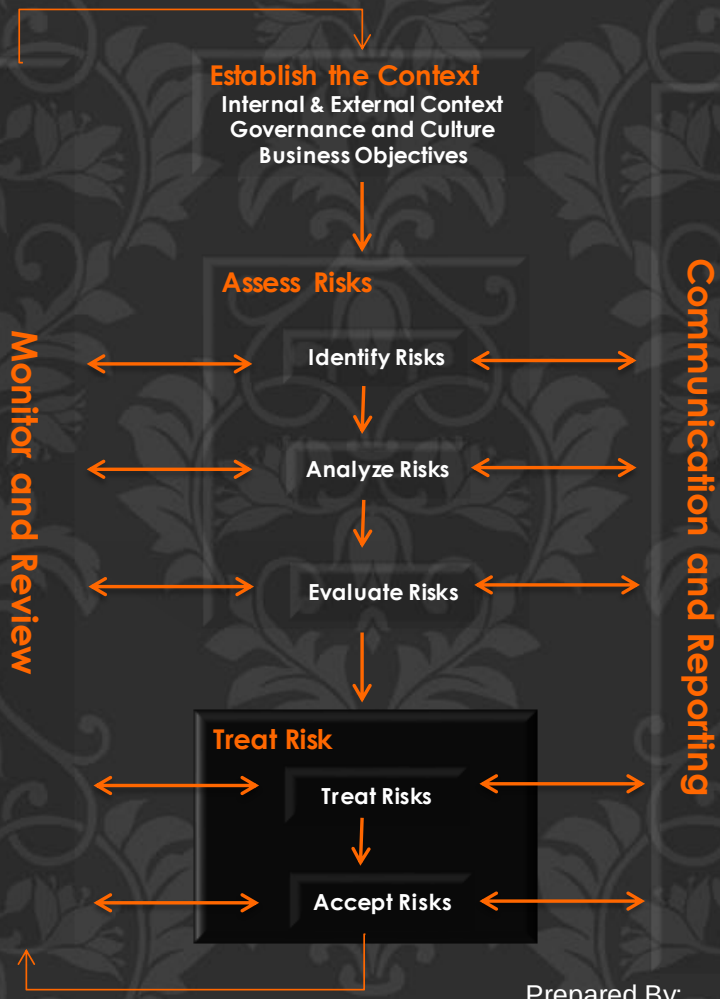
Enterprise Risk Management Process _ Treat Risks

معالجة الأخطار

Risk Management Process

Treat Risks

When risk evaluation determines that a risk is intolerable notwithstanding current risk treatments then additional treatment is required



Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

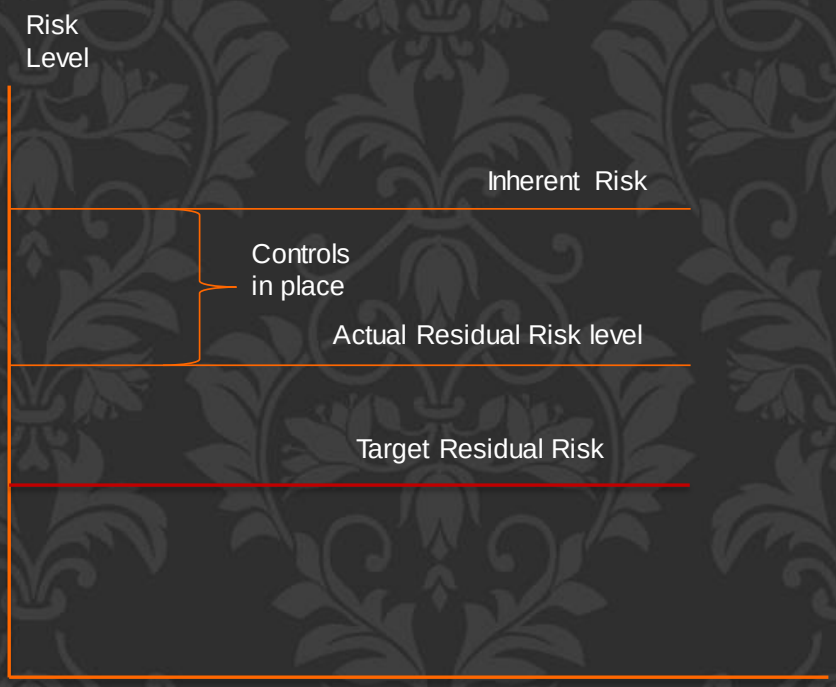
Treat Risks

When risk evaluation determines that a risk is intolerable notwithstanding current risk treatments then additional treatment is required

In case the actual residual risk is higher than the target residual risk, additional treatment is required to mitigate the risk in order to reach the target residual level.

ISO defined Risk Tolerance:
organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.

ISO defined Risk Attitude:
organization's approach to assess, and eventually pursue, retain, take or turn away from risk.



Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Treat Risks

ISO Risk Treatment Approach:

- Avoiding the risk by ending, or not starting the activity which is associated with the risk (e.g. not producing products that require storage, handling or disposal of hazardous materials).
- Increasing the risk to pursue an opportunity (e.g. opening a new location, developing a new product or service).
- Changing the likelihood (e.g. introducing an additional safety control for an activity).
- Changing the consequences (e.g. moving to automated manufacturing where the risk to human health and safety is too great and machines or robots can produce the product and ensure that employees are protected from injuries associated with the manufacturing process).
- Sharing the risk with another party (e.g. purchasing insurance or using contractors or financing partners).
- Retaining the risk by informed choice (e.g. a criteria based determination that the current risk level is acceptable).

COSO Risk Treatment Approach:

- Avoid: Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity.
- Pursue: Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.
- Reduce: Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduces risk to an amount of severity aligned with the target residual risk profile and risk appetite.
- Share: Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist
- Accept: No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite. Risk that is outside the entity's risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies.

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Treat Risks

Accept Risks

Risk Appetite

The types and amount of risk, an organization is willing to accept in pursuit of value.

In other words, who is authorized to accept the risk

درجة تقبل المخاطر

مقدار الخطر ونوعه الذي تسعى المؤسسة لقبوله.

من المخوّل؟

Inherent Risk Level	Acceptable Residual Risk Level	Approval Authority
Low	Low	No additional controls are required. Executive Manager review is required.
Medium	Low	Acceptable residual risk level for a medium inherent risk is Low. General Manager approval is required to accept a higher residual risk.
High	Low	Acceptable residual risk level for a high inherent risk is Low. The President/VP approval is required to accept a higher residual risk.
Extreme	Medium	Acceptable residual risk level for an extreme inherent risk is medium. The President/VP approval is required to accept a higher residual risk.

Prepared By:
Eng. Ahmed Taamah.

Enterprise Risk Management Process _ Communication and Reporting

Risk Management Process

Communication and Reporting

Monitor and review

- Internal and external stakeholders should be identified and their objectives, expectations and concerns should be considered.
- Communication with stakeholders should take place during all stages of the risk management process.
- Risk management process should be monitored and reviewed on an ongoing basis.
- Review the effectiveness of the risk management framework.

