إطار
COSO ERM
VS
ISO 31000

المكونات الخمسة لإطار COSO ERM

١- الحوكمة والثقافة (Governance & Culture)

- تحديد مسؤوليات الرقابة وتحديد الأدوار والمسؤوليات.
- تحديد الهيكل التنظيمي وتفويض السلطات.
- تحديد القيم الأساسية والسلوكيات المرغوبة.
- جذب وتطوير والحفاظ على الكفاءات.
- تعزيز الوعي بالمخاطر داخل الثقافة التنظيمية.

٢- تحديد الاستراتيجية والأهداف (Strategy & Objective-Setting)

- تحليل البيئة الخارجية والداخلية لتحديد المخاطر.
- تحديد شهية المخاطر وربطها بالاستراتيجية.
- تقييم الاستراتيجيات البديلة وتأثيراتها على المخاطر.
- تحديد الأهداف التي تدعم تحقيق الاستراتيجية.

٣- الأداء (Performance)

- تحديد وتقييم المخاطر التي قد تؤثر على تحقيق الأهداف.
- تحديد أولويات المخاطر بناءً على شدتها وتأثيرها.
- تحديد استجابات المخاطر المناسبة (تجنب، تقليل، نقل، قبول).
- تقييم مدى تحمل المخاطر على مستوى المحفظة.
- تحديد مؤشرات الأداء الرئيسية لمراقبة المخاطر

٤- المراجعة والتعديل (Review & Revision)

- مراجعة الأداء مقابل الأهداف المحددة.
- تحديد التغيرات في السياق الداخلي والخارجي.
- تقييم فعالية إدارة المخاطر وتحديد التحسينات اللازمة.

٥- المعلومات والتواصل والإبلاغ (Information, Communication, & Reporting)

- تحديد المعلومات ذات الصلة بإدارة المخاطر وجمعها.
- التواصل الفعال للمعلومات المتعلقة بالمخاطر داخليًا وخارجيًا.
- إعداد تقارير دورية عن المخاطر لدعم اتخاذ القرار.

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

العلاقة بين المكونات والمبادئ

يحتوي إطار COSO ERM على 20 مبدأ موزعة على المكونات الخمسة المذكورة أعلاه. هذه المبادئ تمثل الممارسات الأساسية التي يجب أن تتبعها المؤسسة لضمان إدارة فعالة للمخاطر.

الفوائد الرئيسية لتطبيق COSO ERM

- دمج إدارة المخاطر مع الاستراتيجية والأداء: يساعد الإطار المؤسسات على ربط إدارة المخاطر بأهدافها الاستراتيجية، مما يعزز من قدرتها على تحقيق هذه الأهداف.
- تحسين عملية اتخاذ القرار: من خلال توفير معلومات دقيقة وموثوقة عن المخاطر، يمكن للإدارة اتخاذ قرارات أفضل وأكثر استنارة.
- تعزيز الشفافية والمساءلة: يوفر الإطار هيكلًا واضحًا لتحديد الأدوار والمسؤوليات، مما يعزز من الشفافية والمساءلة داخل المؤسسة.
- تحسين القدرة على التكيف مع التغيرات: من خلال المراجعة والتعديل المستمرين، يمكن للمؤسسة التكيف بسرعة مع التغيرات في البيئة الداخلية والخارجية.

ISO 31000:2018

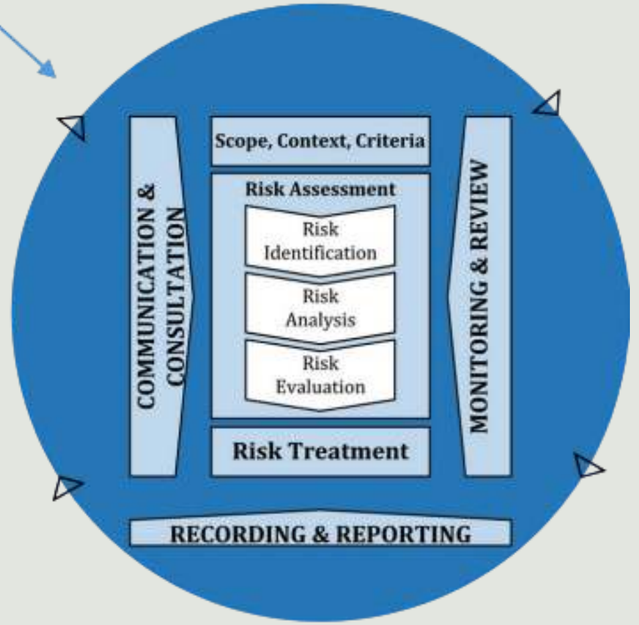
هو معيار دولي يوفر مبادئ وإطارًا وعملية لإدارة المخاطر.

يهدف إلى مساعدة المؤسسات على دمج إدارة المخاطر في جميع أنشطتها،

بما في ذلك اتخاذ القرار والتخطيط والعمليات اليومية.

Principles (clause 4)

Framework (clause 5)



Process (clause 6)

المكونات الرئيسية للمعيار

١- المبادئ (Principles)

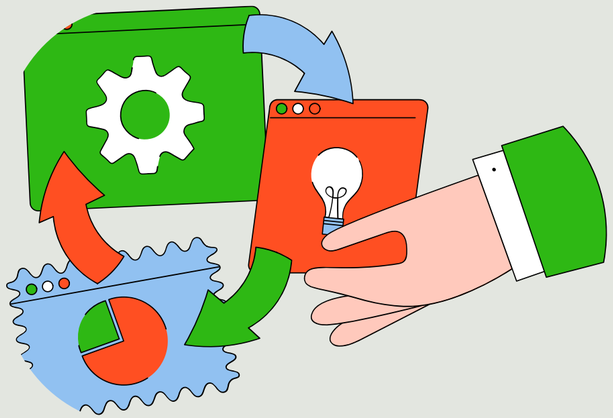
تُشكل المبادئ الأساس الذي يُبنى عليه إدارة المخاطر الفعالة. تشمل هذه المبادئ:

- التكامل (Integrated): يجب أن تكون إدارة المخاطر جزءًا لا يتجزأ من جميع أنشطة المؤسسة.
- الهيكلية والشمولية (Structured and Comprehensive): ينبغي أن تكون العملية منهجية وشاملة لضمان نتائج متسقة.
- التخصيص (Customized): يجب أن تتناسب إدارة المخاطر مع السياق الداخلي والخارجي للمؤسسة.
- الشمولية (Inclusive): ينبغي إشراك أصحاب المصلحة المناسبين لضمان مراعاة جميع وجهات النظر.
- الديناميكية (Dynamic): يجب أن تكون إدارة المخاطر قادرة على التكيف مع التغيرات.
- أفضل المعلومات المتاحة (Best Available Information): ينبغي أن تستند القرارات إلى معلومات موثوقة وحديثة.
- العوامل البشرية والثقافية (Human and Cultural Factors): يجب أن تأخذ إدارة المخاطر في الاعتبار السلوكيات والثقافة التنظيمية.
- التحسين المستمر (Continual Improvement): ينبغي أن تسعى المؤسسة باستمرار لتحسين إدارة المخاطر.

٢- الإطار (FRAMEWORK)

يوفر الإطار الهيكل التنظيمي والنهج الذي يضمن دمج إدارة المخاطر في جميع مستويات المؤسسة. يشمل ذلك:

- القيادة والالتزام (Leadership and Commitment): يجب أن يُظهر القادة التزامًا قويًا بإدارة المخاطر.
- التكامل (Integration): ينبغي دمج إدارة المخاطر في جميع العمليات والأنشطة.
- التصميم (Design): يجب تصميم إطار إدارة المخاطر بما يتناسب مع احتياجات المؤسسة.
- التنفيذ (Implementation): ينبغي تنفيذ إطار العمل بشكل فعال عبر المؤسسة.
- التقييم والتحسين (Evaluation and Improvement): يجب تقييم الأداء وتحسينه بانتظام.



٣- العملية (PROCESS)

تُحدد العملية الخطوات العملية لإدارة المخاطر، وتشمل:

- التواصل والتشاور (Communication and Consultation): التفاعل مع أصحاب المصلحة لضمان فهم المخاطر.
- تحديد السياق (Establishing the Context): فهم البيئة التي تعمل فيها المؤسسة.
- تقييم المخاطر (Risk Assessment): يشمل تحديد المخاطر، تحليلها، وتقييمها.
- معالجة المخاطر (Risk Treatment): تحديد وتنفيذ خيارات لمعالجة المخاطر.
- المراقبة والمراجعة (Monitoring and Review): متابعة فعالية إدارة المخاطر وتحديثها حسب الحاجة.
- التسجيل والإبلاغ (Recording and Reporting): توثيق نتائج إدارة المخاطر وتقديم التقارير المناسبة.

الهدف من ISO 31000:2018

يهدف المعيار إلى تمكين المؤسسات من:

- تحسين عملية اتخاذ القرار من خلال فهم أفضل للمخاطر.
- تحقيق الأهداف التنظيمية بكفاءة وفعالية.
- تعزيز المرونة والقدرة على التكيف مع التغيرات.
- تعزيز الثقة بين أصحاب المصلحة من خلال إدارة فعالة للمخاطر.

مقارنة بين ISO 31000 وCOSO ERM

الجانب	ISO 31000:2018	COSO ERM 2017
المنهجية	مرنة وقابلة للتخصيص	هيكلية وموجهة نحو الأداء
التركيز	دمج إدارة المخاطر في جميع الأنشطة	ربط المخاطر بالاستراتيجية والأداء
القابلية للتطبيق	جميع أنواع المؤسسات	مناسب أكثر للمؤسسات الكبيرة والمعقدة
المبادئ	8 مبادئ	20 مبدأ
الإطار	مرن وقابل للتكيف	هيكل محدد بمكونات واضحة
العملية	خطوات محددة لإدارة المخاطر	موجهة نحو الأداء والمراجعة

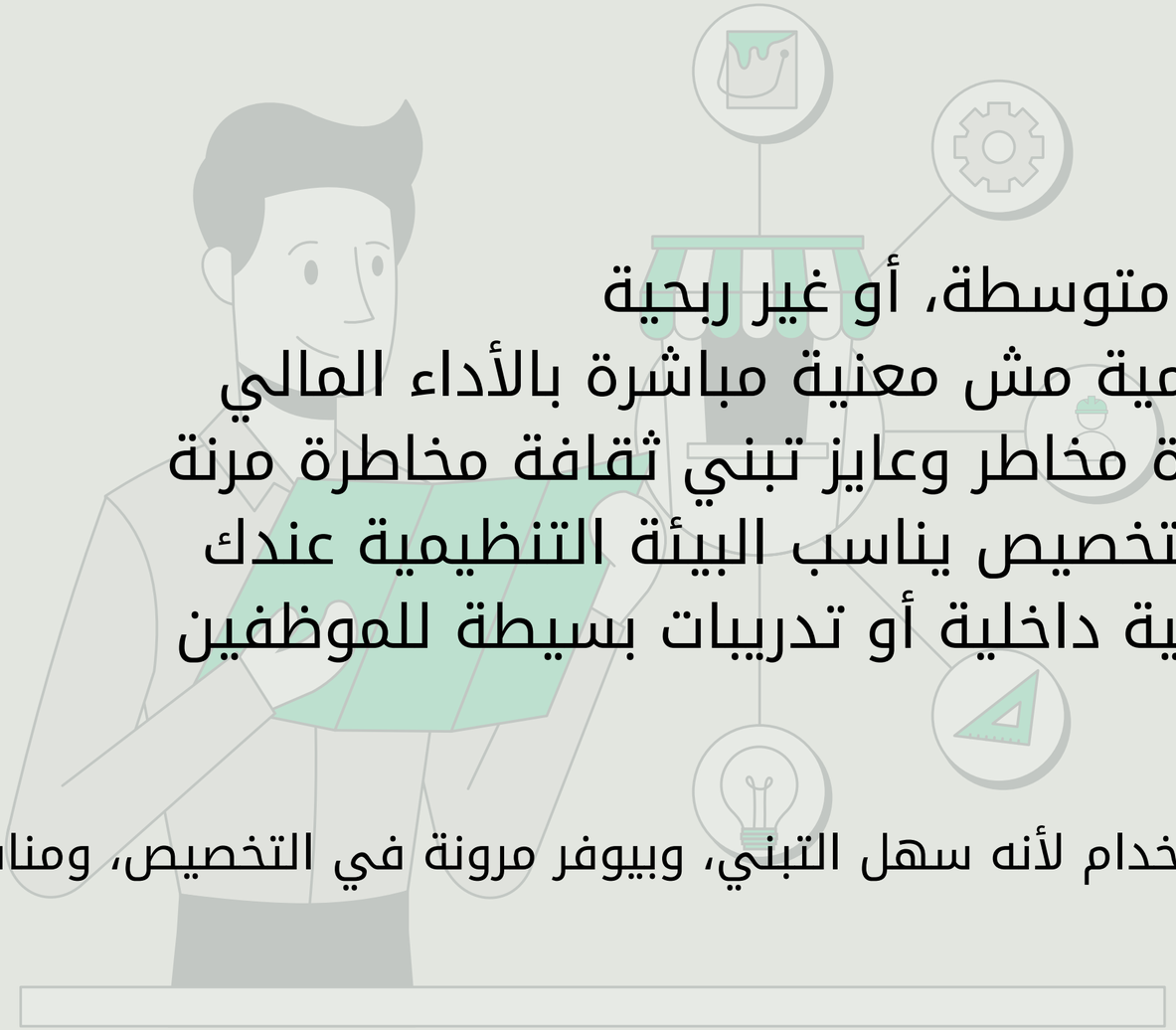
امتى تستخدم COSO؟

لو شركتك:

- مؤسسة مالية أو استثمارية (زي بنك أو صندوق استثمار)
- وبتشتغل وفقًا لإطار حوكمة واضح فيه مجلس إدارة ولجان مراجعة ومخاطر
- وفيها ربط مباشر بين الأهداف الاستراتيجية والأداء المالي
- ومطلوب منك تصدر تقرير حوكمة، تقرير أداء، أو تقرير مخاطر سنوي
- وعايز تبني مصفوفة شهية للمخاطر (Risk Appetite) مرتبطة بالأهداف التشغيلية

يبقى COSO هو الأنسب ليك لأنه بيربط كل عناصر المخاطر بالاستراتيجية والحوكمة بشكل منهجي.

امتى تستخدم ISO 31000؟

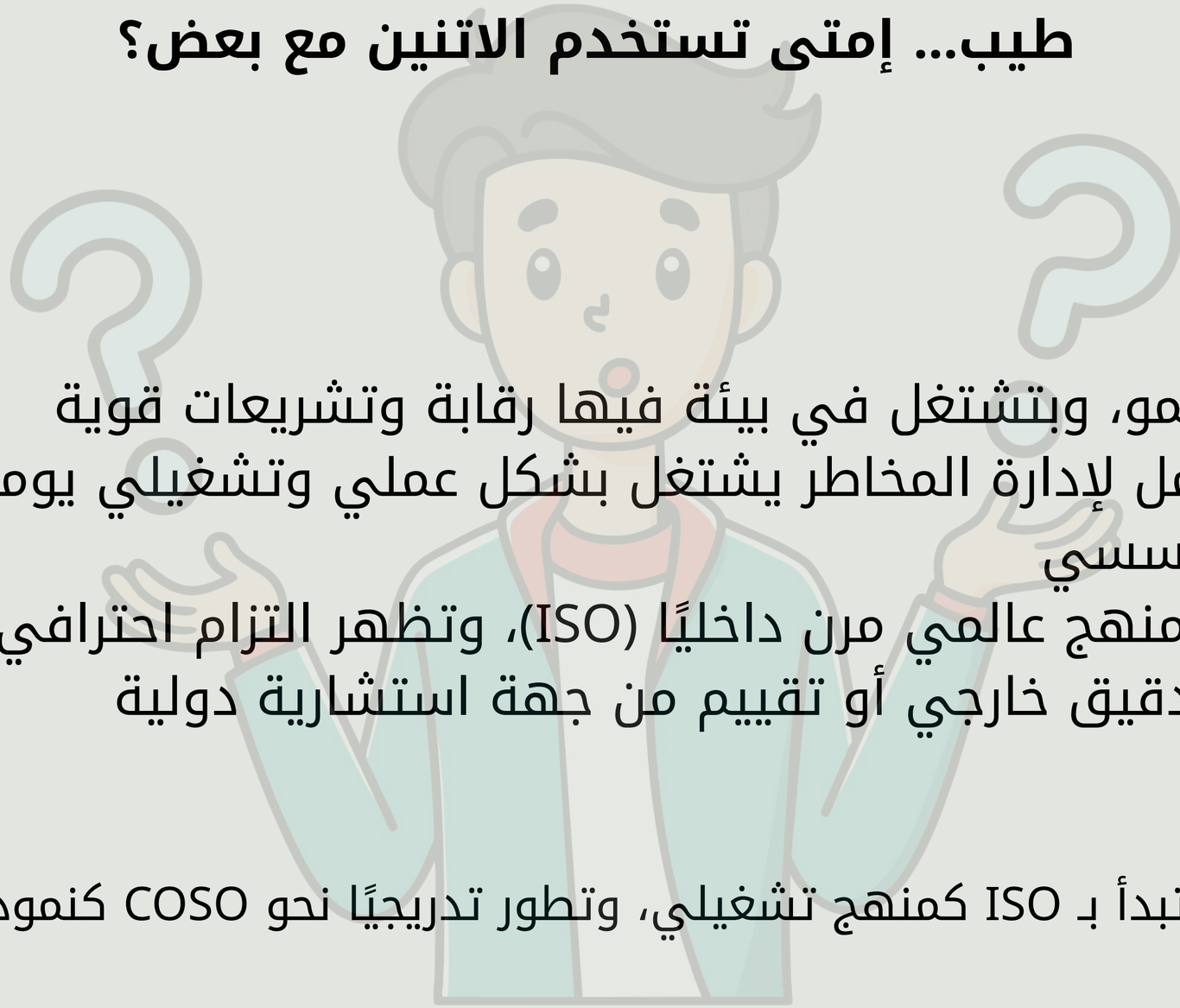


أما لو:

- شركتك ناشئة، صغيرة، متوسطة، أو غير ربحية
- أو جهة حكومية أو خدمية مش معنية مباشرة بالأداء المالي
- ولسه بتبدأ تأسس إدارة مخاطر وعايز تبني ثقافة مخاطرة مرنة
- وعايز إطار عام سهل التخصيص يناسب البيئة التنظيمية عندك
- وبتحتاج تنفذ ورش توعية داخلية أو تدريبات بسيطة للموظفين

هنا ISO 31000 هو الأذكى للاستخدام لأنه سهل التبني، وبيوفر مرونة في التخصيص، ومناسب لأي حجم أو نوع مؤسسة.

طيب... إمتى تستخدم الاتنين مع بعض؟



لو شركتك:

- كبيرة أو سريعة النمو، وبتشتغل في بيئة فيها رقابة وتشريعات قوية
- وبتبني نظام متكامل لإدارة المخاطر يشتغل بشكل عملي وتشغيلي يومي، وفي نفس الوقت مربوط بالحكم المؤسسي
- وعايز تمشي على منهج عالمي مرن داخليًا (ISO)، وتظهر التزام احترافي خارجيًا (COSO)
- أو بتجهّز نفسك لتدقيق خارجي أو تقييم من جهة استشارية دولية

يبقى الحل الأمثل هو: تبدأ بـ ISO كمنهج تشغيلي، وتطور تدريجيًا نحو COSO كنموذج حوكمي استراتيجي.

Thank You

mohammed fathy elzok

+201065275555