



دليل مهني

GRC بين النظريات والتطبيق

دليل عملي لتطوير الحوكمة وإدارة المخاطر والالتزام في الشركات

إعداد: Ahmad Abumaneï | FREE CONSULTANT

التاريخ: تموز 2026 | الإصدار: 3.1

وثيقة مهنية عامة | FC-GRC-GD-001

معلومات الوثيقة

وثيقة مهنية استرشادية صادرة عن منصة Free Consultant، تُحدَّث دوريًا عند صدور تعديل جوهري على أحد المعايير أو التشريعات المشار إليها.

بيانات التعريف

البند	التفصيل
عنوان الوثيقة	GRC بين النظريات والتطبيق: دليل عملي لتطوير الحوكمة وإدارة المخاطر والالتزام
رمز الوثيقة	FC-GRC-GD-001
نوع الوثيقة	دليل مهني استرشادي
الإصدار	1.0
التاريخ	تموز (يوليو) 2026
النطاق الجغرافي	الأردن ودول مجلس التعاون الخليجي، مع قابلية التكيف لبيئات أخرى
المرجعيات الأساسية	ISO 37000:2021 · ISO 31000:2018 · ISO 37301:2021 · COSO ERM 2017 · OECD IIA Three Lines 2020 · GIAS 2024 · 2023
إعداد ومراجعة	أحمد أبو منيع
التصنيف	وثيقة مهنية عامة

سجل الإصدارات

الإصدار	التاريخ	وصف التعديل	أعدّه
0.1	حزيران 2026	مسودة أولية للمراجعة الداخلية	أحمد أبو منيع
1.0	تموز 2026	إصدار أول معتمد للنشر	أحمد أبو منيع

حدود الاستخدام

الإشارات الواردة إلى التشريعات والتعليمات الرقابية المذكورة بغرض التوجيه لا الحصر، وهي عرضة للتعديل. تظل مسؤولية التحقق من النص النافذ وقت التطبيق على عاتق المنشأة ومستشاريها. واعتماد أي من النماذج الواردة هنا لا يُنشئ بذاته امتثالاً تنظيمياً ما لم يُطبَّق فعلياً ويُوَثَّق ويُراجَع.

المحتويات

1	معلومات الوثيقة
1	بيانات التعريف
1	سجل الإصدارات
2	المحتويات
4	تمهيد
5	1. مدخل إلى الدليل
5	1-1 الغرض
5	2-1 النطاق
5	3-1 الجمهور المستهدف
5	4-1 حدود الدليل وإخلاء المسؤولية
6	2. الإطار المفاهيمي The Conceptual Frame
6	1-2 من أين جاء المصطلح؟
6	2-2 تعريف المكونات الثلاثة
6	1-2-2 الحوكمة (Governance)
6	2-2-2 إدارة المخاطر (Risk Management)
6	3-2-2 الالتزام (Compliance)
7	3-2 ما الذي يجعل GRC أكثر من مجرد جمع ثلاثة مكونات؟
8	3. المكون الأول: الحوكمة Governance
8	1-3 المرتكزات المعيارية
8	2-3 مكونات منظومة الحوكمة
9	3-3 مبدأ التناسب في التصميم
10	4. المكون الثاني: إدارة المخاطر Risk Management
10	1-4 العمود الفقري: ISO 31000:2018
10	1-1-4 الخطأ المنهجي الأكثر تكرارًا
11	2-4 العدسة الاستراتيجية: COSO ERM 2017
11	3-4 الرغبة في المخاطرة: بناء تدريجي لا شعاري
12	4-4 سجل المخاطر ومؤشرات المخاطر الرئيسية
13	5. المكون الثالث: الالتزام Compliance
13	1-5 المرجعية المعيارية
13	2-5 عالم الالتزام وسجل الالتزامات
13	3-5 مخاطر عدم الالتزام
15	6. العلاقة بين المكونات الثلاثة The Integration Logic
15	1-6 من التجاور إلى التكامل
16	2-6 سلسلة الوصل: من الهدف إلى التأكيد

16.....	3-6 نموذج الخطوط الثلاثة بوصفه العمود الفقري
17.....	4-6 الشروط الثلاثة للتكامل الفعلي
17.....	5-6 تكلفة غياب التكامل
19.....	7. من النظرية إلى التطبيق Implementation Methodology
19.....	1-7 المرحلة صفر: التفويض والرعاية
19.....	2-7 المرحلة الأولى: تشخيص الوضع الراهن
19.....	3-7 المرحلة الثانية: تصميم الإطار المتكامل
19.....	4-7 المرحلة الثالثة: البناء والتطبيق التجريبي
20.....	5-7 المرحلة الرابعة: التعميم والأتمتة
20.....	6-7 المرحلة الخامسة: الترسخ والتحسين
21.....	8. قياس نضج منظومة GRC Maturity Assessment
21.....	1-8 المستويات الخمسة
21.....	2-8 أبعاد القياس التسعة
23.....	9. مؤشرات قياس أداء المنظومة GRC Performance Indicators
24.....	10. تحديات التطبيق ومعالجتها Implementation Challenges
25.....	11. تطبيق موجز: من التشخيص إلى الأثر
25.....	1-11 وصف الحالة
25.....	2-11 ما أظهره التشخيص
25.....	3-11 الأولويات التي حُددت
25.....	4-11 الأثر بعد اثني عشر شهرًا
26.....	12. خلاصة وتوصيات
26.....	1-12 أول ثلاثين يومًا
27.....	ملحق (أ): قائمة تحقق جاهزية منظومة GRC
29.....	ملحق (ب): مصفوفة أدوار المنظومة
30.....	ملحق (ج): المسرد الثنائي اللغة
31.....	ملحق (د): المراجع المعيارية
31.....	د-1 الحوكمة
31.....	د-2 إدارة المخاطر
31.....	د-3 الالتزام والنزاهة
31.....	د-4 التدقيق الداخلي
31.....	د-5 مرجع المفهوم
32.....	نبذة عن المُعدِّ

تمهيد

في كل ارتباط مهني تقريباً، يتكرر المشهد ذاته. تجد لدى المنشأة لائحة حوكمة معتمدة من المجلس، وسجل مخاطر أعد في ورشة عمل قبل عامين، ومصفوفة التزام تحتفظ بها الدائرة القانونية في ملف منفصل. ثلاث وثائق سليمة كل واحدة على حدة، ولا تتحدث أي منها مع الأخرى. المخاطر المسجلة لا تظهر في خطة التدقيق، والالتزامات التنظيمية ليست ضمن سجل المخاطر، والمجلس يتلقى ثلاثة تقارير في ثلاثة قوالب لا يمكن جمعها في صورة واحدة.

هذا بالضبط ما يعالجه مفهوم GRC. ليست الفكرة إضافة طبقة إدارية رابعة فوق الثلاث القائمة، بل ربطها في منظومة واحدة تشترك في اللغة والبيانات ودورة الاعتماد. المكاسب المتحققة من هذا الربط ملموسة: تقليل ازدواجية العمل بين وظائف الخط الثاني والثالث، وتخفيف ما يُعرف بارهاق التأكيد لدى الوحدات التشغيلية، وقبل ذلك تمكين المجلس من رؤية واحدة متسقة للمخاطر التي تهدد أهدافه.

يقوم هذا الدليل على مبدأين. الأول أن كل توصية فيه مسنودة إلى معيار دولي مُسمى بالبند أو المبدأ، لا إلى «أفضل الممارسات» بصيغتها المرسلّة. والثاني أن التناسب مبدأ تصميمي: ما يصلح لبنك خاضع لتعليمات البنك المركزي لا يصلح بحرفيته لشركة عائلية بخمسين موظفاً، ولذلك يُشار في كل موضع إلى ما هو إلزامي وما هو استرشادي وما يخضع لاجتهاد الإدارة.

وأخيراً، فإن ما يميز الأدلة التي تُطبّق عن تلك التي تُحفظ في الأدراج هو وجود أدوات جاهزة للاستخدام. لذلك ضُمّنت الملاحق قائمة تحقق للجاهزية، ومصفوفة أدوار، ومسرّداً ثنائي اللغة، بحيث يمكن للقارئ أن يبدأ العمل من صفحة الملحق مباشرة إن أراد.

كيف تقرأ هذا الدليل

إن كنت عضو مجلس إدارة أو لجنة تدقيق أو مخاطر: ابدأ من الفصل السادس (العلاقة بين المكونات) ثم الفصل الثامن (نضج المنظومة).

إن كنت مسؤول مخاطر أو التزام: الفصول الرابع والخامس والسابع هي مادتك الأساسية.

إن كنت مدير تدقيق داخلي: راجع الفصل السادس لموقع التدقيق في المنظومة، والفصل التاسع لمؤشرات القياس.

إن كنت تبني المنظومة من الصفر: اتبع الفصل السابع بالتسلسل، واستخدم الملحق (أ) للتشخيص الأولي.

1. مدخل إلى الدليل

1-1 الغرض

- يهدف الدليل إلى تزويد المنشأة بإطار مفاهيمي دقيق وأدوات تنفيذية لبناء منظومة متكاملة للحوكمة وإدارة المخاطر والالتزام، وتحديدًا: توضيح المفاهيم الثلاثة بتعريفات منضبطة مسنودة إلى معايير دولية، وإزالة الخلط الشائع بينها وبين وظائف مجاورة مثل التدقيق الداخلي والرقابة الداخلية.
- بيان طبيعة العلاقة بين المكونات الثلاثة: أين تتقاطع، وأين تنفصل، وأين يؤدي الخلط بينها إلى فجوة رقابية.
- تقديم منهجية تنفيذ متدرجة قابلة للتطبيق خلال 18 شهرًا، مع مخرجات محددة لكل مرحلة.
- توفير أدوات قياس: نموذج نضج، ومؤشرات أداء، وقائمة تحقق للجاهزية.

2-1 النطاق

- يغطي الدليل الطبقة المؤسسية للمنظومة: التصميم، والأدوار، والعمليات، والتقارير، والقياس. ولا يتناول بالتفصيل ما يلي، ويُحال بشأنه إلى أدلة متخصصة:
- منهجيات القياس الكمي المتقدم للمخاطر (محاكاة مونت كارلو، القيمة المعرضة للخطر، نموذج FAIR).
- المتطلبات القطاعية العميقة (بازل للبنوك، الملاءة المالية لشركات التأمين، متطلبات الهيئة الوطنية للأمن السيبراني).
- اختيار وتطبيق أنظمة GRC البرمجية وتقييم مورديها.