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Communication and Reporting

Communication plan for ERM

Report	Prepared by	Reviewed by	Timeline	Contents
Risk and Control Matrix (RCM)	Business Unit Managers	Concerned Vice President.	Quarterly	The RCM includes business unit/department objectives, risks, the inherent and residual risk ratings, risk owner, controls in place, control owner and control assessment.
Top 10 Risks.	ERM Manager.	CEO & Board.	Quarterly	Top 10 Risks Report includes the most critical risks that may affect the achievement of strategic objectives of the organization.
ERM Status Report	ERM Manager	President.	Semi Annually	Comprehensive report presents holistic review of ERM system status.

Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Communication and Reporting

Communication plan for risk management in projects

Report	Prepared by	Reviewed by	Timeline	Contents
General Risk Register	Committee, ERM team	Vice President.	Semi Annually.	General Risk Register includes risks, the inherent and residual risk ratings, Risk owner, proposed controls, action plans, that applies to each group of similar projects
Project Risk Register	Project Manager, ERM team	Area Manager	Monthly	Project Risk Register includes risks, the inherent and residual risk monetary values, inherent and residual risk impact on schedule, action plans, assignment and target date.
Area Wise Risk Summary	Concerned Area Manager	Vice President	Quarterly	Summary of risks for each project, area wise

Prepared By:
Eng. Ahmed Taamah.

Roles and Responsibilities for Enterprise Risk Management

Risk Management

Roles and Responsibilities

Board /Audit & Risk Committee/Risk Committee

- Establishes the direct oversight of enterprise risk management.
- Engages with management to define the suitability of enterprise risk management.
- Promotes a risk aware mindset that aligns.
- Understands how risk is monitored by management.
- Understand how management identifies and communicates severe risks
- Reviews and understands the most significant risks.

CEO / General Manager

- Identify and support the organization's commitment to risk management.
- Approve the risk management framework and risk management policy.
- Set the objectives to be achieved by implementing risk management.
- Approve the risk criteria.
- Approve a mechanism that escalates risk within the organization in accordance with the organization's risk tolerance.

ERM Manager / CRO

- Monitors and reviews the implementation of risk management.
- Communicates with management about the status of enterprise risk management.
- Supports management and staff by identifying appropriate and relevant risk management tools and training.
- Promotes enterprise risk management to the CEO and operating unit leaders and assists in integrating practices into their business plans and reporting.
- Escalating identified or emerging risk exposures to executive management and the board.

Senior Managements

- Integrate risk management into organizational strategy and into management frameworks.
- Always consider risk information as an input to decision making.
- Provide managers and employees with clear information on the organization's oversight of the risk management function.
- Ensure that there is an effective risk management process and that the risk treatment plan is in place and monitored.

Prepared By:
Eng. Ahmed Taamah.

Tips for Practical Implementation of Risk Management

Risk Management

Tips for Implementation

- Standards such as ISO 31000 and COSO ERM Integrating with Strategy and Performance are for guidance.
- Qualitative approach is recommended at all stages, in particular when establishing the framework:
  - In defining impact assessment criterion.
  - In defining likelihood assessment criterion.
  - In assessing the risk score.
  - In defining risk criterion.
  - In defining control effectiveness criterion.
  - In defining risk acceptance criterion (Appetite).
- Risk identification and assessment sessions require the involvement of the following participants:
  - Business unit manager
  - Risk Manager
  - Process Owners
  - Any subject mater experts (SME)
- Right understanding of risk terminologies are mandatory:
  - Inherent risk
  - Residual risk
  - Impact
  - likelihood
  - Internal controls
- Selecting the appropriate candidates for fulfilling the requirements of risk owner and control owner.

Risk Owner:

The name of the person with the accountability and authority to manage the risk.

Control Owner:

The name of the person accountable for the control (takes responsibility for control success or failure identified during testing and implements remediation where necessary), and has the authority to change its design and the way it is being executed.

Prepared By:
Eng. Ahmed Taamah.

Risk Management

Tips for Implementation

Technique	Advantage	Disadvantage
Qualitative	❑ Is relatively **quick and easy** ❑ Provides **rich information** beyond financial impact and likelihood such as vulnerability, speed of onset, and non-financial impacts such as health and safety and reputation ❑ Is **easily understood** by a large number of employees who may not be trained in sophisticated quantification Techniques	❑ Gives limited differentiation between levels of risk (i.e. very high, high, medium, and low) ❑ Is imprecise – risk events that plot within the same risk level can represent substantially different amounts of risk ❑ Cannot numerically aggregate or address risk interactions and correlations. ❑ Provides limited ability to perform cost-benefit Analysis
Quantitative	❑ Allows numerical aggregation taking into account risk interactions when using an "at risk" measure such as Cash Flow at Risk. ❑ **Permits cost-benefit analysis** of risk response options ❑ Enables risk-based capital allocation to business activities with optimal risk-return ❑ Helps compute capital requirements to maintain solvency under extreme Conditions	❑ Can be **time-consuming and costly**, especially at first during model development. ❑ Must choose units of measure such as dollars and annual frequency which may result in qualitative impacts being **overlooked.** ❑ Use of numbers may imply greater precision than the uncertainty of inputs warrants ❑ Assumptions may not be apparent

Both qualitative and quantitative techniques have advantages and disadvantages. **Most enterprises begin with qualitative assessments** and develop quantitative capabilities over time as their decision-making needs dictate.

Prepared By:
Eng. Ahmed Taamah.

Coffee Break

Risk Based Internal Auditing

What is Internal Auditing - Definition

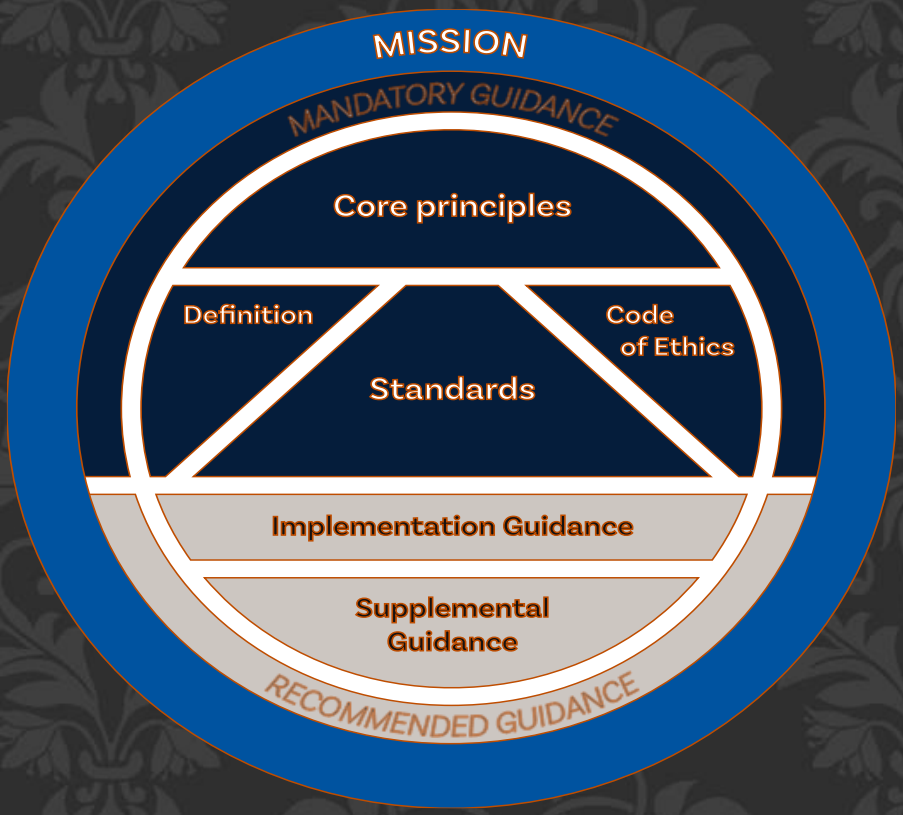
Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

