# Ch. 4

# Enterprise Risk Management (ERM)

↳ إدارة المخاطر المؤسسية

↳ من الأعمدة الرئيسية في طلب عمل Management و عمل Auditor

مراجعة :

GRC → تنفيذياً هي من نطاق عمل الإدارة وليس المدقق

G: Governance
R: Risk Management
C: Internal Control

يدرس GRC ولازم أفهمها بعناية فائقة لأنه التركيز في الله فيه / ح يكون عليهم.

Evaluate and improve the effectiveness of GRC

ERM → Not RM

↳ لأنها بتكون على جميع المؤسسة مش لكل قسم لحال.

Scanned by TapScanner

Difinition of ~~ERM~~: Risk:

According Coso: The possibility that an event will occur and aduersly affect the entity ability to achieve its objectives.

← امكانية حدوث حدث يؤثر سلباً (عكسياً) على قدرة الشركة لتحقيق أهدافها

Risks ← objective

← وجود الهدف يؤدي الى وجود مخاطر

← ممكن يكون هناك عدة مخاطر لهدف واحد

As Management ERM needed to:

① UnderStand (Identify) the Risks فهم المخاطر وتعريفها

② Assess the Risks تقييم المخاطر (بناءً على نسبة الحدوث والتأثير معاً)

③ Manag Risks across the organization. التعامل مع المخاطر

Scanned by TapScanner

# Coso ERM Framework (coso II)

← اطار يناسب جميع الشركات مهما اختلف نوعها
← دليل للشركات حاذا يجب أن تفعل لتشكيل نظام ERM فعّال

ERM: is a process, effected by an Entity BOD, Management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its Risk Appetite, to provide reasonable assurance regarding the achievement of the entity objectives.

Process: step / ongoing  خطوات / مستمرة

BOD: Oversight  الاشراف

Mgt:  وضع النظام  [Mgt: التنفيذ في المؤسسة  الجهاز]

across the enterprise: جميع المؤسسة و لا يمكن تطبيقها  - يجب أن تشمل ERM على قسم كامل

Potential events: Risks ← المخاطر

Risk appetite:  the level of risk that the organization is willing to accept.  مقبولة

Provide Reasonable Assurance: الهدف العام من وجود ERM هو اعطاء تأكيد معقول على قدرة الشركة لتحقيق أهدافها.

Scanned by TapScanner

ERM → Risk mitigation not rist elimination

ليس ④

تخفيض — إزالة

[Cost - Benefit] على مبدأ

# COSO ERM CUBE

3D-Matrix

مكعب كوزو

التشغيل — التقارير — الامتثال

4-types of objectives ← كل شيء مبني عليها

8-Interrelated Components ← المكونات المترابطة

تحدث بالترتيب

① البيئة الداخلية

② وضع الأهداف

③ تحديد الأحداث

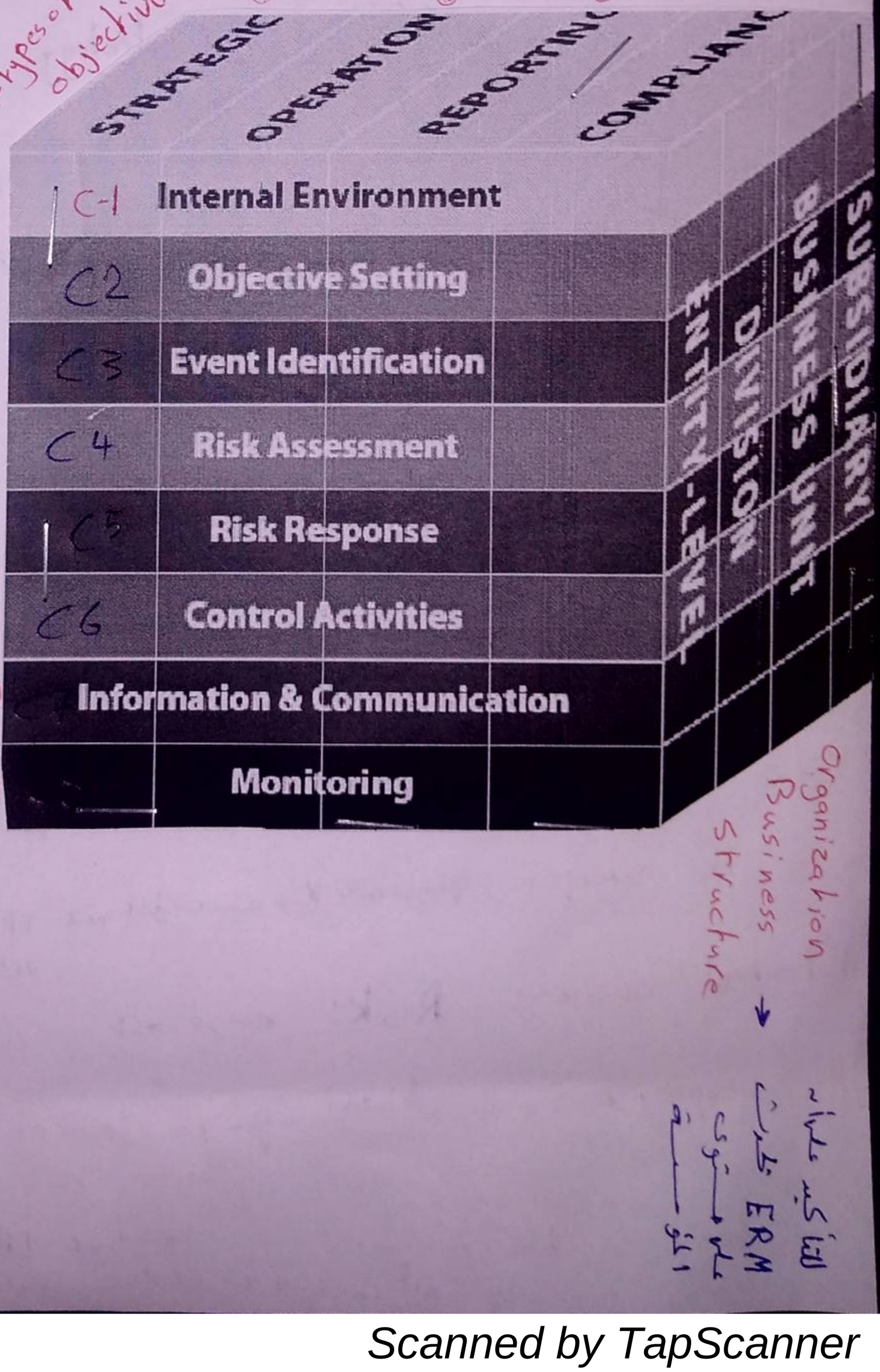
④ تقييم المخاطر

⑤ الاستجابة للمخاطر

⑥ اجراءات الرقابة

⑦ جمع المعلومات وإيصالها

⑧ المراقبة




Organization Structure ← Business ← لتأكيد على أن تحديث ERM يتم من خلال الهيكل التنظيمي

Scanned by TapScanner

# ERM Components:

## C1- Internal Environment البيئة الداخلية

← نقطة البداية لكل المكونات [الأساس Foundation]
← إذا صَلُحَت صَلُحَ النِّظام وإذا فشلت فشل النِّظام

## C1- Include:

① Risk management philosophy فلسفة الإدارة بما يخص إدارة المخاطر

② Risk Appetite [تختلف من شركة لأخرى] شهية المخاطر

③ BOD / Code of Ethics مجلس إدارة فعّال / ميثاق أخلاقي

④ Organization structure الهيكل التنظيمي

⑤ Assignment of authority and responsibility
↳ Job Discription الوصف الوظيفي

⑥ HR policies and procedures

[الهيكل التنظيمي و الوصف الوظيفي]

" صحيتش بال Risks بالمرة
قبل متعمل كار الاشر "
ده شاري الحاج

[① → ⑥] → بكون موثّق يعني بجل ← Documentation

# C2 - Objective Setting

وضع الأهداف

↳ Ch.1

4-types of objectives:

- Strategic objectives
- Operational objectives
- Reporting objectives
- Compliance objectives

← أعداد الأهداف يعتمد على حجم المؤسسة

Precondition? شرط مسبق

C2 شرط مسبق لـ C3 وما يليها

↳ المخرجات من C2 هي وضع وتحديد الأهداف

# C3 - Event Identification

تحديد الأحداث

Potential Events: أحداث متوقع حصولها في المستقبل
[الأحداث اللي إشارات وخلصت بتلزمش]

- Positive effect → Opportunities
- Negative effect → Risks

فرص → Out of scope For IA

مخاطر

↳ هاي اللي بركز عليها لأنه الهدف إني أعمل له فيه ERM مش للفرص.

Scanned by TapScanner

## C4 - Risk Assessment تقييم المخاطر

← تصنيفها حسب خطورتها

يتم تقييم الخطر من جانبين:
- Impact ← تأثير الخطر
- likelihood ← احتمالية حدوث الخطر

يتم التقييم بطريقتين:
- Quantitative ← كمية ← بعمل score / Rating الأرقام
- Qualitative ← نوعية ← بعمل تصنيف نوعي [High, Medium, low] [H, M, L]

### Risk Rating (RR) / Risk Score

- Quantitative → Average $\left[\frac{\text{Impact} + \text{likelihood}}{2}\right]$
- Qualitative → Matrix / احتمالات: HM, HL, ML

## C5 - Risk Response الاستجابة للمخاطر

الاستجابة للمخاطر تعتمد على:

① Risk Rating

level of Risks:

- Inherent risk: الخطر الفطري

Gross, before any management action (control)

← هو الخطر الذي يمكن أن يحدث وبدون تدخل الإدارة [الخطر قبل وضع control عليه]

Scanned by TapScanner

Residual risk:

Net, after management action(control)

الخطر المتبقي بعد وضع اجراءات رقابية.

## 5- Risk Response الاستجابة للمخاطر

الاستجابة للمخاطر تعتمد على:

① Risk Rating (RR)

② Cost and benefit يجب أن تتجاوز المنفعة التكلفة

③ Residual Risk and risk tolerance

الخطر المقبول ← acceptable risk

risk tolerance ← Residual risk يعني بعد الوصول

Types of risk responses [استراتيجيات] طرق الاستجابة للمخاطر

- Avoidance التجنب ← الباب اللي يجيلك منه الريح سدّه واستريح
- Sharing المشاركة ← نقل الخطر أو مشاركته مع أطراف أخرى مثل التأمين أو outsorcing
- Acceptance القبول ← Take No action
- Reduction تخفيض ← Impact or likelihood يأثر على من خلال وضع controls

← عادة يكون عندي Reduction يلزم أضع إجراءات رقابية فعالة [IC]

Scanned by TapScanner

## C6 - Control Activities — النشاطات الرقابية

↳ Policies and procedures — سياسات واجراءات

لضمان تنفيذ الاستجابة للمخاطر

Reduction — المخاطر اللي قررت اعملها

Examples

① Top Level Reviews: Actual Budget Comparison
↳ على مستوى الوحدة

② Direct Functional or Activity Management Review
↳ Department ~~Department~~ — على مستوى

③ physical Controls: ... مثل الكاميرات / أقفال
↳ اجراءات رقابية مادية

④ SOD : A / R / C / R
↳ Segregation of Duties — فصل المهام

[يجب فصل المهام المتعلقة بعملية معينة — مش لازم تكون بيد شخص واحد عشان ما يقدر يقفل أخطاء ويداري عليها]

A: Authorization — الموافقة أو التفويض على القيام بحركة ما
R: Recording — التسجيل
C: Custody — العهدة → مثل أمين العهدة → المسؤول عن Asset بشكل مادي
R: Reconciliations — المطابقات

↳ إذا كانت جميع هاي المهام على شخص واحد بإمكانه يعمل Fraud ويغطي على حالو بسهولة لذلك لا يجوز جميع هاي المهام مع شخص واحد.

Scanned by TapScanner

C7- Information and Communication

← جمع المعلومات وإيصالها للمهتمين عشان يقدروا ينجزوا مسؤولياتهم

Forms of communication
- e-mails
- Memos
- ⋮

C8- Monitoring المراقبة

ERM فحص ما إذا كان نظام [Assess]
- existence ← موجود
- Functioning ← يعمل

~~Monitoring ERM~~

2-methods of monitoring:
- Self Assessment : Ongoing monitoring
- separate evaluation تقييم منفصل
  - Internal Auditor
  - External Auditor

Scanned by TapScanner

## Risk Management and Compliance Function

دائرة إدارة المخاطر والامتثال

- Chief Risk Officer (CRO) يرأسها
  - Senior management position

نقطة اتصال لتسهيل انشطة ادارة المخاطر
Focal point to facilitate RM activities

CEO → يقيّم → CRO
عمل

IAF مستقل CRO ويتم تقييم

هاي الدائرة هي اللي بتنفذ كل ERM إنما هي الجهة الاشرافيه

ERM → تتبنى مسؤولية حماية على كل الدوائر.

Scanned by TapScanner

# ERM Responsibilities ?

BOD : Oversight

Management: Developing and maintaning the ERM

Internal Auditors: evaluate and provide reasonable assurance and recommendations Regarding on Design Adequcy and Operating Effectiveness of the ERM system.

RUBA MTOOR

Scanned by TapScanner