3-1 الجمهور المستهدف

جدول (1-1): الجمهور المستهدف وموقعه من الدليل

الفصول ذات الأولوية	ما يعنيه في هذا الدليل	الغاية
2، 6، 8، 9	فهم ما يجب أن يطلبه المجلس ويعتمده، وكيف يقرأ التقارير الواردة إليه	مجلس الإدارة ولجانه
3، 6، 7	موقع الإدارة بوصفها مالكة للمخاطر، وأثر المنظومة على القرار التشغيلي	الإدارة التنفيذية
4، 6، 7، 9	المنهجية، ومعايير المخاطر، والرغبة في المخاطرة، ومؤشرات المخاطر	وظيفة إدارة المخاطر
5، 6، 7	بناء عالم الالتزام وسجل الالتزامات وربطه بسجل المخاطر	وظيفة الالتزام
4، 6، 8	موقع الخط الثالث، والتخطيط المبني على المخاطر، وتقييم فاعلية المنظومة	التدقيق الداخلي
الدليل كاملاً	منهجية تشخيص وتصميم قابلة للتطبيق على ارتباطات العملاء	المستشارون والممارسون

4-1 حدود الدليل وإخلاء المسؤولية

هذا الدليل وثيقة مهنية استرشادية. الإشارات الواردة فيه إلى التشريعات والتعليمات الرقابية في الأردن ودول الخليج مذكورة بغرض التوجيه لا الحصر، وهي عرضة للتعديل. تظل مسؤولية التحقق من النص النافذ وقت التطبيق على عاتق المنشأة ومستشاريها القانونيين. كما أن اعتماد المنشأة لأي من النماذج الواردة هنا لا ينشئ بذاته امتثالاً تنظيمياً ما لم يُطبَّق فعلياً ويوثَّق ويُراجع.

واتساقاً مع مبدأ حياد المصطلحات وسلامة الإسناد، تُعرَض في هذا الدليل مواقف الأطر المختلفة كما هي، ويُمَيَّز صراحةً بين ما تفرضه المعايير وما يُوصى به وما يمثل اجتهداً مهنيّاً للمُعد.

2. الإطار المفاهيمي The Conceptual Frame

1-2 من أين جاء المصطلح؟

لم ينشأ مصطلح GRC داخل معيار دولي، بل نشأ في الممارسة. صاغته منظمة OCEG في منتصف العقد الأول من الألفية استجابةً لواقع عملي: كانت المنشآت بعد قانون ساربنز أوكسلي (2002) تبني وظائف رقابية متعددة على التوازي، كل واحدة بمنهجيتها وسجلاتها وتقاريرها، حتى صار العبء الرقابي نفسه مصدر مخاطرة. وعرفت OCEG المفهوم بأنه القدرة المتكاملة على تحقيق الأهداف، ومعالجة عدم اليقين، والتصرف بنزاهة، وهو ما أطلقت عليه «الأداء المنضبط» (Principled Performance).

هذا الأصل التاريخي مهم لسببين. الأول أنه يفسر لماذا لا يوجد «معيار GRC» واحد يمكن الحصول على شهادة فيه، بخلاف ISO 31000 أو ISO 37301؛ فـ GRC مظلة تنظيمية تجمع معايير متعددة ولا تحل محلها. والثاني أنه يفسر الالتباس الأكثر شيوعاً في السوق: استخدام الاختصار للإشارة إلى فئة من البرمجيات وليس إلى منهج إداري.

تنبيه على الخلط الشائع

شراء نظام GRC برمجي لا يُنتج منظومة GRC. النظام يؤتمت منهجية قائمة؛ فإذا كانت المنهجية غائبة أو التصنيفات غير موحدة، فإن الأتمتة تُسرّع إنتاج بيانات غير قابلة للاستخدام. القاعدة العملية: لا تؤتمت قبل أن تستقر المنهجية وتُختبر يدوياً على وحدتين تشغيليتين على الأقل.

2-2 تعريف المكونات الثلاثة

التعريفات التالية مختارة من المصادر المعيارية الأكثر رسوخاً، لا من الاستخدام الدارج:

1-2-2 الحوكمة (Governance)

وفق ISO 37000:2021، الحوكمة هي المنظومة التي يجري بها توجيه المنظمة ومساءلتها والرقابة عليها، وهي مسؤولية هيئة الحوكمة (مجلس الإدارة أو مجلس الأمناء). جوهر الحوكمة إذاً سؤال واحد: من يقرر ماذا، وبأي صلاحية، وأمام من يُسأل عن النتيجة؟

2-2-2 إدارة المخاطر (Risk Management)

يُعرّف ISO 31000:2018 المخاطرة بأنها أثر عدم اليقين على الأهداف، وهو تعريف محايد يشمل الأثر السلبي والإيجابي معاً. وإدارة المخاطر هي الأنشطة المنسقة لتوجيه المنظمة والرقابة عليها فيما يتعلق بالمخاطر. ويستحق التعريف وقفة: ما دامت المخاطرة مرتبطة بالأهداف، فإن أي سجل مخاطر لا ينطلق من أهداف المنشأة المعتمدة هو سجل معلق في الهواء.

3-2-2 الالتزام (Compliance)

وفق ISO 37301:2021، الالتزام هو الوفاء بجميع متطلبات الالتزام الواجبة على المنظمة، وهي نوعان: متطلبات إلزامية مصدرها التشريع والتعليمات الرقابية والعقود، ومتطلبات طوعية تبنتها المنظمة بإرادتها كالمواثيق الأخلاقية والمعايير التي التزمت بها. هذا التقسيم عملي جداً عند بناء سجل الالتزامات، لأن الإخلال بكل نوع له نتائج مختلفة.

جدول (1-2): المقارنة البنوية بين المكونات الثلاثة

وجه المقارنة	الحوكمة	إدارة المخاطر	الالتزام
السؤال المحوري	من يقرر ومن يُسأل؟	ما الذي قد يعترض تحقيق الهدف؟	ما الذي يجب علينا الوفاء به؟
الأفق الزمني	هيكلي طويل المدى	استشرافي متجدد	حاضر ومستمر
المرجع المعياري	ISO 37000 · OECD 2023	ISO 31000 · COSO ERM	ISO 37301 · ISO 37001
المخرَج الرئيسي	مواثيق، صلاحيات، هيكل، تقارير المجلس	سجل مخاطر، خطط معالجة، مؤشرات	سجل التزامات، تقارير الحالة، بلاغات
المالك التنظيمي	مجلس الإدارة وأمانة سره	الإدارة (ملكية) ووظيفة المخاطر (منهجية)	الإدارة (تنفيذ) ووظيفة الالتزام (إشراف)
موقعه في الخطوط الثلاثة	فوق الخطوط جميعاً	خط ثانٍ	خط ثانٍ

وجه المقارنة	الحوكمة	إدارة المخاطر	الالتزام
أثر الغياب	قرارات بلا مساءلة	مفاجآت متكررة وردود فعل متأخرة	غرامات وإيقاف نشاط وضرر بالسمعة

يُقرأ الجدول أفقيًا لا عموديًا. فالفروق بين الأعمدة الثلاثة ليست فروق أهمية بل فروق وظيفة؛ ومحاولة دمج الوظائف الثلاث في مسمى وظيفي واحد، وهو ما يحدث كثيرًا في المنشآت المتوسطة، تُنتج غالبًا وظيفة تُتقن أحد الجوانب وتُهمل الجانبين الآخرين.

3-2 ما الذي يجعل GRC أكثر من مجرد جمع ثلاثة مكونات؟

الإجابة المختصرة: العلاقة نفسها. المكونات الثلاثة تشترك في ثلاثة أشياء لا يمكن أن تختلف عليها من دون أن تنهار قيمة المنظومة:

1. التصنيف الموحد. لا بد أن يكون لدى المنشأة تصنيف واحد للمخاطر والضوابط تستخدمه إدارة المخاطر والالتزام والتدقيق الداخلي. اختلاف التصنيفات هو السبب الأول في تعذر تجميع الصورة الكلية.
2. المصدر الواحد للبيانات. الضابط الرقابي يُوصف مرة واحدة، ويُقيّم مرة واحدة، وتستخدم نتيجة التقييم في السياقات الثلاثة، بدلًا من أن تُختبر الوحدة التشغيلية ثلاث مرات على الضابط نفسه.
3. لغة تقارير مشتركة. مقاييس الأثر والاحتمالية والأهمية النسبية تُعرّف مرة واحدة على مستوى المنشأة، لا داخل كل وظيفة على حدة.

من دون هذه العناصر الثلاثة تبقى الوظائف متجاوزة لا متكاملة، وهو الفرق الجوهرى الذي يعالجه الفصل السادس بالتفصيل.

3. المكون الأول: الحوكمة Governance

1-3 المرتكزات المعيارية

تستند الحوكمة إلى مرجعيتين دوليتين متكاملتين لا متنافستين. مبادئ منظمة التعاون الاقتصادي والتنمية (OECD G20, 2023) هي المرجع الأوسع اعتمادًا لدى منظمي أسواق المال، وتتنظم في ستة فصول: أساس إطار الحوكمة الفعال، وحقوق المساهمين، والمستثمرون المؤسسيون وأسواق المال، ودور أصحاب المصلحة، والإفصاح والشفافية، ومسؤوليات المجلس. وقد أضاف إصدار 2023 فصلاً مستقلاً للاستدامة والمرونة، وهو تطور جوهري لأنه نقل الاستدامة من هامش التقارير إلى صلب مسؤولية المجلس.

أما ISO 37000:2021 فيقدم أحد عشر مبدأً لحوكمة المنظمات تدور حول محور مركزي هو الغرض (Purpose)، وتشمل خلق القيمة، والاستراتيجية، والرقابة، والمساءلة، والإشراف، والقيادة، والبيانات والقرارات، وإشراك أصحاب المصلحة، والمسؤولية، والاستدامة، والمرونة. وميزته العملية أنه لا يفترض شركة مساهمة عامة، ما يجعله المرجع الأنسب للشركات العائلية والجمعيات والجهات الحكومية التي لا تنطبق عليها لوائح هيئات الأوراق المالية.

وفي البيئة المحلية، تضيف التشريعات طبقة إلزامية فوق ما سبق. ففي الأردن تصدر هيئة الأوراق المالية تعليمات حوكمة الشركات المساهمة المدرجة، ويصدر البنك المركزي تعليمات حوكمة البنوك، ويحكم قانون الشركات الإطار العام. وفي السعودية تصدر هيئة السوق المالية لائحة حوكمة الشركات، ويحكم نظام الشركات (2022) الأساس، وتصدر مؤسسة النقد أطرها الخاصة بالجهات الخاضعة لإشرافها. والفرق العملي بين المستويين حاسم: مخالفة المبدأ الدولي تُضعف الممارسة، ومخالفة النص التنظيمي تُنتج مسؤولية.