التدقيق الداخلي هو نشاط مستقل وموضوعي، يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها . ويساعد هذا النشاط في تحقيق أهداف المؤسسة من خلال اتباع أسلوب منهجي منظم لتقييم وتحسين فاعلية عمليات الحوكمة وإدارة المخاطر و الرقابة الأهداف

Note: IIA “institute of internal auditors” established in 1941, is an international professional association and the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Prepared By:
Eng. Ahmed Taamah.

What is Internal Auditing - Standards



IPPF: International Professional Practices Framework

Prepared By:
Eng. Ahmed Taamah.

What is Internal Auditing - Mission

To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

تعزيز وحماية قيمة المؤسسة من خلال تقديم التأكيد و المشورة والبصيرة، الموضوعية و المستندة على المخاطر، لأصحاب المصلحة

Prepared By:
Eng. Ahmed Taamah.

What is Internal Auditing – Core Principles

Internal The Core Principles, above all, define tangible internal audit effectiveness. When all Principles are present and operating cohesively, internal audit function achieves maximum efficiency. Though the way every internal auditor approaches these Core Principles may vary from organization to organization, there's no denying that a failure to achieve any of the Principles would signal an internal audit activity that's not performing at its absolute best.

- **Demonstrates integrity.**
- **Demonstrates competence and due professional care.**
- **Is objective and free from undue influence (independent).**
- **Aligns with the strategies, objectives, and risks of the organization.**
- **Is appropriately positioned and adequately resourced.**
- **Demonstrates quality and continuous improvement.**
- **Communicates effectively.**
- **Provides risk-based assurance.**
- **Is insightful, proactive, and future-focused.**
- **Promotes organizational improvement.**

- **إظهار نزاهة كاملة.**
- **إظهار الكفاءة والعناية المهنية اللازمة**
- **أن يكون موضوعيا و متحررا من أي تأثيرات غير مناسبة (مستقل)**
- **أن يكون متوافقا مع استراتيجيات، أهداف ومخاطر المؤسسة.**
- **أن يكون في المركز الوظيفي المناسب ويمتلك الموارد الكافية**
- **إظهار الجودة والتحسن المستمر.**
- **التواصل بشكل فعّال**
- **تقديم تأكيد مرتكز على المخار**
- **ذو بصيرة ، مبادر وذونظرة مستقبلية**
- **يدعم تطوير وتحسين المؤسسة**

Prepared By:
Eng. Ahmed Taamah.

Internal Audit Services

Internal Audit Services

Prepared By:
Eng. Ahmed Taamah.

Internal Audit Services – Assurance

Assurance Services

خدمات التأكيد

An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements

هي عملية فحص موضوعي للأدلة بغرض تقديم تقييم مستقل لعمليات الحوكمة وإدارة المخاطر والرقابة. ومن الأمثلة على خدمات التأكيد:
مهمات تدقيق المالية، والأداء، والإمتثال للأنظمة والقوانين، وأمن النظم، والعناية اللازمة.

Prepared By:
Eng. Ahmed Taamah.

Internal Audit Services – Consulting

Consulting Services

الخدمات الاستشارية

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

أنشطة تقديم المشورة والخدمات المتعلقة بها لعميل ما، والتي يتمّ الإتفاق على طبيعتها ونطاقها مع هذا العميل، ويكون المقصود بها إضافة قيمة وتحسين عمليات الحوكمة وإدارة المخاطر والرقابة، وذلك من دون أن يضطلع المدقق الداخلي بأي مسؤوليات إدارية. ومن بين الأمثلة على هذه الخدمات تقديم المشورة والنصيحة والتسهيل والتدريب.

Prepared By:
Eng. Ahmed Taamah.

Internal Audit Services – Special

Special Assignment
مهام خاصة

- Forensic accounting and fraud indicators: This type of special assignments consider unethical or otherwise inappropriate activity or behavior, violation of laws, and/ established policies, when such activity is recognized through the scope of internal audit work or reported through the appropriate channels. This assignment may include determining misuse of assets, manipulations of records, fiscal misconduct, conflict of interest, and policy violations.
- Ad hoc: The BoD, ARC, and the company senior management may request ad hoc reviews where they define the objectives and scope of such a review.

- مؤشرات والاحتيال: تحديد أي نشاط أو سلوك غير مقبول يتضمن انتهاكًا للقوانين والسياسات والتي يتم استخلاصها من خلال نطاق عمل التدقيق الداخلي أو الإبلاغ عنه من خلال القنوات المناسبة. من أمثلة ذلك، إساءة استخدام الأصول، والتلاعب في السجلات، وسوء السلوك المالي ، وتضارب المصالح ، وانتهاكات سياسات الشركة.
- قد يطلب مجلس الإدارة أو لجنة المراجعة الداخلية أو الإدارة العليا للشركة مراجعات خاصة يتم تحديد أهدافها وطبيعتها من قِبلهم.

Prepared By:
Eng. Ahmed Taamah.

Internal Audit Services – Assurance

Assurance Services

خدمات التأكيد

Financial

Financial engagements assess, evaluate, and make recommendations to management regarding accounting and financial reporting of transactions and activities. Areas of financial audits may include accounting, procurement, segregation of duties, authorizations and approvals, reconciliations.

Business Technology

The business technology audit function will develop audit programs to assess, evaluate, and make recommendations to management regarding the adequacy of internal controls and security inherent in business systems

Operation

will assess risks and evaluate internal controls for operations. Audit areas may include tendering and contract pricing, procurement, sales and marketing, strategic planning, maintenance, Design, security of assets, quality management, safety, planning, training, administration services, HR, project costs schedule management.

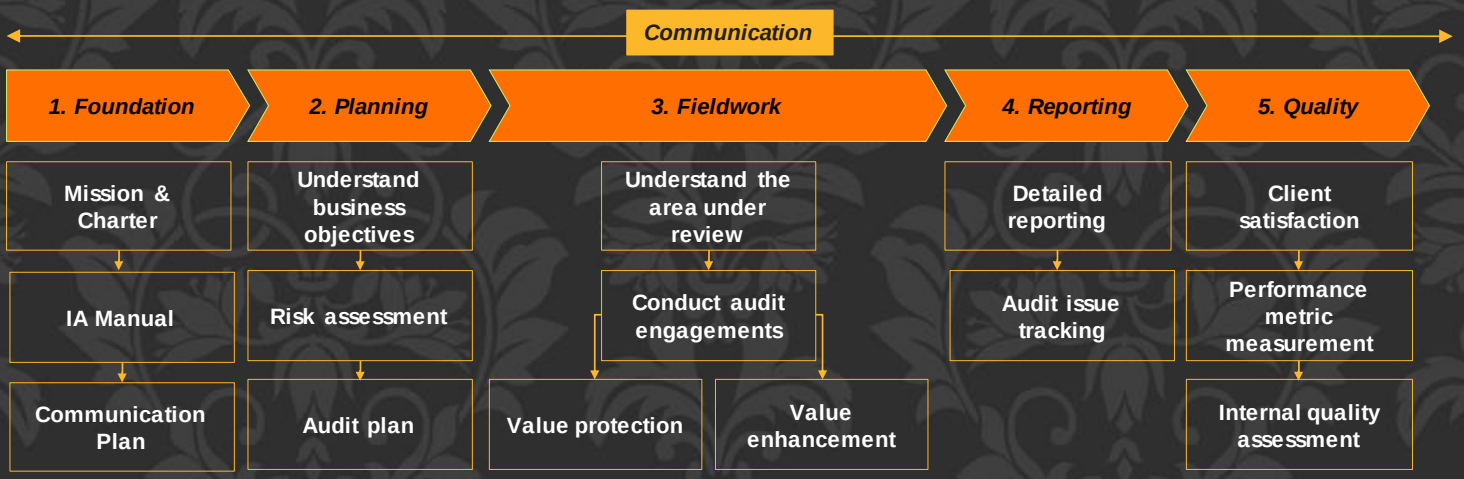
Compliance

The compliance audit function will focus on compliance risks and the related mitigation plans. The function will promote awareness of current and emerging laws and regulations impacting the company.

Prepared By:
Eng. Ahmed Taamah.

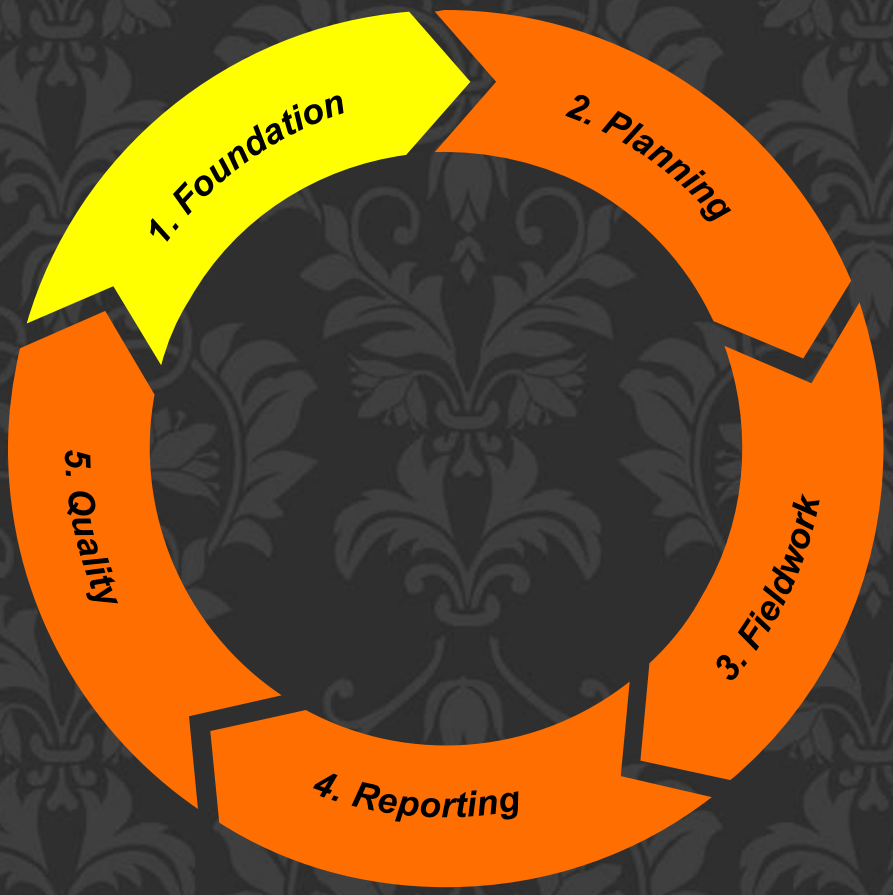
IA Framework and Methodology

IA Framework and Methodology



Prepared By:
Eng. Ahmed Taamah.

IA Framework - Foundation



Prepared By:
Eng. Ahmed Taamah.

IA Framework - Foundation

Audit Charter

The internal audit charter is a formal document that defines the internal audit activity's **purpose, authority, and responsibility**. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

ميثاق التدقيق الداخلي هو مستند رسمي يحدد الغرض من نشاط التدقيق الداخلي وصلاحياته ومسؤولياته. ويحدد ميثاق التدقيق الداخلي موقع نشاط التدقيق الداخلي في المؤسسة، ويخوّل الإطلاع على السجلات والإتصال بالموظفين والوصول إلى الممتلكات المادية بما يُمكّن من أداء مهمات التدقيق، كما يحدد نطاق أنشطة التدقيق الداخلي.

Prepared By:
Eng. Ahmed Taamah.

