

PMG 611

Enterprise Risk Management

Prepared by Dr. Abdullah Jameel Halawany

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 9

Role of Internal Audit in Enterprise
Risk Management



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 9

Session Outline

Internal Audit Standards for
Evaluating Risk

ERM for More Effective
Internal Audit Planning

Risk Tolerance and Building
Internal Audit Plans

Risk-Based Internal Audit
Findings and
Recommendations

Audit And Risk Committee
Coordination



Lecture
9

Introduction



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- **Internal Audit** the “eyes and ears” of management in their role as specialists who visit all areas of an enterprise and report to the audit committee and management on the internal controls status of the operations visited.
- They have historically had ongoing concerns and interests in risk management.

- With limited time and internal auditor resources available for the many areas and activities in an enterprise to review, an internal audit department and its *Chief Audit Executive* (CAE) should focus their time and attention on the riskier areas of the enterprise, deferring other audit review candidates for another time.

- Earlier risk assessment processes used for internal audit planning were often informal and limited in scope.
- An internal audit function with the responsibility for reviews of multiple internal controls and operations throughout an enterprise often would decide which of these often activities to include in an annual audit plan based on concerns expressed by the board of director's audit committee or only on some very informal internal audit risk measures.

- With only very limited knowledge, internal auditors often made quick, cursory decisions on whether some area should be considered high or low risk and then focused their audit planning on the assumed higher risk areas.
- These risk assessment planning approaches were often based on only limited areas of the enterprise, such as an emphasis on operations and processes at the unit's headquarters rather than units covering the entire breadth of the enterprise.

- ***Enterprise Risk Management (ERM)*** encourages a more formal and comprehensive approach to risk-based thinking and encourages internal auditors to give much more attention to risk management when planning for and performing many of their internal audits.
- An internal auditor should be prepared to better understand risks under ERM

Lecture
9

Internal Audit Standards for Evaluating Risk



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- With the wide range of reviews over many areas and processes to be considered in a plan of enterprise internal audits, effective activity planning is a major responsibility of internal audit at all levels.
- The audit committee has responsibility for an enterprise's internal audit function.

- Over the years, internal auditors have frequently asserted that their internal audit planning decisions were based on “risk,” but these assertions were often made without a formal risk assessment approach or a good understanding of the various risks surrounding their enterprises and how those risks would have impacted their audit planning.

- Internal Auditors Standards call for to monitor the effectiveness of the enterprise's risk management system.
- Many enterprises did not have an effective and consistent risk management system prior to COSO ERM.
- This begs the question of how internal audit functions in the past had been able to evaluate the effectiveness of their enterprise's risk management systems when there had been no consistent definition of risk management.

- The earlier IIA standards also did not have a specific section on risk management but discussed the “consideration of risk” as part of the standards for planning the internal audit.
- Our references here are examples for an older, out-of-date set of IIA standards that have been long ago renumbered and superseded with the current standards.
- ERM has changed things here and promotes better internal audit planning and performance at all levels.

Lecture
9

ERM For More Effective Internal Audit Planning



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- **Internal Audit** functions prepare annual audit plans to inform their audit committee and senior management of their planned upcoming costs and internal audit activities.
- **Internal Audit** risk assessments were often not all that formal, and many internal audit planning decisions were heavily dependent on just the strategy and preferences of the senior management.
- **Internal Audit** outsourcing was common.

- Many of the external audit firms probably had better audit planning risk assessment processes than did many internal auditors.
- However, the activities and plans of these outsourced internal auditors did not always consider the risks and objectives of the enterprise but tended to be much more aligned with the goals and often billing revenue objectives of their external auditors.

- “*Audit Universe*” list all auditable entities in the enterprise and to develop a plan that would allow for audits at each of these units over current and future periods.
- This audit universe list gave little consideration to risk—some units would be scheduled for annual internal audits even though past audit findings were minimal and the risks low.
- For many internal audit departments, this audit universe concept broke down because of a lack of audit resources to cover these long lists of auditable entities in any reasonable manner.

- ERM has changed all of this for developing and planning individual internal audits today.
- There is now a need to better consider an enterprise's overall ERM processes as well as specific known audit risks and protective audit requirements when developing an annual internal audit plan.
- *For many other enterprises, an effective internal audit function will often be a key catalyst in launching ERM.*

- There are many areas in enterprise operations where internal audit's presence is needed even though the review area has never been a problem.
- For example, observation may be necessary at some locations because of the large amount of physical assets even though past inventories have been clean with no expected problems.