2-3 مكونات منظومة الحوكمة

حين تطلب المنشأة «حوكمة مكتملة» فإن المقصود عملياً تسع طبقات متتابعة. غياب أي طبقة يُنتج أثراً محدداً يمكن التنبؤ به، وهو ما يوضحه الجدول التالي:

جدول (1-3): طبقات منظومة الحوكمة وأثر غياب كل طبقة

#	الطبقة	أبرز مكوناتها	أثر غيابها عملياً
1	الطبقة التأسيسية	النظام الأساسي، دليل/لائحة الحوكمة، ميثاق المجلس	لا مرجعية عند الخلاف على الصلاحية
2	هيئات الإشراف	المجلس، لجنة التدقيق، لجنة الترشيحات والمكافآت، لجنة المخاطر	تركز القرار وغياب التحدي البناء
3	الطبقة الهيكلية	الهيكل التنظيمي، بطاقات الوصف الوظيفي، نطاق الإشراف	ازدواج المهام وفجوات المسؤولية
4	طبقة الصلاحيات	مصفوفة الصلاحيات، صلاحيات التوقيع، مصفوفة RACI	قرارات تُتخذ خارج حدود التفويض
5	طبقة السياسات	عالم السياسات وإجراءاتها التفصيلية	اعتماد على الأشخاص بدل النظام
6	طبقة النزاهة والسلوك	قواعد السلوك، تعارض المصالح، الأطراف ذات العلاقة، الإبلاغ عن المخالفات	بيئة مواتية للاحتيال وتعارض غير معلن
7	طبقة الإفصاح وأصحاب المصلحة	سياسة الإفصاح، إطار الجمعية العامة، آليات التظلم	فجوة ثقة مع المساهمين والجهات الرقابية
8	طبقة التأكيد	ميثاق التدقيق الداخلي، إطار الالتزام، علاقة المدقق الخارجي، تقييم المجلس	لا دليل مستقل على أن الضوابط تعمل
9	الطبقة التشغيلية	النماذج، السجلات، خطة عمل المجلس السنوية، أمانة السر	حوكمة موثقة وغير مُمارَسة

التسلسل في الجدول ليس اعتباطياً. الطبقات من الأولى إلى الرابعة تشكل البنية الدستورية التي لا يمكن بناء ما بعدها من دونها؛ فمن غير المجدي كتابة أربعين سياسة تشغيلية قبل اعتماد مصفوفة الصلاحيات، لأن السياسات ستحيل إلى صلاحيات غير موجودة.

3-3 مبدأ التناسب في التصميم

لا يوجد هيكل حوكمة صحيح بإطلاق. الشركة العائلية التي تضم أربعين موظفًا وثلاثة شركاء من عائلة واحدة لا تحتاج أربع لجان دائمة؛ حاجتها الأولى غالبًا فصل ملكية القرار عن إدارته، وتوثيق محاضر، ومصفوفة صلاحيات واقعية. في المقابل، البنك الخاضع لتعليمات البنك المركزي تُفرض عليه لجان محددة بنصوص لا مجال للاجتهاد فيها.

القاعدة التي أعمل بها عند تصميم أي هيكل: ابدأ من الإلزام التنظيمي (ما لا خيار فيه)، ثم أضف ما تفرضه طبيعة المخاطر الفعلية للمنشأة (خطر تشغيلي مرتفع يستدعي لجنة مخاطر ولو لم تُفرض نصًا)، ثم اترك الباقي لمرحلة لاحقة. الهيكل الذي يفوق قدرة المنشأة على تشغيله ينتهي إلى اجتماعات صورية ومحاضر مكررة، وهذا أسوأ من غيابه لأنه يمنح إحساسًا زائفًا بالسيطرة.

علامات إنذار على حوكمة شكلية

محاضر مجلس متطابقة في صياغتها من دورة إلى أخرى، وخالية من أي اعتراض أو تحفظ مسجل.
 لجنة تدقيق لا تجتمع منفردة بالمدقق الخارجي ولا بمدير التدقيق الداخلي من دون حضور الإدارة التنفيذية.
 مصفوفة صلاحيات لم تُحدَّث بعد تغيير في الهيكل التنظيمي أو في حجم النشاط.
 سياسة تعارض مصالح معتمدة من دون إقرارات سنوية موقعة ومحفوظة في سجل.
 تقارير ترفع إلى المجلس تعرض ما أنجز فقط، من دون ما تأخر ومن دون تفسير التأخير.

4. المكوّن الثاني: إدارة المخاطر Risk Management

1-4-1 العמוד الفقري: ISO 31000:2018

يقدم المعيار ثلاث كتل مترابطة: المبادئ (البند 4)، والإطار (البند 5)، والعملية (البند 6). والخلط بينها شائع، مع أن كلّاً منها يجب عن سؤال مختلف. المبادئ تجيب عن «ما الذي يجعل إدارة المخاطر ذات قيمة؟»، والإطار يجيب عن «كيف تُدمج في المنشأة؟»، والعملية تجيب عن «كيف تُنفذ على مخاطرة بعينها؟».

المبادئ الثمانية تشترط أن تكون إدارة المخاطر مدمجة في العمليات لا موازية لها، ومنظمة وشاملة، ومخصصة لسياق المنشأة، وشاملة لأصحاب المصلحة، وديناميكية، ومبنية على أفضل المعلومات المتاحة، ومراعية للعوامل البشرية والثقافية، وقابلة للتحسين المستمر. ومن هذه الثمانية، أكثر ما يُحقّق فيه عملياً مبدأ الدمج ومبدأ العوامل البشرية؛ إذ تُبنى المنظومة تقنياً سليمة ثم تُترك خارج دورة اتخاذ القرار الفعلية.

أما الإطار (البند 5) فيضع القيادة والالتزام في المركز، وحوله خمسة أنشطة دائرية: الدمج، والتصميم، والتنفيذ، والتقييم، والتحسين. ويُستخدم هذا البند عند تقييم منظومة المنشأة نفسها، بخلاف البند 6 الذي يُستخدم عند إجراء تقييم مخاطر فعلي.

الشكل (2): عملية إدارة المخاطر وفق ISO 31000:2018 (البند 6)



الشكل (2): عملية إدارة المخاطر وفق ISO 31000:2018، البند 6

1-1-4 الخطأ المنهجي الأكثر تكراراً

البند 3-6 يفرض تحديد معايير المخاطر قبل التقييم، أي تعريف مقاييس الاحتمالية والأثر بصيغة قابلة للقياس، وتحديد مصفوفة التقييم، وربطها بالرغبة في المخاطرة. الممارسة الشائعة تقلب هذا الترتيب: تُعقد ورشة عمل، ويُطلب من المشاركين تقييم كل مخاطرة من 1 إلى 5، من دون تعريف مسبق لما يعنيه «3» في الأثر المالي أو التشغيلي. النتيجة سجل يبدو منضبطاً رقمياً وهو في حقيقته تجميع لانطباعات شخصية غير قابلة للمقارنة بين الوحدات ولا عبر الزمن.

قاعدة عملية عند وضع معايير المخاطر
عَرِّف مقياس الأثر بأربعة أبعاد على الأقل: مالي (بمبلغ محدد أو نسبة من الإيرادات)، وتشغيلي (بمدة توقف)، وتنظيمي (بنوع الجزاء)، وسمعي (بمدى التغطية والانتشار).
اربط الحد الأعلى للمقياس بحدود التحمل المعتمدة من المجلس، لا برقم اعتباطي. إن كان أقصى خسارة مقبولة سنوياً مليون دينار، فيجب أن يعكس المستوى الخامس هذا الحد.
اختبر المقياس على ثلاث مخاطر معروفة سابقاً وقعت فعلاً. إن لم يُنتج المقياس تصنيفاً يطابق ما شعرت به الإدارة وقت وقوعها، فالمقياس يحتاج معايرة.

2-4 العدسة الاستراتيجية: COSO ERM 2017

يختلف إطار COSO ERM عن ISO 31000 في موضع التركيز لا في الجوهر. فبينما يقدم ISO عملية قابلة للتطبيق على أي مخاطرة، يربط COSO المخاطر بالاستراتيجية والأداء عبر خمسة مكونات وعشرين مبدأ: الحوكمة والثقافة، والاستراتيجية ووضع الأهداف، والأداء، والمراجعة والتتبع، والمعلومات والاتصال والتقارير.

وأبرز ما ينفرد به COSO عملياً هو المبدأ الرابع عشر: الرؤية المحفظية (Portfolio View). فالمخاطر تتفاعل فيما بينها، ومجموع تصنيفاتها الفردية لا يساوي وضع المنشأة الكلي. مثال مباشر: مخاطرة اعتماد على مورد واحد مصنفة «متوسطة»، ومخاطرة سيولة مصنفة «متوسطة»، ومخاطرة تركيز جغرافي مصنفة «متوسطة»؛ اجتماعها في سيناريو واحد قد يُنتج تهديداً وجودياً للمنشأة لا يظهر في أي صف من صفوف السجل.

جدول (1-4): متى تستخدم ISO 31000 ومتى تستخدم COSO ERM

وجه المقارنة	ISO 31000:2018	COSO ERM 2017
طبيعة الوثيقة	إرشادي، غير قابل للاعتماد (Certification)	إطار مرجعي صادر عن لجنة مهنية أمريكية
نقطة الانطلاق	الأهداف وسياق المنشأة	الاستراتيجية وقرار اختيارها
البنية	مبادئ + إطار + عملية	خمس مكونات وعشرون مبدأ
نقطة القوة	قابلية التطبيق على أي منشأة وأي نوع مخاطرة	ربط المخاطر بالأداء والاستراتيجية والثقافة
الاستخدام الأنسب	بناء المنهجية وتشغيل دورة التقييم	حوار المجلس، الرؤية المحفظية، تقييم الثقافة
التوصية العملية	يُعد أساساً للمنهجية التشغيلية	يُستدعى عند مناقشة الاستراتيجية والرقابة العليا

لا يوجد تعارض يستدعي الاختيار بينهما. الترتيب الذي أعتمدته في الارتباطات: ISO 31000 مرجعاً للمنهجية والعملية، وCOSO ERM مرجعاً لطبقة الحوكمة والثقافة والرؤية المحفظية، مع تصريح واضح في سياسة المخاطر بأي البندين يُحتكم إليه عند الاختلاف.