Communications - IA Key Stakeholders

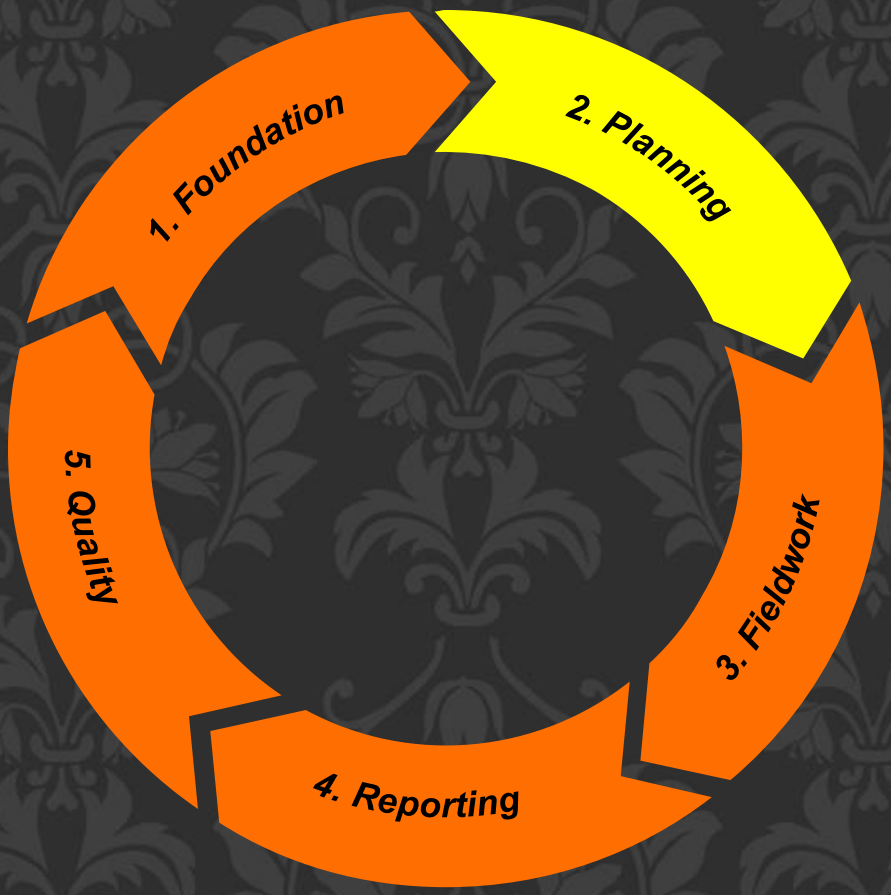
IA Framework - Foundation

Communications - IA Key Stakeholders

Report	Approved by	To	Timeline/ Frequency	Contents
Draft audit report	Chief Audit Executive	Management and Process Owner	In a week after the closing meeting	The draft report includes an executive summary, overall rating, and detailed findings.
Final audit report	Chief Audit Executive	ARC, Senior Management, Management, and Process Owner	In two weeks after issuing the draft audit report	The final report includes an executive summary, agreed overall rating, detailed findings, management response and agreed action plans and implementation timelines.
Follow up audit report	Chief Audit Executive	ARC, Senior Management, Management, and Process Owner	In a week after completing the follow up fieldwork	The follow up audit report includes findings, agreed action plans, agreed implementation timelines, and implementation status.

Prepared By:
Eng. Ahmed Taamah.

IA Framework - Planning



Prepared By:
Eng. Ahmed Taamah.

Identify

3. Fieldwork

IA Framework - Planning

Planning – Risk Assessment and Audit Plan

Auditable Units:

The auditable units represent the way management runs the entity based on the organizational structure such as the location, process, Department, or product. Auditable units represent the audit universe.

Impact	Likelihood				
	1	2	3	4	5
5	Significant	Significant	High	High	High
4	Moderate	Significant	Significant	High	High
3	Moderate	Moderate	Significant	Significant	High
2	Low	Moderate	Moderate	Significant	Significant
1	Low	Low	Moderate	Moderate	Significant

3. Field of

HIGH:
- The most exposed activities to risk
- Activities that have material impact on the achievement of objectives
- Activities that require immense need to study their controls nature

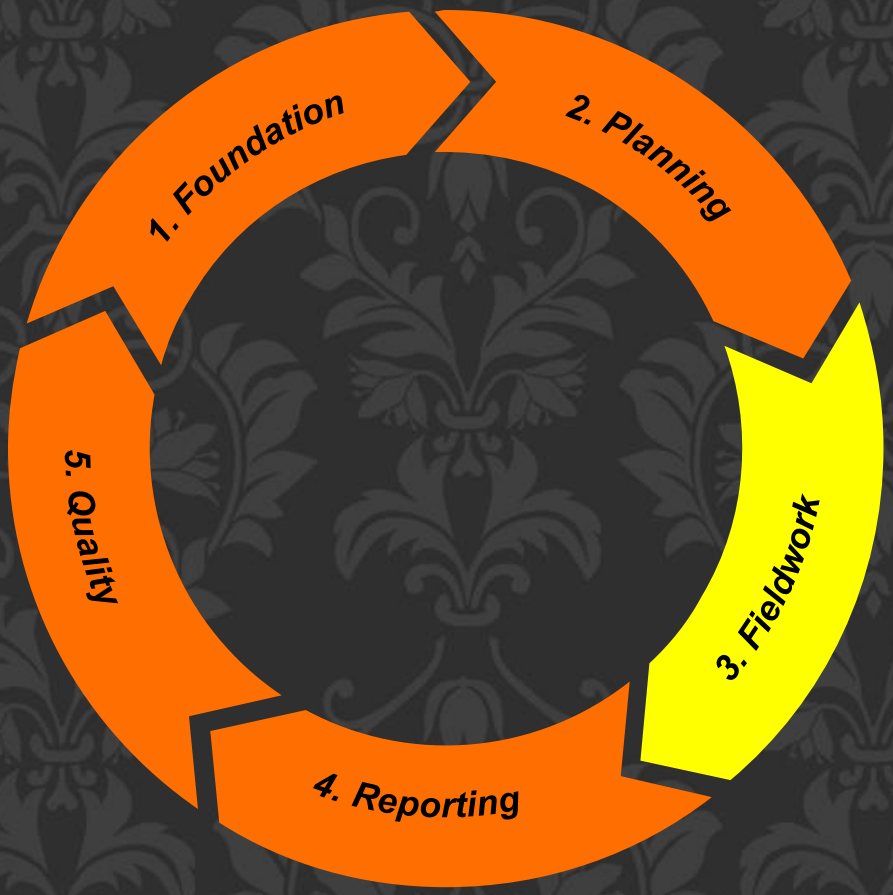
Significant:
- Activities exposed to risks
- Activities that clearly has an impact on the achievement of objectives
- Activities that need monitoring its extent of compliance with the designed procedures

Moderate:
- Activities that may be exposed to risks
- Activities that may have an impact on achieving objectives

Audit Requirement Rating	Level of Internal Audit work to be performed
High	Auditable unit to be considered in scope for the Internal Audit every year
Significant	Auditable Unit to be considered in scope every second year
Moderate	Auditable Unit to be considered in scope every third year (or every fourth or fifth)
Low	Optional / Voluntary

Prepared By:
Eng. Ahmed Taamah.

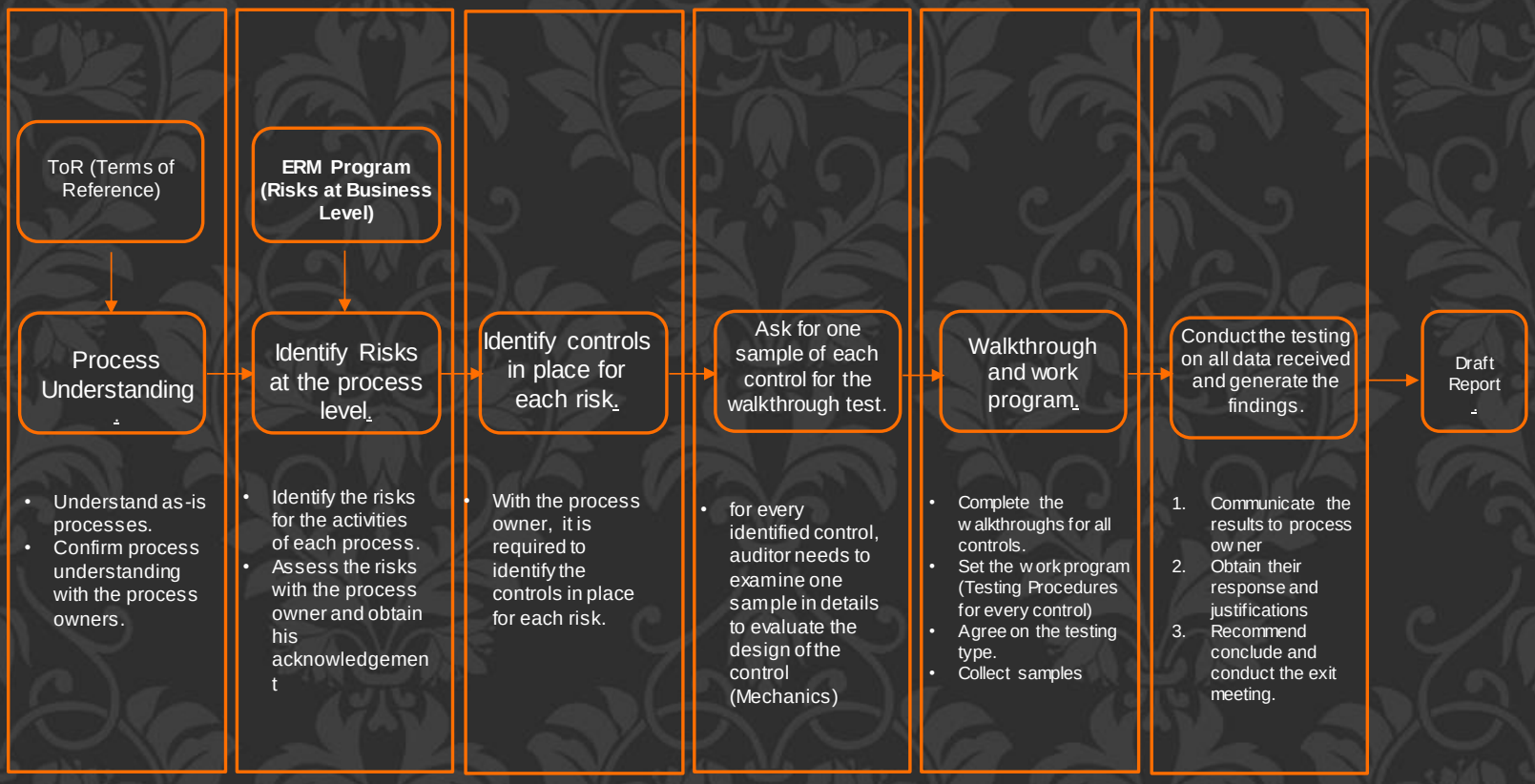
IA Framework - Fieldwork



Prepared By:
Eng. Ahmed Taamah.

IA Framework - Fieldwork

Audit Engagement Process



Prepared By:
Eng. Ahmed Taamah.

Risk Management Process

Asses Risks

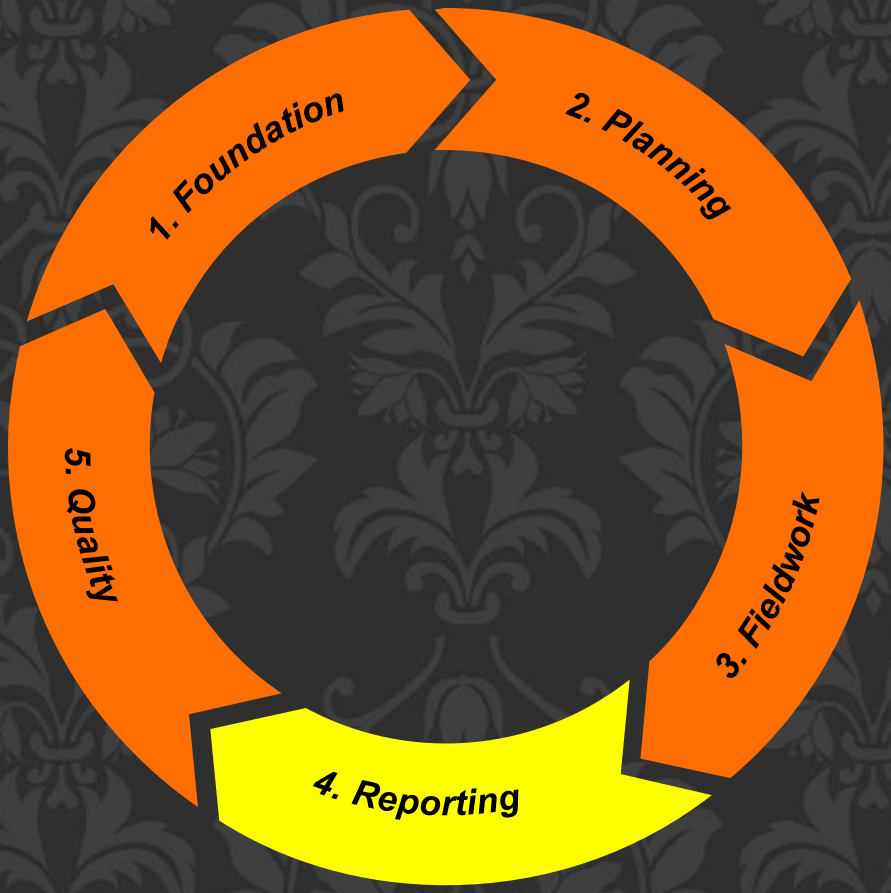
Risk Criteria

To identify the need of any required action/response to risk/controls against each risk identified and analyzed, risk criteria must be defined as follows:

Score	Inherent Risk Level	Required Action
2,3	Low	Rational for not evaluating mitigating controls in place should be documented. Executive Manager review is required.
4,5	Medium	Primary mitigating controls in place should be evaluated to determine residual risk level. General Manager review is mandatory.
6,7	High	All mitigating controls in place must be evaluated to determine residual risk level. The President/VP review is mandatory.
8,9,10	Extreme	All mitigating controls in place must be evaluated to determine residual risk level. The President/VP review is mandatory.

Prepared By:
Eng. Ahmed Taamah.

IA Framework - Reporting



Prepared By:
Eng. Ahmed Taamah.

IA Framework - Reporting

Report	Approved by	To	Timeline/ Frequency	Contents
Audit engagement SoW	Chief Audit Executive	Management and Process Owner	One month before audit commencement	The SoW includes context, objectives, scope of work, initial list of risks, commencement date, deliverables, plan and timelines, budget, team structure, escalation procedure, and initial list of requirements.
Kick off meeting minutes	Chief Audit Executive	Management and Process Owner	In three days after the meeting	The minutes of the kick off meeting includes confirmation of scope, timelines, list of requirements, escalation procedures, key points of contact, roles and responsibilities, and other discussed topics.
Audit closing meeting minutes	Chief Audit Executive	Management and Process Owner	In three days after the meeting	The minutes of the kick off meeting includes confirmation of audit scope, the audit findings, any additional information or explanations from process owner, and the report finalization procedure and timelines.
Draft audit report	Chief Audit Executive	Management and Process Owner	In a week after the closing meeting	The draft report includes an executive summary, overall rating, and detailed findings.
Follow up audit report	Chief Audit Executive	ARC, , Executive Management, Management, and Process Owner	In a week after completing the follow up fieldwork	The follow up audit report includes findings, agreed action plans, agreed implementation timelines, and implementation status.

Prepared By:
Eng. Ahmed Taamah.