- The same **concept** for ranking the risk (the relative likelihood of the risk occurring and the significance of that risk to the enterprise) can be used to rank the audit universe list of auditable entities.
- Using three different and linked scoring measures for each entity.
 - *Audit Requirement Score*
 - *Internal Control Significance of the Auditable Entity*
 - *Likelihood of Significant Internal Control Weaknesses*

- **Audit Requirement Score (1 or 0)**
 - **1** if internal audit knows that it will be performing an audit. Often this is a senior management or external audit mandated matter. No matter the level of risk, internal audit will be required to schedule a review over this auditable entity.
 - **0** if internal audit does not have a requirement to perform a review during the current period but may schedule an audit based on its risk assessments and further analysis.
- ***Sets the rule of whether or not an entity should be reviewed by internal audit during a period.***

- ***Internal Control Significance of the Auditable Entity***

- Each item should receive an internal controls significance rating of between 0.01 and 0.99.
- The lower end of this range says that the auditable entity has essentially minimal internal control significance, from an internal audit perspective.
 - Corporate legal department should have its own professional internal control responsibilities, and internal audit should probably not get involved in any direct reviews of such areas. The ranking score would be low.
 - Computer systems applications security, general ledger balancing procedures, or annual physical inventory would receive relatively higher scores.

- *Likelihood of Significant Internal Control Weaknesses*
- Each item again also should receive a rating of between 0.01 and 0.99.
- This rating would be a relative ranking based on internal audit's assessment of the possible number of internal control failures in the area, following this approach:
 - Significant weaknesses from past internal audits would receive a higher score.
 - Lower scores would be assigned to areas with limited internal control exposures. For example, office materials inventories in a shipping department might receive a lower score than other high-value inventory materials.

Lecture 9

ERM For More Effective Internal Audit Planning

- These will provide support for building a risk-ranked internal audit plan.

Control #	Entity Description	Audit Rqmt	I/C Significance	Weakness Likelihood	Prelim Score	Audit Score	Rank
San Jose Finance & Accounting Auditable Entities							
SJ FN 1	Accounts Receivable & Billing	1	0.90	0.90	0.81	1.81	1
SJ FN 2	Purchasing & Accounts Payable	0	0.65	0.60	0.39	0.39	9
SJ FN 3	Financial Reporting	1	0.95	0.60	0.57	1.57	3
SJ FN 4	Intra-Company Transactions	0	0.85	0.65	0.55	0.55	7
San Jose Operations Auditable Entities							
SJ OP 1	Shop Floor Scheduling	0	0.65	0.72	0.47	0.47	8
SJ OP 2	Quality Assurance Procedures	0	0.25	0.55	0.14	0.14	12
SJ OP 3	Packaging & Shipping	0	0.80	0.90	0.72	0.72	5
SJ OP 4	Receiving & Inventory Controls	1	0.85	0.60	0.51	1.51	4
SJ OP 5	Order Processing	0	0.66	0.85	0.56	0.56	6

San Jose Information Technology Auditable Entities

SJ IT 1	IT Continuity Planning	1	0.95	0.80	0.76	1.76	2
SJ IT 2	Applications Development SDLC Procedures	0	0.30	0.85	0.26	0.26	10
SJ IT 3	Service Support Help Desk Operations	0	0.40	0.45	0.18	0.18	11
SJ IT 4	Service Delivery Operations Scheduling	0	0.35	0.35	0.12	0.12	13

Lecture
9

Risk Tolerance and Building Internal Audit Plans



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Using the auditable entity risk assessment approach discussed in the previous section, internal audit and its CAE should next build and develop an annual audit plan for their enterprise based on both a ERM risk-based framework as well as internal audit's responsibility to management to be management's "eyes and ears" reviewing all activities.
- This latter requirement says that an effective internal audit function also must at least consider planning reviews of all areas in an enterprise, even some lower risk areas.

- That internal audit plan should be based on the following general concepts:
- Understand the risk universe surrounding the enterprise, including the number of auditable entities in the enterprise and their estimated risk-related levels significance and probability.
- Based on the mixture of required auditable entities and the risk-ranked units, develop a general audit plan for all areas in the enterprise. This should be discussed with senior management and others.