3-4 الرغبة في المخاطرة: بناء تدرّجي لا شعاري

أكثر بيانات الرغبة في المخاطرة التي تُعرض على نُصاغ في جملة واحدة عامة من نوع «تتبنى الشركة نهجاً متحفّظاً تجاه المخاطر». هذه ليست رغبة في المخاطرة، بل تجنّب لصياغتها. البناء السليم يمر بأربع طبقات متصلة:

جدول (2-4): تدرّج الرغبة في المخاطرة من المجلس إلى القرار التشغيلي

الطبقة	من يعتمدها	صيغتها	مثال تطبيقي
بيان الرغبة في المخاطرة	مجلس الإدارة	نوعية، لكل فئة مخاطر على حدة	لا رغبة إطلاقاً في مخاطر الالتزام بتشريعات مكافحة غسل الأموال
حدود التحمل	المجلس بتسيب لجنة المخاطر	كمية وقابلة للقياس	ألا تتجاوز الخسائر التشغيلية السنوية 2% من صافي الإيراد
الحدود التشغيلية	الإدارة التنفيذية	حدود مدمجة في القرار اليومي	سقف انتماني للعميل الواحد 250 ألف دينار

الطبقة	من يعتمدها	صيغتها	مثال تطبيقي
قاعدة الربط	وظيفة المخاطر	إلزامية في كل تقييم	كل مخاطرة في السجل تُقارن بحد التحمل، وأي تجاوز يُصعد فوراً

الطبقة الرابعة هي التي تُحوّل البيان من نص في محضر إلى أداة إدارة. من دون قاعدة الربط، يبقى بيان الرغبة وثيقة مستقلة لا أثر لها على تصنيف مخاطرة واحدة.

4-4 سجل المخاطر ومؤشرات المخاطر الرئيسية

سجل المخاطر هو المخزّج الأكثر ظهوراً للوظيفة، وهو أيضاً الأكثر عرضة للتشوّه. المشكلات المتكررة التي أصادفها: صياغة المخاطرة بوصفها حدثاً واقعاً لا احتمالاً («ضعف نظام المشتريات» بدل «احتمال تنفيذ مشتريات خارج الصلاحيات نتيجة ضعف ضوابط النظام»)، ودمج عدة مخاطر في صف واحد فيتعذر تتبع المعالجة، وخلط الخطر بسببه الجذري بآثره.

أما مؤشرات المخاطر الرئيسية فالقاعدة فيها أن القلة المفيدة أفضل من الكثرة الشكالية. خمسة إلى عشرة مؤشرات لكل فئة مخاطر رئيسية، يحمل كل منها بطاقة تعريف كاملة تشمل الاسم، والمخاطرة المرتبطة برقمها في السجل، والمعادلة الحسابية، ومصدر البيانات ومالكه، والتكرار، والعتبات بالأرقام (أخضر/برتقالي/أحمر) مشتقة من حد التحمل، ومسار التصعيد بالأسماء والمهل الزمنية.

التمييز بين المؤشر المتقدم والمتأخر

المؤشر المتأخر يسجل ما وقع: عدد الحوادث، قيمة الخسائر، عدد الشكاوى المستلمة. مفيد للمساءلة، عديم الفائدة للوقاية.
المؤشر المتقدم يتنبأ: نسبة الصيانة الوقائية المتأخرة، معدل دوران الموظفين في وظائف حساسة، عمر أقدم تحديث أمني غير مثبت، نسبة الشواغر في وظائف الرقابة.
المنظومة الناضجة تجمع النوعين وتربطهما: ارتفاع المؤشر المتقدم يجب أن يُحدث إجراءً قبل أن يتحرك المؤشر المتأخر.

5. المكوّن الثالث: الالتزام Compliance

1-5 المرجعية المعيارية

يقدم ISO 37301:2021 أول نموذج قابل للاعتماد لنظام إدارة الالتزام، ويقوم على بنية الأنظمة الإدارية المعروفة: سياق المنظمة، والقيادة، والتخطيط، والدعم، والتشغيل، وتقييم الأداء، والتحسين. ويشترط عناصر محددة لا تُعد وظيفة الالتزام قائمة من دونها: تحديد متطلبات الالتزام وتوثيقها، وتقييم مخاطر عدم الالتزام، وسياسة معتمدة، ووظيفة التزام ذات استقلالية وصلاحيّة وصول مباشر إلى هيئة الحوكمة، وآلية إبلاغ عن المخالفات تحمي المبلّغ، ودورة رصد وقياس وتحسين.

ويُستكمل بـ ISO 37001:2016 الخاص بمكافحة الرشوة حين يكون تعرّض المنشأة للرشوة جوهرياً (تعامل حكومي واسع، وسطاء وكلاء، أسواق مرتفعة المخاطر). العلاقة بينهما علاقة عام بخاص: الأول يبني النظام، والثاني يعمّقه في مجال واحد شديد الحساسية.

2-5 عالم الالتزام وسجل الالتزامات

نقطة البدء العملية ليست كتابة سياسة، بل حصر مصادر الالتزام (Compliance Universe). وهو تمرين يتطلب الجمع بين القراءة القانونية والمعرفة التشغيلية، لأن كثيراً من الالتزامات لا تظهر في التشريعات العامة بل في شروط الترخيص وفي بنود العقود.

جدول (1-5): مصادر الالتزام النموذجية في البيئتين الأردنية والخليجية

فئة المصدر	أمثلة على المصدر	ملاحظة على التطبيق
التشريع العام	قانون الشركات، قانون العمل، قوانين الضريبة	يسري على جميع المنشآت بصرف النظر عن القطاع
التعليمات الرقابية القطاعية	تعليمات هيئة الأوراق المالية، تعليمات البنك المركزي الأردني، لوائح هيئة السوق المالية، أطر مؤسسة النقد	يحدد القطاع والشكل القانوني ما ينطبق منها
الجرائم المالية	تشريعات مكافحة غسل الأموال وتمويل الإرهاب وقوائم العقوبات	الالتزام ذو طبيعة جزائية؛ لا يقبل التدرج في التطبيق
حماية البيانات	قانون حماية البيانات الشخصية في الأردن، نظام حماية البيانات الشخصية في السعودية	يتطلب سجل معالجة وتقييم أثر وضوابط نقل البيانات
الأمن السببراني	الضوابط الأساسية للأمن السببراني وضوابط الأنظمة الحساسة	إلزامي على الجهات المشمولة بنطاق التطبيق
الضريبة والفوترة	ضريبة القيمة المضافة، الزكاة، الفوترة الإلكترونية	الالتزام ذو دورة تشغيلية شهرية أو ربعية
الالتزامات التعاقدية	اتفاقيات التمويل، عقود العملاء الكبار، اتفاقيات الترخيص	كثيراً ما تكون أشد صرامة من التشريع نفسه
الالتزامات الطوعية	شهادات ISO، موثائق القطاع، تعهدات الاستدامة	اختيارية في نشأتها، ملزمة بعد التبني والإعلان

يُحوّل هذا الحصر إلى سجل التزامات تشغيلي بأعمدة ثابتة: الرقم المرجعي، ومصدر الالتزام (النص والمادة)، والمتطلب بصيغته العملية، والوحدة المالكة، والضابط الرقابي المنفّذ، وتكرار الوفاء، ودليل الإثبات المطلوب، وحالة الالتزام، وتاريخ آخر تحقق، ومخاطرة عدم الالتزام المرتبطة برقمها في سجل المخاطر. العمود الأخير هو نقطة الوصل مع الفصل الرابع، وهو الذي يمنع نشوء سجلين متوازيين.

3-5 مخاطر عدم الالتزام

من الأخطاء البنيوية التعامل مع عدم الالتزام بوصفه فئة مخاطر منفصلة تُدار خارج منظومة المخاطر. الصحيح أنه فئة داخل سجل المخاطر نفسه، تخضع لمعايير التقييم ذاتها، مع خصوصية واحدة: أن الأثر التنظيمي فيها كثيراً ما يتجاوز الأثر المالي المباشر. غرامة قد تكون محتملة، لكن إيقاف الترخيص أو رفض تجديده تهديد وجودي لا يقاس بمقياس الخسارة النقدية.

ولهذا السبب توصي معظم الأطر بأن يكون لبعض فئات الالتزام موقف صريح بعدم وجود أي رغبة في المخاطرة إطلاقاً (Zero Appetite)، لا أن تُقيّم بالمصفوفة العامة. هذا الموقف يجب أن يُنص عليه في بيان الرغبة في المخاطرة، ويُترجم إلى ضوابط مانعة لا كاشفة.

اختبار عملي لجاهزية وظيفة الالتزام
اطلب من مسؤول الالتزام تحديد عدد المتطلبات التنظيمية المسجلة لديه، ونسبة ما جرى التحقق من الوفاء به خلال الاثني عشر شهرًا الأخيرة،
مع دليل الإثبات.
إن تعذر إعطاء رقمين محددين خلال دقائق، فالوظيفة تعمل بالاستجابة لا بالمنهج؛ وهذا هو التشخيص الفعلي بصرف النظر عن وجود سياسة
معتمدة.

6. العلاقة بين المكونات الثلاثة The Integration Logic

هذا هو الفصل المحوري في الدليل. فالمفاهيم الثلاثة مشروحة في عشرات المراجع، أما ما يندر تناوله بدقة فهو طبيعة الوصل بينها: أين تلتقي بالضبط، وبأي آلية، وما الذي ينكسر عند انقطاع الوصل.

1-6 من التجاور إلى التكامل

المنشآت تمر عادةً بثلاث حالات. في الحالة الأولى تكون الوظائف الثلاث غائبة أو مجتمعة في شخص واحد يؤدي ما يستطيع. في الحالة الثانية، وهي الأكثر شيوعاً، تكون الوظائف موجودة ومنفصلة: لكل منها سياستها وسجلها وتقريرها ودورها الزمنية، وتتقاطع بالصادفة لا بالتصميم. أما الحالة الثالثة فهي التكامل، حيث تبقى الوظائف مستقلة في مسؤولياتها لكنها تشترك في البنية التحتية للمعلومات وفي دورة التقارير.

ويهم التوضيح أن التكامل لا يعني الدمج التنظيمي. اقترح دمج المخاطر والالتزام والتدقيق الداخلي تحت إدارة واحدة يبدو موقراً للتكلفة، لكنه يُلغي استقلالية الخط الثالث ويناقض نموذج الخطوط الثلاثة. التكامل يقع على مستوى البيانات والمنهجية والتقارير، لا على مستوى الهيكل.

الشكل (1): نموذج تكامل الحوكمة وإدارة المخاطر والالتزام



الشكل (1): نموذج تكامل الحوكمة وإدارة المخاطر والالتزام

يوضح الشكل ثلاث نقاط تقاطع ثنائية ونقطة مركزية واحدة. التقاطع بين الحوكمة وإدارة المخاطر هو الرقابة على المخاطر، أي مسؤولية المجلس عن اعتماد الرغبة في المخاطرة ومساءلة الإدارة عن البقاء ضمنها. والتقاطع بين الحوكمة والالتزام هو الرقابة على الالتزام، أي مسؤولية المجلس عن ثقافة النزاهة وتلقي تقارير حالة الالتزام. أما التقاطع بين المخاطر والالتزام فهو مخاطر عدم الالتزام كما ورد في الفصل الخامس. والمركز حيث تلتقي الثلاثة هو ما تسميه OCEG الأداء المنضبط، أي تحقيق الأهداف مع إدارة عدم اليقين والتصرف بنزاهة في آن واحد.

2-6 سلسلة الوصل: من الهدف إلى التأكيد

أوضح طريقة لفهم العلاقة عملياً هي تتبع سلسلة واحدة متصلة تبدأ من هدف مؤسسي وتنتهي عند رأي مستقل. كل حلقة في السلسلة تنتمي إلى مكون، وانقطاع أي حلقة يُبطل ما بعدها:

جدول (1-6): سلسلة الوصل بين المكونات الثلاثة

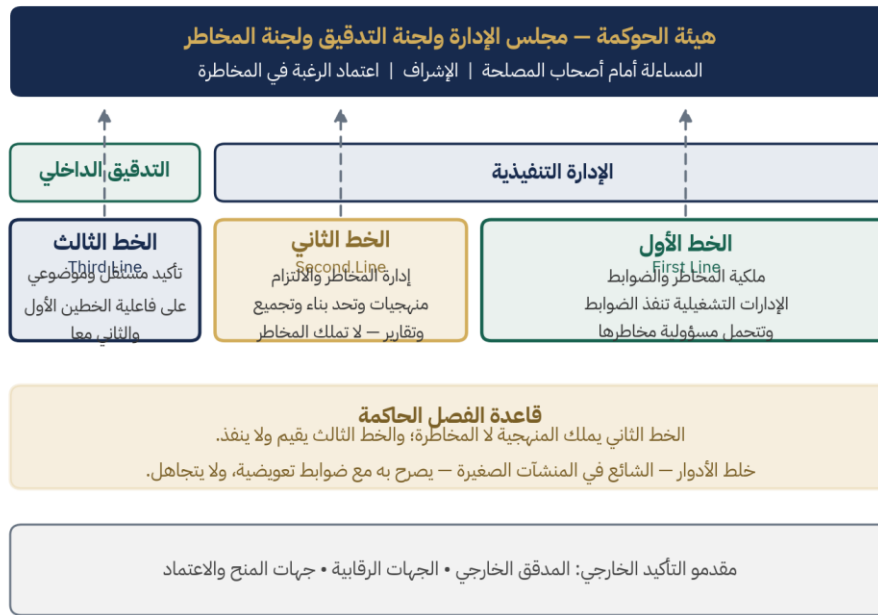
الحلقة	المخرَج	المكون المالك	أثر انقطاع الحلقة
الهدف المؤسسي	اهداف معتمدة وقابلة للقياس	الحوكمة	سجل مخاطر بلا مرجع يُقاس عليه
الرغبة في المخاطرة	بيان معتمد وحدود تحمل رقمية	الحوكمة	تقييم المخاطر بلا معيار حكم
تحديد المخاطرة	صف في سجل المخاطر بصيغة احتمالية	إدارة المخاطر	إدارة بردود الفعل
المتطلب التنظيمي	صف في سجل الالتزامات مرتبط بالمخاطرة	الالتزام	مخاطر تنظيمية خارج الرادار
الضابط الرقابي	ضابط موصوف ومالك ودليل تشغيل	الإدارة (الخط الأول)	معالجة معلنة وغير منفذة
تقييم الضابط	حكم على التصميم وفاعلية التشغيل	الخط الثاني	مخاطرة متبقية غير معروفة
التأكيد المستقل	تقرير تدقيق داخلي ورأي	الخط الثالث	اعتماد المجلس على تطمين ذاتي
قرار الحوكمة	قرار المجلس واللجان ومتابعة التنفيذ	الحوكمة	تقارير تُقرأ ولا يترتب عليها أثر

لاحظ أن السلسلة تبدأ وتنتهي عند الحوكمة. هذه ليست مصادفة في التصميم، بل هي جوهر النموذج: الحوكمة تحدد ما يُقاس، وتستقبل نتيجة القياس، وتتخذ القرار بناءً عليها. أي منظومة مخاطر أو التزام لا تُغلق دائرتها عند المجلس تتحول إلى نشاط توثيقي.

3-6 نموذج الخطوط الثلاثة بوصفه العمود الفقري

أصدر معهد المدققين الداخليين نسخته المحدثّة من النموذج في 2020، وتخلّى فيها عن التصور الدفاعي القديم (خطوط دفاع) لصالح تصور قائم على الأدوار والتعاون. والتحديث مهم لأنه أزال الانطباع بأن الخطوط جدران متتالية، وأكد أن هيئة الحوكمة تعلق الخطوط الثلاثة جميعاً، وأن التنسيق بينها واجب لا خيار.

الشكل (3): توزيع أدوار GRC وفق نموذج الخطوط الثلاثة (IIA 2020)



الشكل (3): توزيع أدوار GRC وفق نموذج الخطوط الثلاثة

التطبيق العملي للنموذج يحسم ثلاثة نزاعات متكررة داخل المنشآت. الأول: من يملك المخاطرة؟ الإجابة أن مالكيها هو المدير التنفيذي للوحدة المعنية، لا مدير المخاطر. الثاني: هل يجوز لوظيفة المخاطر تصميم الضوابط؟ يجوز أن تدعم وتقتصر، لكن ملكية التنفيذ تبقى للخط الأول وإلا فقدت استقلالية التحدي. الثالث: هل يجوز للتدقيق الداخلي بناء سجل المخاطر؟ لا، لأنه سيدقق لاحقاً على عمله؛ ويقتصر دوره على تقييم كفاية السجل ومنهجيته.

وفي المنشآت الصغيرة والمتوسطة يصعب الفصل التام بين الخطين الثاني والثالث لأسباب اقتصادية. الموقف المهني السليم هنا ليس التظاهر بوجود فصل غير قائم، بل التصريح به في ميثاق التدقيق ووضع ضوابط تعويضية: تقييد دور الوظيفة المزدوجة في التصميم، ورفع الحالات التي شاركت في تصميمها إلى مراجعة خارجية دورية، وإخطار لجنة التدقيق بمواضع التداخل صراحةً.

4-6 الشروط الثلاثة للتكامل الفعلي

4. تصنيف موحد للمخاطر والضوابط. إذا صنفت إدارة المخاطر خطراً تحت «تشغيلي» وصنفته التدقيق تحت «امتثال» وصنفته الالتزام تحت «تنظيمي»، فلا سبيل لتجميع صورة واحدة مهما بلغت جودة كل تقرير منفرداً. يُعتمد التصنيف مرة واحدة بقرار من لجنة المخاطر ويلزم به الجميع.
5. مصدر واحد للحقيقة بشأن الضوابط. الضابط يُسجل مرة واحدة برقم فريد، ويُقيم وفق دورة معتمدة، وتُستخدم نتيجة التقييم من الوظائف الثلاث. هذا الشرط وحده يلغي معظم ازدواجية الاختبار التي تُرهق الوحدات التشغيلية.
6. دورة تقارير متزامنة. أن ترفع الوظائف الثلاث تقاريرها في الدورة الزمنية نفسها وبلغة القياس نفسها، بحيث يقرأ المجلس صورة مركبة لا ثلاث صور متفرقة يتولى هو التوفيق بينها.

5-6 تكلفة غياب التكامل

من المفيد عرض الكلفة بلغة الأعراض الملموسة، لأن غياب التكامل نادراً ما يظهر بوصفه مشكلة مستقلة، بل يظهر عبر آثاره:

جدول (2-6): أعراض غياب التكامل وأسبابها الجذرية

المعالجة	السبب الجذري	العرض الملاحظ
سجل ضوابط مركزي ودورة تقييم موحدة	غياب المصدر الواحد للضوابط	اختبار الوحدة التشغيلية على الضابط نفسه ثلاث مرات في السنة
اعتماد معايير مخاطر واحدة على مستوى المنشأة	اختلاف مقاييس الأثر بين الوظائف	تقارير متعارضة عن مستوى المخاطرة ذاتها
عمود ربط إلزامي بين السجلين	انفصال سجل الالتزامات عن سجل المخاطر	مخاطرة تنظيمية جوهرية غائبة عن سجل المخاطر
تخطيط مبني على المخاطر موثق في ميثاق التدقيق	عدم استخدام سجل المخاطر مدخلاً للتخطيط	خطة تدقيق داخلي لا تعكس أولويات المخاطر
توحيد الرزنامة وتقرير GRC مجتم	تباعد دورات رفع التقارير	قرارات مجلس متأخرة عن الأحداث
سجل واحد للتوصيات بمالك وتاريخ استحقاق	غياب سجل متابعة موحد للتوصيات	توصيات متكررة في تقارير متتالية

الخلاصة التي أقدّمها للمجالس

المؤشر الأصديق على وجود منظومة **GRC** متكاملة ليس عدد السياسات المعتمدة، بل قدرة المنشأة على الإجابة عن سؤال واحد في جلسة واحدة: ما أهم عشرة مخاطر تهدد أهدافنا هذا العام، ومن يملك كل واحدة منها، وما الضابط الذي يخفّضها، ومن قدم تأكيداً مستقلاً على أن الضابط يعمل؟ إن تعدّرت الإجابة من مصدر واحد متسق، فالمنظومة متجاوزة لا متكاملة مهما بلغ عدد وثائقها.

7. من النظرية إلى التطبيق Implementation Methodology

يعرض هذا الفصل منهجية تنفيذ من ست مراحل، مصممة لتُنجز خلال ثمانية عشر شهرًا في منشأة متوسطة الحجم. المدد تقديرية وتتأثر بحجم المنشأة ودرجة نضجها الحالية وتوافر الموارد، لكن التسلسل نفسه لا ينبغي تغييره لأن كل مرحلة تُنتج مدخلًا للتي تليها.

1-7 المرحلة صفر: التفويض والرعاية

لا تبدأ المنظومة من ورشة عمل، بل من قرار مجلس. المطلوب في هذه المرحلة ثلاثة مخرجات محددة: قرار مجلس يعتمد المبادرة ويحدد نطاقها، وتعيين راعٍ تنفيذي بمستوى يسمح له بتجاوز مقاومة الوحدات، وتخصيص موازنة ووقت من كوادرات التشغيلية. تجاوز هذه المرحلة هو السبب الأول في تعثر المبادرات؛ إذ تتحول إلى مشروع لدائرة واحدة تحاول إقناع باقي الدوائر بالتعاون من دون سند.

2-7 المرحلة الأولى: تشخيص الوضع الراهن

التشخيص عمل ميداني لا مكتبي. يشمل جمع الوثائق القائمة وفحصها فحصًا نقديًا، ومقابلات مع مالكي العمليات، وفحص أدلة تشغيل عينة من الضوابط، ومراجعة محاضر المجلس ولجانه للسنتين الأخيرتين. مخرجه تقرير تشخيص يتضمن قياس النضج وفق الفصل الثامن، وسجل فجوات مرتب بحسب الأولوية، وخارطة أولية لأصحاب المصلحة.