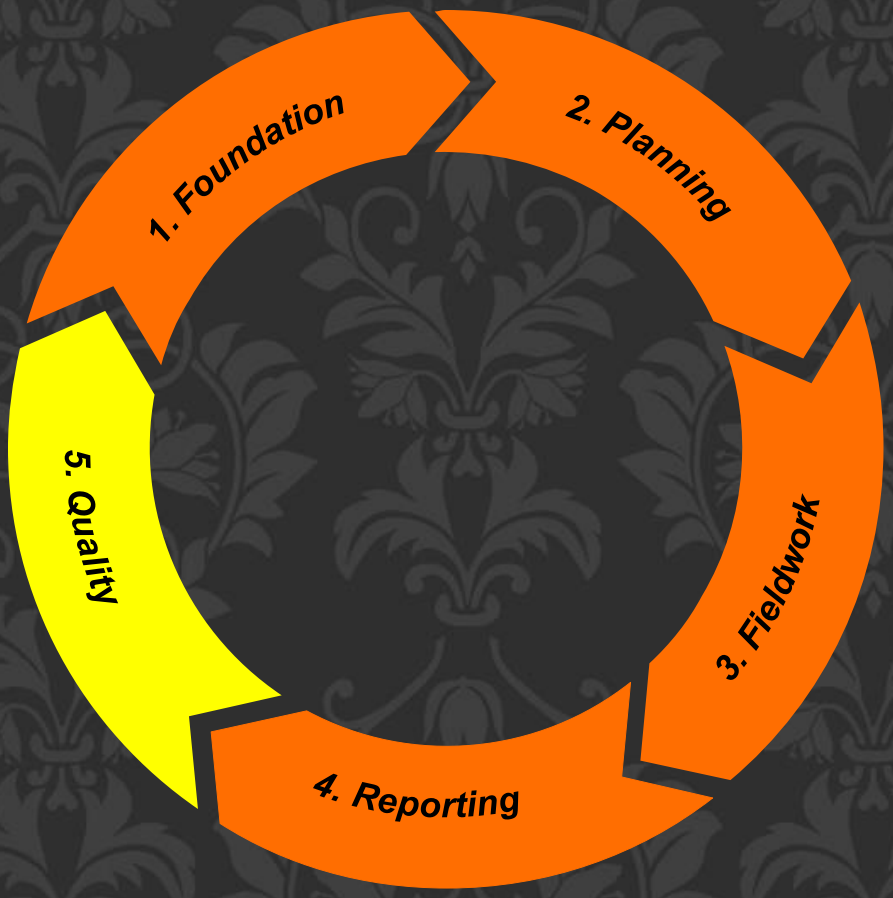
IA Framework - Reporting

Reporting – Follow Up Assurance

Status	Description
Action Plan – in Progress	implementation is ongoing.
Action Plan – Implemented and unverified	Implementation has been completed, however, the auditee needs to provide supporting evidence or the audit team needs to review the supporting evidence provided.
Action Plan - Implemented, verified, and satisfactory	The auditee has completed the implementation and provided supporting evidence. The audit team has reviewed the supporting evidence and concluded implementation is satisfactory. The implementation will be reviewed during the next follow up audit.
Action Plan - Implemented, verified, and unsatisfactory	The auditee has completed the implementation and provided supporting evidence. The audit team has reviewed the supporting evidence and concluded implementation is unsatisfactory.
Action Plan – Canceled	IAD and the auditee agreed to cancel the action plan because changed circumstances have made it irrelevant.
Action Plan - Rejected	Auditee has assumed the risk of not implementing the agreed action plans for the reported finding

Prepared By:
Eng. Ahmed Taamah.

IA Framework - Reporting



Prepared By:
Eng. Ahmed Taamah.

IA Framework - Quality

1300 – Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Internal Assessment

Ongoing Monitoring

- Enforcing standardized work procedures and supervisor's review at various points through out the engagement.
- Solicit feedback immediately following the engagement from the auditee and other stakeholders regarding the efficiency and effectiveness of the internal audit team using the Questionnaire form.

Periodic Self Assessment

A self assessment will be performed every year. to evaluate:

- The quality and supervision of work performed.
- The adequacy and appropriateness of internal audit policies and procedures.
- The ways in which the IAD adds value.
- The achievement of key performance indicators.
- The degree to which stakeholder expectations are met.

External Assessment

Every **five years a**t least by qualified independent assessor or by the CAE with independent external validation to assess:

- The level of conformance with the Standards and the Code of Ethics
- The efficiency and effectiveness of the internal audit activity.
- The extent to which the IAD meets expectations of the board, senior management, and operations management, and adds value to the organization.

Communication OF QAIP

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

Indicating that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing is appropriate only if supported by the results of the quality assurance and improvement program.

Indicating that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing is appropriate only if supported by the results of the quality assurance and improvement program.

Prepared By:
Eng. Ahmed Taamah.

IA Competency Framework

IA Competency Framework

1210 – Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

يجب على المدققين الداخليين أن يمتلكوا المعارف والمهارات والكفاءات الأخرى اللازمة لتنفيذ المسؤوليات الفردية المنوطة بكل منهم. ويجب على نشاط التدقيق الداخلي ككل أن يمتلك أو يحصل على المعارف والمهارات والكفاءات الأخرى اللازمة لتنفيذ المسؤوليات المنوطة به.

Professionalism

- Mission of internal auditing
- Internal audit charter
- Organizational independence
- Individual objectivity
- Ethical behavior
- Due professional care
- Professional development

Performance

- Organizational governance
- Fraud
- Risk management
- Internal control
- Engagement planning
- Engagement fieldwork
- Engagement outcomes

Environment

- Organizational strategic planning and management
- Common business processes
- Social responsibility and sustainability
- Information technology
- Accounting and finance

Leadership & Communication

- Internal audit strategic planning and management
- Audit planning and coordinating assurance efforts
- Quality Assurance and Improvement Program

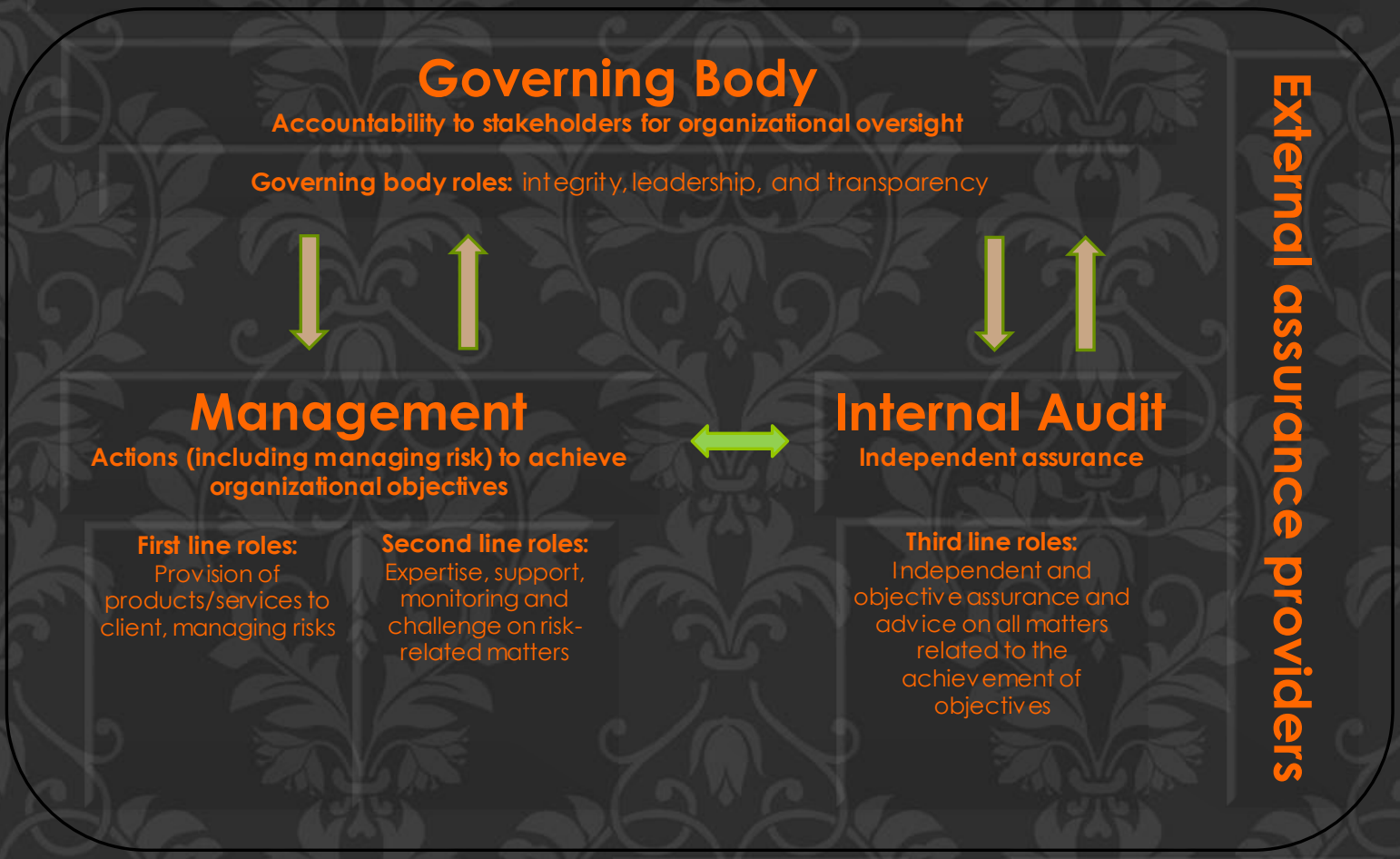
Prepared By:
Eng. Ahmed Taamah.

Role of Internal Auditing in Risk Management

Internal Audit's Core Assurance Roles

The IIA`s Three Lines Model

The IIA`s Three Lines Model



KEY: ↑ Accountability, reporting ↓ Delegating, direction resources, oversight ⟷ Alignment, communication Coordination, collaboration

Prepared By:
Eng. Ahmed Taamah.

The IIA`s Three Lines Model

Management

Actions (including managing risk) to achieve organizational objectives

First line roles:

- leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organization.
- Maintains a continuous dialogue with the governing body, and reports on: planned, actual, and expected outcomes linked to the objectives of the organization; and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control).
- Ensures compliance with legal, regulatory, and ethical expectations.

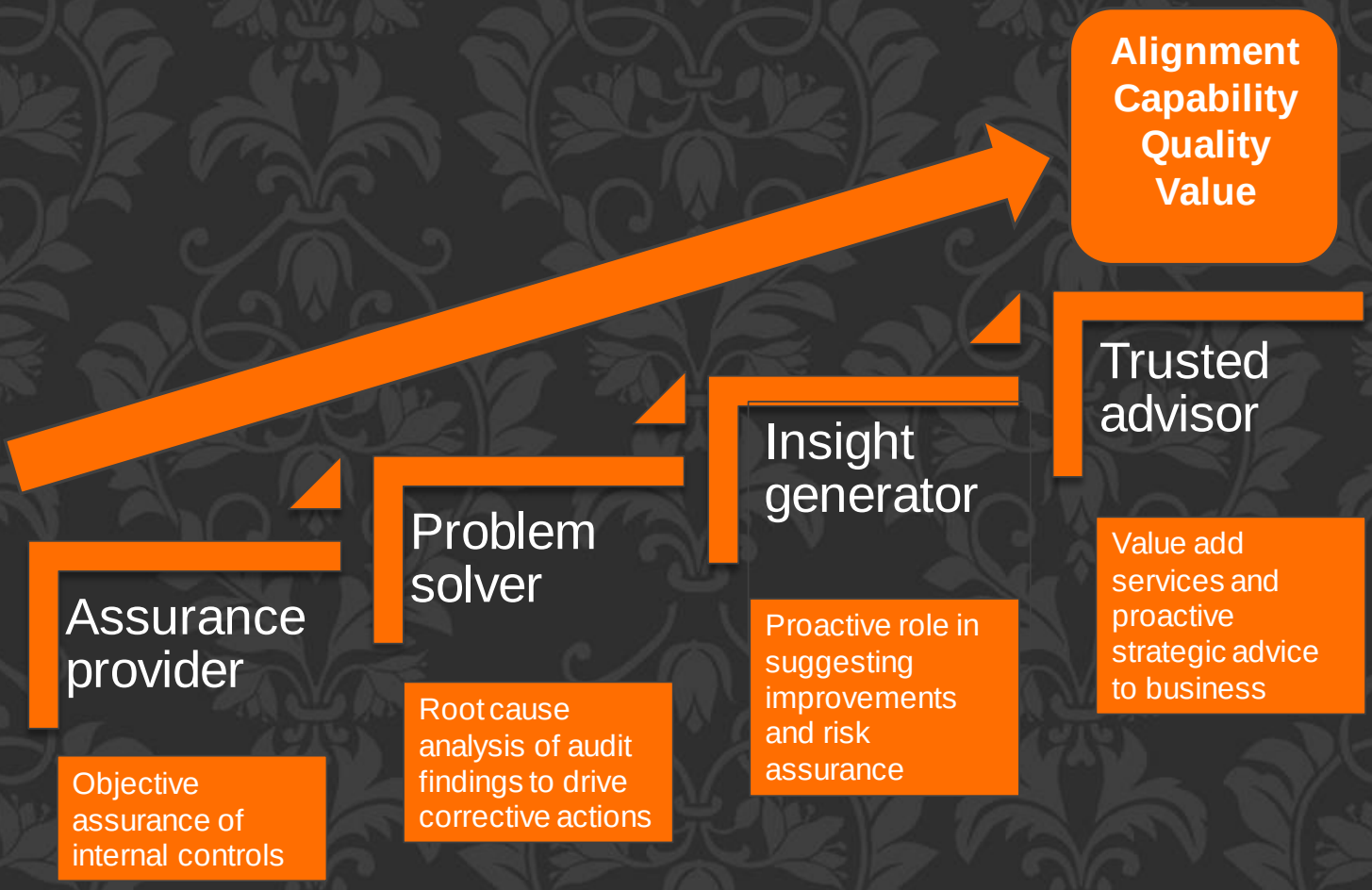
Second line roles:

- Provide complementary expertise, support, monitoring, and challenge related to the management of risk, including:
  1. The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, systems, and entity level.
  2. The achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.
- Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control).

Prepared By:
Eng. Ahmed Taamah.

Operating Continuum

Operating Continuum



Prepared By:
Eng. Ahmed Taamah.

Thank you