- Develop time and duration estimates of the internal audit resource requirements to perform internal audits for these various auditable audit candidates.
- Based on current internal audit capacities and capabilities, develop a series of alternative internal audit plans to cover these audit universe auditable entities.
- Review audit plan alternatives with the audit committee and senior management
- and obtain their approvals.

Lecture
9

Risk-Based Internal Audit Findings And Recommendations



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- An internal audit report with its formal findings and recommendations is the major output product from an internal audit function.
- Internal auditors will review internal control procedures, based on internal audit standards, audit department procedures, and the individual auditor's own knowledge, and then will comment on the status of these controls through a formal audit report with its findings and recommendations.

- Unless the internal audit function has some very strong quality assurance processes in place, those audit report recommendations can sometimes cause problems for the people who were audited.
- It is sometimes difficult or impractical to implement the auditor's recommendations because the overall process was not fully considered in the audit report.
- Such that Internal Auditors should better consider risk when planning their internal audits, those same risk considerations should be considered when drafting internal audit reports.

Lecture
9

Audit And Risk Committee Coordination



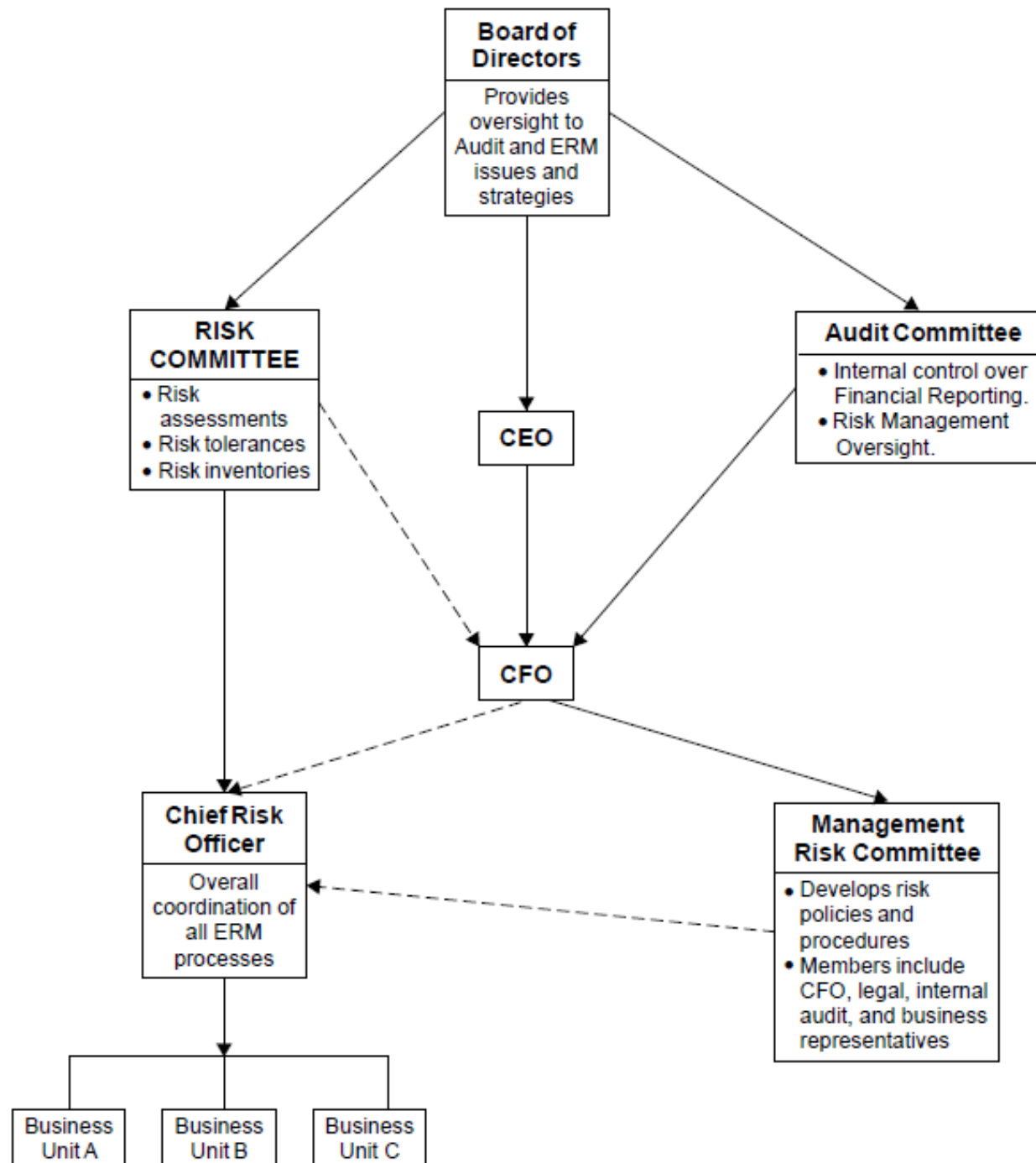
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- The increased level of responsibility for and attention given to audit committees today very much supports the concept of a board risk management committee working in parallel with the audit committee.
- This split allows separate but independent board attention to be given to both audit committee matters and board risk management issues.