نصيحة من الممارسة

اقرأ محاضر لجنة التدقيق للسنتين الأخيرتين قبل أي مقابلة. المحاضر تكشف ما لا تكشفه المقابلات: أي القضايا تكررت من دون إغلاق، وأي التوصيات أُلجّت أكثر من مرة، وأين تتوقف المتابعة عادةً. هذه المواضع هي الفجوات الحقيقية، وما عداها غالبًا مشكلات توثيق.

3-7 المرحلة الثانية: تصميم الإطار المتكامل

في هذه المرحلة تُبنى الأسس المشتركة قبل أي سجل. المخرجات المطلوبة بالترتيب: تصنيف موحد للمخاطر والضوابط، ثم سياسة إدارة المخاطر وسياسة الالتزام، ثم معايير المخاطر (مقاييس الأثر والاحتمالية والمصفوفة)، ثم بيان الرغبة في المخاطرة وحدود التحمل، ثم موافقة موثقة اللجان ومصفوفة الصلاحيات مع الأدوار الجديدة. الترتيب مقصود. بناء سجل مخاطر قبل اعتماد التصنيف والمعايير يعني إعادة بنائه لاحقًا؛ وهي خسارة وقت ومصادقية معًا.

4-7 المرحلة الثالثة: البناء والتطبيق التجريبي

يُطبق الإطار على وحدتين تشغيليتين مختلفتين في الطبيعة (مثلًا وحدة عمليات ووحدة مساندة) قبل التعميم. الهدف من التجريب اكتشاف ما لا يظهر في التصميم: صعوبة توفير بيانات مؤشر ما، أو غموض في تعريف مستوى من مستويات الأثر، أو ضابط لا مالك واقعي له.

جدول (1-7): مخرجات المراحل ومعايير الانتقال إلى المرحلة التالية

المرحلة	المخرجات الأساسية	معايير الانتقال (Gate)
صفر: التفويض	قرار مجلس، راعٍ تنفيذي، موازنة	محضر مجلس يوثق النطاق والراعي
1: التشخيص	تقرير تشخيص، قياس نضج، سجل فجوات	اعتماد لجنة المخاطر أو التدقيق للتقرير
2: التصميم	تصنيف موحد، سياسات، معايير مخاطر، بيان رغبة	اعتماد المجلس للسياسات وبيان الرغبة
3: التجريب	سجل مخاطر والتزامات لوحدتين، ضوابط موصوفة	إقفال ملاحظات التجريب وتعديل المنهجية
4: التعميم	سجلات على مستوى المنشأة، لوحة مؤشرات، تقرير مجمع	أول تقرير GRC مجمع يُعرض على المجلس
5: الترسيع	أتمتة، مراجعة مستقلة، إعادة قياس النضج	ارتفاع موثوق في مستوى النضج مقابل خط الأساس

5-7 المرحلة الرابعة: التعميم والأتمتة

بعد استقرار المنهجية يجري التعميم على باقي الوحدات، ثم يُطرح سؤال الأتمتة. معايير القرار التي أستخدمها: عدد الضوابط التي تحتاج تتبعًا دوريًا، وعدد الوحدات المشمولة، وحجم متطلبات الإثبات التنظيمي، وتكرار التقارير المطلوبة. دون خمسين ضابطًا وثلاث وحدات، يكفي جدول بيانات منضبط مع ضوابط إصدار؛ وما فوق ذلك تبدأ تكلفة العمل اليدوي في تجاوز تكلفة الأداة.

6-7 المرحلة الخامسة: الترسيع والتحسين

الترسيخ يعني أن تصبح المنظومة جزءًا من دورات القرار القائمة لا نشاطًا موازيًا لها: أن يُرفق تقييم مخاطر بأي استثمار رأسمالي يتجاوز حدًا معينًا، وأن تُدرج حالة الالتزام في تقييم أداء مديري الوحدات، وأن تنطلق خطة التدقيق الداخلي من سجل المخاطر المعتمد. وحين يصل الأمر إلى هذه الحال، يصبح قياس النضج مجددًا مفيدًا لأنه يقيس تغييرًا حقيقيًا.

الشكل (5): خارطة طريق تنفيذ منظومة GRC متكاملة



الشكل (5): خارطة طريق تنفيذ منظومة GRC متكاملة خلال 18 شهرًا

8. قياس نضج منظومة GRC Maturity Assessment

القياس شرط لأي تحسين قابل للإثبات. والنموذج المعروض هنا يقيس تسعة أبعاد على مقياس من خمسة مستويات، ويُطبق مرتين على الأقل: مرة عند التشخيص لتكوين خط الأساس، ومرة بعد اثني عشر إلى ثمانية عشر شهرًا لقياس الأثر.

1-8 المستويات الخمسة

جدول (1-8): مستويات نضج منظومة GRC

المستوى	التسمية	الوصف	الدليل المتوقع
1	بدائي	ممارسات فردية غير موثقة تعتمد على أشخاص بعينهم	لا توجد وثائق أو سجلات منتظمة
2	ناشئ	وثائق أولية موجودة والتطبيق متقطع وغير موحد	سياسة معتمدة من دون سجلات محدثة
3	محدد	منهجية موثقة ومعتمدة ومطبقة على معظم الوحدات	سجلات محدثة ومحاضر اعتماد ودورة معلومة
4	مُدار	تطبيق متسق مع قياس بمؤشرات وتصعيد فعلي للتجاوزات	مؤشرات بعثبات، وحالات تصعيد موثقة
5	متقدم	تحسين مستمر ومقارنة مرجعية ودمج كامل في القرار	مراجعات مستقلة وتعديلات موثقة على المنهجية

2-8 أبعاد القياس التسعة

يُقيّم كل بُعد على حدة، ولا يُختزل التقييم في رقم واحد للمنشأة. فالمتوسط الحسابي يُخفي المشكلات: منشأة بمستوى 4 في الحوكمة ومستوى 1 في البيانات والتقنية ليست في المستوى المتوسط، بل هي منشأة تُصدر قرارات جيدة الشكل بناءً على بيانات غير موثوقة.

جدول (2-8): أبعاد قياس النضج وسؤال التشخيص لكل بُعد

#	البُعد	سؤال التشخيص المباشر
1	الحوكمة والإشراف	هل تتلقى لجنة مختصة تقارير المخاطر والالتزام دوريًا وتتخذ قرارات موثقة بشأنها؟
2	الإطار والسياسات	هل توجد سياسات معتمدة سارية المفعول ومراجعة خلال آخر دورة مقرر؟
3	ثقافة المخاطر	هل يُبلغ عن الحوادث والأخطاء طوعًا من دون خشية جزاء؟
4	انضباط العمليات	هل تُنفذ دورة التقييم في مواعيدها بمنهجية واحدة عبر الوحدات؟
5	الرغبة في المخاطرة	هل يمكن إبراز حالة واحدة على الأقل تغيّر فيها قرار بسبب تجاوز حد تحمّل؟
6	منظومة الالتزام	هل يوجد سجل التزامات كامل مع أدلة إثبات وتاريخ آخر تحقق؟
7	البيانات والتقنية	هل توجد نسخة واحدة معتمدة من سجل المخاطر والضوابط يعرفها الجميع؟
8	جودة التقارير	هل تعرض التقارير التغيّر والقرار المطلوب، أم تسرد الوضع فقط؟
9	واجهة التأكيد	هل تنطلق خطة التدقيق الداخلي من سجل المخاطر المعتمد؟

الشكل (4): مثال على مخطط نضج GRC – الوضع الحالي مقابل المستهدف



الشكل (4): مثال توضيحي على مخطط نضج GRC، الوضع الحالي مقابل المستهدف

في المثال المعروض يظهر نمط شائع جداً: نضج مقبول في طبقة الحوكمة والسياسات، وضعف واضح في البيانات والتقنية وفي ترجمة الرغبة في المخاطرة إلى قرارات. وهذا النمط يوجّه خطة التحسين مباشرة: لا حاجة إلى مزيد من السياسات، بل إلى بنية بيانات موحدة وقاعدة ربط بين حدود التحمل وقرارات الاعتماد.

كيف يُستخدم القياس من دون أن يفقد مصداقيته

لا تُقيّم بمنح درجات من الذاكرة. كل مستوى يُسند بدليل قابل للفحص (وثيقة، محضر، سجل، تقرير).
لا تستهدف المستوى الخامس في كل الأبعاد. المستوى 4 في الأبعاد الحرجة و3 في الباقي هدف واقعي لأغلب المنشآت المتوسطة.
اجعل القياس الثاني بواسطة جهة غير التي أجرت الأول حيثما أمكن، أو راجع نتائجه مراجعة مستقلة، وإلا فقد قيمته المقارنة.

9. مؤشرات قياس أداء المنظومة GRC Performance Indicators

تقيس المؤشرات التالية أداء المنظومة نفسها لا أداء المنشأة. وهي مقترحة كنقطة انطلاق تُكَيَّف بحسب القطاع والحجم، ولا يُنصح بتبنيها كاملة دفعة واحدة؛ ثمانية إلى عشرة مؤشرات مختارة بعناية أُجدي من ثلاثين مؤشرًا يصعب تغذيتها بالبيانات.

جدول (9-1): مؤشرات مقترحة لقياس أداء منظومة GRC

المكوّن	المؤشر	المعادلة أو طريقة القياس	التكرار
الحوكمة	نسبة حضور أعضاء المجلس	الحضور الفعلي ÷ الحضور الواجب × 100	ربع سنوي
الحوكمة	نسبة إغلاق قرارات المجلس في مواعيدها	القرارات المنفذة في موعدها ÷ إجمالي القرارات المستحقة	ربع سنوي
الحوكمة	نسبة السياسات المراجعة ضمن دورتها	السياسات المراجعة في موعدها ÷ إجمالي السياسات السارية	نصف سنوي
المخاطر	نسبة المخاطر ذات خطة معالجة معتمدة	المخاطر التي لها خطة ومالك وتاريخ ÷ إجمالي المخاطر المسجلة	ربع سنوي
المخاطر	نسبة خطط المعالجة المتأخرة	الخطط المتجاوزة تاريخ استحقاقها ÷ إجمالي الخطط النشطة	شهري
المخاطر	عدد تجاوزات حدود التحمل المصغدة	عدّ مباشر مع بيان مدة الاستجابة لكل حالة	ربع سنوي
المخاطر	نسبة تغطية المؤشرات للمخاطر العالية	المخاطر العالية التي لها مؤشر ÷ إجمالي المخاطر العالية	نصف سنوي
الالتزام	نسبة المتطلبات المتحقق منها	المتطلبات التي جرى التحقق منها بدليل ÷ إجمالي المتطلبات	ربع سنوي
الالتزام	عدد حالات عدم الالتزام المكتشفة ذاتيًا	عدّ مباشر، مع نسبة المكتشف ذاتيًا إلى المكتشف خارجيًا	ربع سنوي
الالتزام	متوسط زمن معالجة بلاغات المخالفات	مجموع أيام المعالجة ÷ عدد البلاغات المغلقة	نصف سنوي
التكامل	نسبة تغطية خطة التدقيق للمخاطر العالية	المخاطر العالية المشمولة بالخطة ÷ إجمالي المخاطر العالية	سنوي
التكامل	نسبة الضوابط المسجلة مرة واحدة	الضوابط ذات الرقم الفريد ÷ إجمالي الضوابط الموصوفة	نصف سنوي

المؤشران الأخيران هما مؤشرا التكامل تحديداً، وهما الأقل شيوعاً في الممارسة والأكثر دلالة على أن المنظومة موحدة فعلاً. فإذا كانت نسبة الضوابط المسجلة مرة واحدة منخفضة، فذلك دليل رقمي مباشر على ازدواجية العمل بين الوظائف.

10. تحديات التطبيق ومعالجتها Implementation Challenges

التحديات التالية مستخلصة من أنماط متكررة في السوقين الأردني والخليجي. عرضها هنا ليس تشخيصاً لمنشأة بعينها، بل مادة لمقارنة المنشأة بنفسها.

جدول (1-10): التحديات المتكررة وأسبابها ومعالجتها

التحدي	السبب الجذري الغالب	المعالجة العملية
المنظومة تُدار بوصفها مشروع توثيق	ربط النجاح بعدد الوثائق لا بأثرها على القرار	اجعل معيار النجاح قراراً واحداً على الأقل تتغير بسبب المنظومة كل ربع
مقاومة الوحدات التشغيلية	إدراك المنظومة بوصفها رقابة إضافية عليها	ابدأ من مخاطرة توريق الوحدة فعلاً، وأظهر أن المنظومة تخدمها قبل أن تراقبها
سجل مخاطر جامد لا يتحرك	غياب محفّز للتحديث بين الدورات السنوية	اربط التحديث بأحداث محددة: مشروع جديد، حادثة، تغيير تنظيمي، تجاوز حد تحمل
ازدواج العمل بين المخاطر والالتزام والتدقيق	غياب التصنيف الموحد وسجل الضوابط المركزي	نفذ الشروط الثلاثة الواردة في البند 4-6 قبل أي توسع
ضعف بيانات المؤشرات	تصميم مؤشرات لا تتوفر لها مصادر بيانات	لا يُعتمد مؤشر قبل تحديد مصدر بياناته ومالكه وتكرار توفره
اعتماد الأداة قبل المنهجية	ضغط لإظهار إنجاز سريع	أجل الأتمتة حتى استقرار المنهجية على وحدتين تشغيليتين على الأقل
خلط أدوار الخطين الثاني والثالث	محدودية الموارد في المنشآت المتوسطة	صرّح بالتداخل في الميثاق وضع ضوابط تعويضية ومراجعة خارجية دورية
تقارير طويلة لا تُقرأ	سرد الوضع بدل عرض التغير والقرار	ابدأ التقرير بما تتغير وما هو مطلوب من اللجنة، وآخر التفاصيل إلى الملاحق

11. تطبيق موجز: من التشخيص إلى الأثر

الحالة التالية توضيحية، مركبة من أنماط شائعة ولا تشير إلى منشأة بعينها. الغرض منها إظهار كيف تتصل فصول الدليل ببعضها في سياق واحد.

11-1 وصف الحالة

شركة صناعية أردنية متوسطة، نحو 320 موظفًا، مجلس إدارة من سبعة أعضاء بينهم عضوان مستقلان، ولجنة تدقيق قائمة منذ ثلاث سنوات. لديها دائرة تدقيق داخلي بموظفين اثنين، ومسؤول جودة يتولى ملف شهادات ISO، ولا توجد وظيفة مخاطر أو التزام مستقلة. تصدر نحو 40% من إنتاجها إلى ثلاثة أسواق خليجية.

11-2 ما أظهره التشخيص

- لائحة حوكمة معتمدة قبل أربع سنوات ولم تُراجع بعد تعديل الهيكل التنظيمي مرتين.
- سجل مخاطر أعدّ في ورشة عمل، يضم 46 مخاطرة، 31 منها مصاغة بوصفها ضعفاً قائماً لا احتمالاً مستقبلياً، ولا يوجد لأي منها مالك مسمّى.
- لا يوجد سجل التزامات؛ المتطلبات التنظيمية موزعة بين الدائرة القانونية والمالية والجودة من دون حصر موحد.
- خطة التدقيق الداخلي مبنية على دوران الدوائر لا على المخاطر، ولا ترد فيها المخاطر المتعلقة بتركز الأسواق التصديرية.
- قياس النضج أعطى: الحوكمة 3، السياسات 3، ثقافة المخاطر 2، انضباط العمليات 2، الرغبة في المخاطرة 1، الالتزام 2، البيانات 1، التقارير 2، واجهة التأكيد 2.

11-3 الأولويات التي حُدِّت

7. لم تكن التوصية إعداد مزيد من السياسات، لأن طبقة السياسات كانت أفضل الطبقات نضجاً. الأولويات الثلاث المعتمدة كانت: اعتماد معايير مخاطر وحدود تحمل من المجلس، مع تركيز خاص على حد تركّز المبيعات في سوق واحدة، باعتباره المخاطرة التي كشفها التشخيص ولم تكن مسجلة أصلاً.
8. إعادة صياغة سجل المخاطر بصيغة احتمالية مع تسمية مالك لكل مخاطرة من مديري الدوائر، وتقليص العدد من 46 إلى 24 مخاطرة جوهرية بعد دمج المكرر وفصل المدمج.
9. بناء سجل التزامات موحد يبدأ بالمصادر ذات الأثر التنظيمي المباشر (الضريبة، العمل، اشتراطات التصدير للأسواق الثلاث)، مع ربط كل التزام بمخاطرة في السجل.

11-4 الأثر بعد اثني عشر شهرًا

ارتفع النضج في بُعدي الرغبة في المخاطرة والالتزام من 1 و 2 إلى 3، وبقي بُعد البيانات والتقنية عند 2 لأن الأتمتة أُجِّلَت عن قصد. الأثر الأوضح لم يكن في أرقام النضج بل في قرار واحد: عند دراسة توسعة إنتاجية ممولة باقتراض، عُرض على المجلس تقييم مخاطر مرفق بالدراسة يبيّن أثر التوسعة على حد تركّز الأسواق وعلى نسبة خدمة الدين، فعُذِّل حجم التوسعة وجرى ربط المرحلة الثانية منها بفتح سوق تصديرية رابعة. هذا النوع من الأثر هو المعيار الفعلي لنجاح المنظومة.

12. خلاصة وتوصيات

يمكن اختزال الدليل في ست خلاصات عملية:

10. **GRC** ليس معيارًا يُعتمد ولا برنامجًا يُشترى، بل منهج لربط ثلاث وظائف قائمة أصلًا في معظم المنشآت. قيمة المنهج في الربط لا في المكونات.
11. المكونات الثلاثة تجيب عن أسئلة مختلفة: الحوكمة عن المساءلة، والمخاطر عن عدم اليقين، والالتزام عن الواجب. دمجها في وظيفة واحدة يُضعف كلاً منها.
12. التكامل يتحقق بثلاثة شروط لا رابع لها: تصنيف موحد، ومصدر واحد للضوابط، ودورة تقارير متزامنة. ما دون ذلك تجاور لا تكامل.
13. نموذج الخطوط الثلاثة هو أداة الحسم في نزاعات الأدوار. وحيث يتعذر الفصل التام، يُصرَّح بالتداخل وتُوضع ضوابط تعويضية بدل التظاهر بوجود فصل غير قائم.
14. التسلسل في التنفيذ ليس تفصيلًا إجرائيًا: المعايير قبل السجلات، والمنهجية قبل الأتمتة، والتجريب قبل التعميم.
15. المعيار الوحيد المعتبر لنجاح المنظومة هو أثرها على القرار. منظومة لا يُستشهد بها في قرار واحد خلال ربع سنة هي منظومة توثيق مهما بلغت جودة وثائقها.

1-12 أول ثلاثين يومًا

- للمنشة التي تريد بداية ملموسة قبل أي مشروع كامل، هذه أربع خطوات قابلة للتنفيذ خلال شهر بموارد قائمة:
- احصر مصادر الالتزام المباشرة الأعلى أثرًا (خمسة إلى عشرة مصادر) وسجلها في جدول واحد بمالك وتاريخ تحقق أخير.
- راجع سجل المخاطر القائم وأعد صياغة أعلى عشر مخاطر بصيغة احتمالية، وسمّ مالكا لكل واحدة من مديري الدوائر لا من وظيفة المخاطر.
- اعرض على المجلس أو لجنته المختصة مسودة مقياس أثر بأربعة أبعاد لا اعتمادها، فهذه هي البوابة التي تفتح كل ما بعدها.
- قارن خطة التدقيق الداخلي الحالية بأعلى عشر مخاطر، ووثّق الفجوة. الفجوة نفسها تصلح مادة لأول تقرير **GRC** يُعرض على اللجنة.

ملحق (أ): قائمة تحقق جاهزية منظومة GRC

تُستخدم القائمة للتشخيص السريع. يُجاب عن كل بند بـ «مستوفى» أو «مستوفى جزئياً» أو «غير مستوفى»، مع الإشارة إلى دليل الإثبات. أي بند لا يمكن إسناده بدليل يُعامل معاملة غير المستوفى.

جدول (أ-1): قائمة تحقق الجاهزية

#	بند التحقق	المكون	دليل الإثبات المتوقع
1	وجود لائحة/دليل حوكمة معتمد وساري المفعول	حوكمة	محضر اعتماد ونسخة موقعة
2	مراجعة اللائحة خلال دورتها المقررة	حوكمة	محضر مراجعة أو نسخة معدلة مؤرخة
3	مواثيق معتمدة لجميع اللجان المنبثقة	حوكمة	المواثيق ومحاضر اعتمادها
4	مصفوفة صلاحيات محدثة بعد آخر تغيير هيكل	حوكمة	المصفوفة مع تاريخ آخر تحديث
5	إقرارات تعارض مصالح سنوية موقعة ومحفوظة	حوكمة	سجل الإقرارات
6	خطة عمل سنوية للمجلس تغطي بنود مسؤوليته	حوكمة	الخطة ومحاضر متابعتها
7	سياسة إدارة مخاطر معتمدة من المجلس	مخاطر	السياسة ومحضر الاعتماد
8	مقاييس أثر احتمالية معرفة كمياً ومعتمدة	مخاطر	وثيقة معايير المخاطر
9	بيان رغبة في المخاطرة لكل فئة مخاطر	مخاطر	البيان المعتمد
10	حدود تحمل رقمية مرتبطة ببيان الرغبة	مخاطر	جدول حدود التحمل
11	سجل مخاطر بصياغة احتمالية ومالك مسمى لكل مخاطرة	مخاطر	السجل بنسخته السارية
12	خطط معالجة بمالك وتاريخ استحقاق ومخاطرة متبقية	مخاطر	السجل وأعمدة المعالجة
13	مؤشرات مخاطر بعبئات ومسار تصعيد للمخاطر العالية	مخاطر	بطاقات المؤشرات
14	تحديث السجل عند الأحداث لا سنوياً فقط	مخاطر	سجل التعديلات مع تواريخها
15	سياسة التزام معتمدة ووظيفة ذات وصول مباشر للمجلس	التزام	السياسة والهيكل والميثاق
16	حصر موثق لمصادر الالتزام (عالم الالتزام)	التزام	وثيقة الحصر
17	سجل التزامات بأدلة إثبات وتواريخ تحقق	التزام	السجل بنسخته السارية
18	ربط كل التزام جوهري بمخاطرة في سجل المخاطر	التزام	عمود الربط في السجلين
19	آلية إبلاغ عن المخالفات تحمي هوية المبلغ	التزام	السياسة وسجل البلاغات
20	تقارير حالة التزام دورية ترفع إلى لجنة مختصة	التزام	التقارير ومحاضر المناقشة
21	تصنيف موحد للمخاطر والضوابط معتمد ومستخدم	تكامل	وثيقة التصنيف واستخدامها في السجلات
22	سجل ضوابط مركزي بأرقام فريدة	تكامل	سجل الضوابط
23	دورة تقييم ضوابط موحدة تستفيد منها الوظائف الثلاث	تكامل	خطة التقييم ونتائجها
24	خطة تدقيق داخلي منطلقة من سجل المخاطر المعتمد	تكامل	الخطة وورقة ربطها بالسجل
25	رزمة تقارير موحدة للوظائف الثلاث	تكامل	الرزمة ومحاضر العرض
26	سجل واحد لمتابعة التوصيات من كل المصادر	تكامل	سجل التوصيات

#	بند التحقق	المكوّن	دليل الإثبات المتوقع
27	قياس نضج موثّق يشكّل خط أساس	تكامل	تقرير القياس
28	إثبات على قرار واحد تغيّر بسبب مخرجات المنظومة	تكامل	محضر القرار المرتبط

ملحق (ب): مصفوفة أدوار المنظومة

تُستخدم الرموز التالية: (M) مسؤول عن التنفيذ، (A) معتمد نهائي، (C) يُستشار، (I) يُبلغ. المصفوفة نموذجية وتُكيّف بحسب هيكل المنشأة وحجمها.

جدول (ب-1): مصفوفة الأدوار في أنشطة GRC الرئيسية

النشاط	المجلس ولجانه	الإدارة التنفيذية	المخاطر والالتزام	التدقيق الداخلي
اعتماد سياسة المخاطر والالتزام	A	C	M	I
اعتماد معايير المخاطر وحدود التحمل	A	C	M	I
تحديد المخاطر وتقييمها في الوحدات	I	M	C	I
ملكية المخاطرة وتنفيذ المعالجة	I	M	C	I
تجميع سجل المخاطر والتحديات المنهجية	I	C	M	I
حصر مصادر الالتزام وبناء السجل	I	C	M	I
تشغيل الضوابط الرقابية	I	M	C	I
تقييم تصميم الضوابط وفاعلية تشغيلها	I	C	M	C
التأكيد المستقل على المنظومة	A	I	C	M
اعتماد خطة التدقيق الداخلي	A	C	C	M
رفع تقارير GRC المجمعة	A	C	M	C
متابعة تنفيذ التوصيات	A	M	C	C

ينبغي الانتباه إلى الصفين الخامس والثامن تحديداً: وظيفة المخاطر مسؤولة عن التجميع والتحديات لا عن الملكية، ووظيفة المخاطر تُقيم الضوابط بينما يظل التدقيق الداخلي مستشاراً في هذا النشاط لا منفذاً له، حفاظاً على قدرته على التأكيد المستقل لاحقاً.

ملحق (ج): المسرد الثنائي اللغة

جدول (ج-1): المصطلحات المعتمدة في هذا الدليل

المصطلح بالعربية	المصطلح بالإنجليزية	ملاحظة على الاستخدام
الحوكمة وإدارة المخاطر والالتزام	Governance, Risk & Compliance (GRC)	يُستخدم الاختصار بعد أول ذكر كامل
الأداء المنضبط	Principled Performance	مصطلح OCEG للغاية من التكامل
هيئة الحوكمة	Governing Body	تشمل مجلس الإدارة ومجلس الأمناء
نموذج الخطوط الثلاثة	Three Lines Model	إصدار IIA لعام 2020
الرغبة في المخاطرة	Risk Appetite	بيان نوعي معتمد من المجلس
حدود التحمل	Risk Tolerance	حدود كمية مشتقة من بيان الرغبة
الحدود التشغيلية	Operational Limits	حدود مدمجة في القرار اليومي
المخاطرة المتبقية	Residual Risk	المستوى بعد أثر الضوابط القائمة
المخاطرة الكامنة	Inherent Risk	المستوى قبل اعتبار الضوابط
معايير المخاطر	Risk Criteria	ISO 31000 البند 3-6
سجل المخاطر	Risk Register	صف واحد لكل مخاطرة، بلا دمج
مؤشر المخاطر الرئيسي	Key Risk Indicator (KRI)	يُفضّل المؤشر المتقدم على المتأخر
الرؤية المحفظية	Portfolio View	COSO ERM المبدأ 14
متطلبات الالتزام	Compliance Obligations	إلزامية وطوعية
عالم الالتزام	Compliance Universe	حصر شامل لمصادر الالتزام
مخاطر عدم الالتزام	Compliance Risk	فئة داخل سجل المخاطر لا خارجه
انعدام الرغبة في المخاطرة	Zero Appetite	يُنزج إلى ضوابط مانعة
الضوابط الرقابي	Control	يُوصف مرة واحدة برقم فريد
فاعلية التشغيل	Operating Effectiveness	تُقاس بالاختبار لا بالتصميم
التأكيد المستقل	Independent Assurance	مسؤولية الخط الثالث
إرهاق التأكيد	Assurance Fatigue	أثر ازدواج الاختبار على الوحدات
سجل الفجوات	Gap Register	مخرَج التشخيص
نضج المنظومة	Maturity	خمسة مستويات، تسعة أبعاد
الإبلاغ عن المخالفات	Whistleblowing	مع حماية هوية المبلّغ

ملحق (د): المراجع المعيارية

المراجع مرتبة بحسب المكوّن. أرقام البنود المشار إليها في المتن تعود إلى النسخ المذكورة أدناه؛ ويجب التحقق من صدور نسخ محدّثة قبل الاستناد إليها في وثيقة ملزمة.

د-1 الحوكمة

- مبادئ حوكمة الشركات الصادرة عن مجموعة العشرين ومنظمة التعاون الاقتصادي والتنمية، إصدار 2023 (G20/OECD Principles of Corporate Governance, 2023)
- المواصفة ISO 37000:2021 — Governance of organizations: Guidance
- نموذج الخطوط الثلاثة الصادر عن معهد المدققين الداخليين، 2020 (The IIA's Three Lines Model)
- قانون الشركات الأردني وتعليمات حوكمة الشركات المساهمة المدرجة الصادرة عن هيئة الأوراق المالية، وتعليمات حوكمة البنوك الصادرة عن البنك المركزي الأردني
- نظام الشركات السعودي (2022)، ولانحة حوكمة الشركات الصادرة عن هيئة السوق المالية، وأطر الحوكمة الصادرة عن البنك المركزي السعودي

د-2 إدارة المخاطر

- المواصفة ISO 31000:2018 — Risk management: Guidelines
- المواصفة IEC 31010:2019 — Risk assessment techniques
- إطار COSO Enterprise Risk Management — Integrating with Strategy and Performance (2017)
- إطار COSO Internal Control — Integrated Framework (2013)
- المواصفة ISO 22301:2019 — Business continuity management systems

د-3 الالتزام والنزاهة

- المواصفة ISO 37301:2021 — Compliance management systems: Requirements with guidance for use
- المواصفة ISO 37001:2016 — Anti-bribery management systems
- توصيات مجموعة العمل المالي (FATF Recommendations) وتشريعات مكافحة غسل الأموال وتمويل الإرهاب النافذة في الأردن والسعودية
- قانون حماية البيانات الشخصية الأردني، ونظام حماية البيانات الشخصية السعودي وضوابطه التنفيذية

د-4 التدقيق الداخلي

- المعايير العالمية للتدقيق الداخلي الصادرة عن معهد المدققين الداخليين (Global Internal Audit Standards, 2024)
- الإطار المرجعي الدولي للممارسات المهنية (IPPF) بما يشمل ميثاق التدقيق والتخطيط المبني على المخاطر

د-5 مرجع المفهوم

- نموذج OCEG GRC Capability Model (Red Book)، وهو المصدر الأصلي لمفهوم GRC ولالأداء المنضبط

أحمد أبو منيع، مدقق داخلي معتمد ومتخصص في إدارة المخاطر والحوكمة، يعمل عبر السوقين الأردني والخليجي في مجالات التدقيق الداخلي وإدارة المخاطر المؤسسية والحوكمة والالتزام وتدقيق تقنية المعلومات والتحليل المالي.

حاصل على شهادة المدقق الداخلي المعتمد (CIA)، إضافةً إلى اعتمادات في النمذجة والتحليل المالي (FMVA) وتحليل الائتمان والأعمال (CBCA) والإدارة المالية (CFM) والالتزام الرقابي (CRCM) والتحليل المالي التطبيقي (FTIP). وهو حاصل على درجة البكالوريوس في المحاسبة من جامعة الزرقاء بتقدير امتياز.

مؤسس منصة Free Consultant، التي تربط الممارسين المستقلين المعتمدين بالمشآت الباحثة عن خدمات التدقيق الداخلي وإدارة المخاطر، ويعمل ضمن ترتيبات تعاونية مع مكاتب مهنية في الأردن والسعودية لتنفيذ ارتباطات التدقيق والحوكمة.

للتواصل أو طلب نسخة قابلة للتكليف من الأدوات الواردة في الملاحق: free-consultant.com



نحو قرارات أوضح، وضوابط أقوى

FREE CONSULTANT

بيانات التواصل

البريد الإلكتروني: ahmad.abumanie@outlook.com

الموقع الإلكتروني: www.free-consultant.com

© Free Consultant 2026. جميع الحقوق محفوظة.

يجوز استخدام هذا الدليل لأغراض داخلية غير تجارية مع الإشارة إلى المصدر.