- Following Exhibit shows how these two committees might operate in a board corporate governance framework.
- The risk committee and the audit committee would each operate as senior board committees reporting directly to the full board of directors and its chair.

- Both board committees would directly supervise the work of the CFO, with the risk committee having additional responsibilities for the CRO.
- The chart in Following Exhibit shows the CRO reporting to the CFO, with the board risk committee

Lecture 9



Audit And Risk Committee Coordination

Lecture
9

Summary



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- The effective use of ERM should be an important element of internal audit's work.
- In addition to this internal audit planning and performing role, all internal auditors should develop a good understanding of the COSO ERM framework and use it where appropriate in their internal audit activities.
- We have used the example of internal audit as the “eyes and ears” to review and monitor enterprise activities.

Lecture 9

Summary

- When an enterprise embraces a new initiative, such as COSO ERM, not all units will embrace things.
- For some it will be due to a lack of education or communication while for others it will be the often natural resistance to change.
- Auditor who understands ERM should be able to discuss and describe it to others and help them in its appropriate application. Of course, when an internal auditor encounters resistance to new COSO ERM principles, the matter should be discussed in audit reports or raised to the audit committee when appropriate.

- The same **concept** for ranking the risk (the relative likelihood of the risk occurring and the significance of that risk to the enterprise) can be used to rank the audit universe list of auditable entities.
- Using three different and linked scoring measures for each entity.
 - **Audit Requirement Score**
 - **Internal Control Significance of the Auditable Entity**
 - **Likelihood of Significant Internal Control Weaknesses**



- These will provide support for building a risk-ranked internal audit plan.

Control #	Entity Description	Audit Rqmt	I/C Significance	Weakness Likelihood	Prelim Score	Audit Score	Rank
San Jose Finance & Accounting Auditable Entities							
SJ FN 1	Accounts Receivable & Billing	1	0.90	0.90	0.81	1.81	1
SJ FN 2	Purchasing & Accounts Payable	0	0.65	0.60	0.39	0.39	9
SJ FN 3	Financial Reporting	1	0.95	0.60	0.57	1.57	3
SJ FN 4	Intra-Company Transactions	0	0.85	0.65	0.55	0.55	7
San Jose Operations Auditable Entities							
SJ OP 1	Shop Floor Scheduling	0	0.65	0.72	0.47	0.47	8
SJ OP 2	Quality Assurance Procedures	0	0.25	0.55	0.14	0.14	12
SJ OP 3	Packaging & Shipping	0	0.80	0.90	0.72	0.72	5
SJ OP 4	Receiving & Inventory Controls	1	0.85	0.60	0.51	1.51	4
SJ OP 5	Order Processing	0	0.66	0.85	0.56	0.56	6

San Jose Information Technology Auditable Entities

SJ IT 1	IT Continuity Planning	1	0.95	0.80	0.76	1.76	2
SJ IT 2	Applications Development SDLC Procedures	0	0.30	0.85	0.26	0.26	10
SJ IT 3	Service Support Help Desk Operations	0	0.40	0.45	0.18	0.18	11
SJ IT 4	Service Delivery Operations Scheduling	0	0.35	0.35	0.12	0.12	13

Lecture 9

References

- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. *Robert R. Moeller*.



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY