FREE CONSULTANT

كيف تبني سجل مخاطر احترافيًا من الصفر

وفق المواصفة الدولية ISO 31000:2018

دليل عملي للممارس

مرجع تطبيقي يربط بناء السجل بمتطلبات المعايير الدولية للتدقيق الداخلي (GIAS 2024) والنموذج ذي الخطوط الثلاثة وإطار COSO لإدارة مخاطر المؤسسة.

إعداد

أحمد أبو منيع

CIA · FMVA · CBCA · CFM · CRCM · FTIP

المحتويات

1. مقدمة: لماذا يبدأ النضج المؤسسي من سجل المخاطر	3
2. الأساس المرجعي: فهم ISO 31000:2018	3
3. الجسر بين سجل المخاطر ومعايير GIAS 2024	5
4. ما قبل البناء: السياق والنطاق والمعايير وتقبّل المخاطر	6
5. تشريح السجل الاحترافي: بنية الأعمدة	7
6. خارطة الطريق: خمس خطوات للبناء من الصفر	9
7. الخطوة الأولى: تحديد المخاطر وصياغتها	10
8. الخطوة الثانية: التحليل (المتأصّل والمتبقّي)	11
9. الخطوة الثالثة: التقييم وترتيب الأولويات	11
10. الخطوة الرابعة: المعالجة وخطط العمل	12
11. الخطوة الخامسة: الرصد والمراجعة والإبلاغ	13
12. أخطاء شائعة وكيف تتجنّبها	13
13. قائمة تحقق عملية لبناء السجل	14
14. خاتمة	14
حول الكاتب	16

1. مقدمة: لماذا يبدأ النضج المؤسسي من سجل المخاطر

لا تُقاس قدرة المؤسسة على البقاء بحجم أرباحها في سنةٍ جيدة، بل بقدرتها على رؤية ما قد يعصف بها قبل أن يقع. هنا يأتي دور سجل المخاطر. هو ليس جدولًا نملؤه لإرضاء المدقق أو الجهة الرقابية، وليس وثيقةً تُعدّ مرة في السنة وتُنسى في درج. سجل المخاطر، حين يُبنى بطريقة صحيحة، هو الذاكرة المنظَّمة للمؤسسة تجاه ما يهدد أهدافها، وأداتها لتحويل القلق الغامض إلى قراراتٍ واضحة قابلة للمساءلة.

كثير من المؤسسات تملك «سجلًا» بالاسم فقط. تفتح الملف فتجد قائمة مخاطر عامة منسوخة من قوالب جاهزة، صياغتها مبهمة، وتقييمها انطباعي، ولا أحد يعرف من يملك كل خطر ولا متى يُراجَع. هذا النوع من السجلات يمنح شعورًا زائفًا بالأمان، وقد يكون أخطر من غيابه، لأنه يوهم المجلس واللجنة بأن المخاطر مُدارة بينما هي في الحقيقة مجرد كلمات على ورق.

هذا الدليل يأخذك خطوة بخطوة لبناء سجل مخاطر من الصفر، بمنهجية منضبطة تستند إلى المواصفة الدولية ISO 31000:2018، وتتقاطع مع المعايير الدولية للتدقيق الداخلي (GIAS) الصادرة عام 2024، ومع إطار COSO لإدارة مخاطر المؤسسة. الهدف أن تخرج بوثيقةٍ حيّة تُستخدم فعلًا في اتخاذ القرار، لا بنموذجٍ شكلي يُملأ ويُؤرشف.

ما الذي يميّز هذا الدليل؟ أنه عملي بالدرجة الأولى. ستجد فيه بنية الأعمدة التي يحتاجها سجل احترافي، وصياغة المخاطر القائمة على الاحتمالية، وآلية التقييم باستخدام مصفوفة الاحتمالية والأثر، وربط كل ذلك بمتطلبات المعايير التي يُحاسَب عليها المدقق الداخلي. الرسوم التوضيحية المرافقة ليست زينة، بل خرائط تساعدك على تثبيت الفكرة بصريًا قبل التطبيق.

2. الأساس المرجعي: فهم ISO 31000:2018

قبل أن نبني أي سجل، علينا أن نفهم البيت الذي ننتمي إليه. المواصفة الدولية ISO 31000:2018، الصادرة عن المنظمة الدولية للتقييس، هي المرجع العالمي الأوسع قبولًا لإدارة المخاطر. وهي لا تفرض نموذجًا واحدًا يناسب الجميع، بل تقدّم منطقًا متكاملًا يقوم على ثلاثة عناصر مترابطة: المبادئ، والإطار، والعملية.

الشكل (1): البنية الثلاثية للمواصفة ISO 31000:2018.

المبادئ: لماذا ندير المخاطر أصلًا

تنطلق المواصفة من غايةٍ واحدة تحكم كل ما عداها، وهي خلق القيمة وحمايتها. ومن هذه الغاية تتفرّع ثمانية مبادئ تحدد ملامح إدارة المخاطر الجيدة. فهي يجب أن تكون متكاملة مع حوكمة المؤسسة وعملياتها لا منفصلة عنها، ومنظَّمة وشاملة لتعطي نتائج متّسقة، ومُفصّلة على سياق المؤسسة وحجمها وقطاعها لا مستنسخة من غيرها. كما تتطلب الشمول بإشراك أصحاب المصلحة بمعارفهم المختلفة، والديناميكية لأن المخاطر تتغير مع تغير الظروف، والاعتماد على أفضل المعلومات المتاحة مع الإقرار بحدودها، ومراعاة العوامل البشرية والثقافية، والتحسين المستمر بالتعلّم من التجربة.

الإطار: من يحمل المسؤولية وكيف

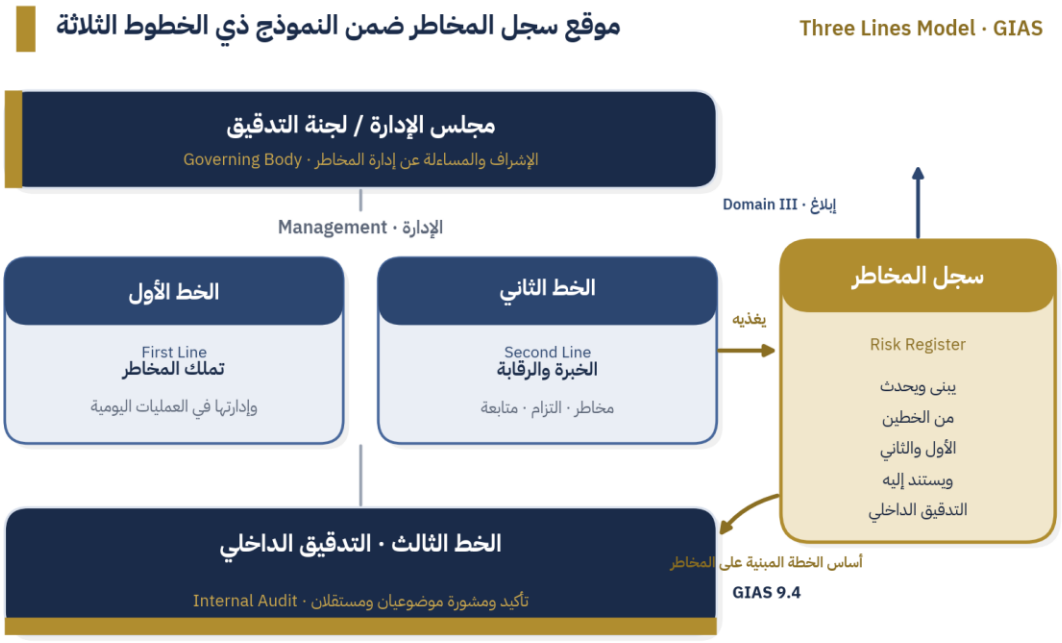
الإطار هو البنية الحوكمية التي تجعل إدارة المخاطر ممكنة ومستدامة. جوهره القيادة والالتزام من مجلس الإدارة والإدارة التنفيذية، إذ لا تنجح أي منهجية مخاطر إن لم تتبنّها القمة فعليًا لا شكليًا. يدور الإطار في حلقةٍ تبدأ بالتكامل مع هياكل الحوكمة، ثم التصميم الذي يحدد الأدوار والموارد والسياسات، فالتطبيق على أرض الواقع، ثم التقييم لقياس الفاعلية، وأخيرًا التحسين الذي يعيد ضخّ الدروس في الدورة من جديد. سجل المخاطر هو أحد أبرز المخرجات الملموسة لهذا الإطار.

العملية: الخطوات التنفيذية

العملية هي الجزء الذي نلمسه يوميًا، وهي ما يترجم المبادئ والإطار إلى ممارسة. وتتألف من تحديد السياق ووضع المعايير، ثم تقييم المخاطر بمراحله الثلاث (التحديد والتحليل والتقدير)، فالمعالجة، يحفّ بها على الدوام التواصل والتشاور من جهة، والرصد والمراجعة من جهة أخرى، مع التوثيق والإبلاغ في كل مرحلة. الفصل القادم يفصّل هذه العملية، لأنها العمود الفقري لبناء السجل.

3. الجسر بين سجل المخاطر ومعايير GIAS 2024

بالنسبة للمدقق الداخلي، سجل المخاطر ليس وثيقةً تخص الإدارة وحدها، بل نقطة ارتكاز لعمله كله. المعايير الدولية للتدقيق الداخلي الصادرة عن معهد المدققين الداخليين عام 2024، والمعروفة اختصارًا بـ Global Internal Audit Standards، حلّت محل الإطار المهني السابق، وهي تربط جودة وظيفة التدقيق ارتباطًا مباشرًا بفهمٍ سليم للمخاطر.



الشكل (2): موقع سجل المخاطر ضمن النموذج ذي الخطوط الثلاثة.

النموذج ذو الخطوط الثلاثة، الذي أصدره معهد المدققين الداخليين في صيغته المحدّثة عام 2020، يوضّح أين يقف السجل. الخط الأول يملك المخاطر ويديرها في صلب العمليات اليومية. الخط الثاني يوفّر الخبرة والرقابة ويُسهم في تصميم منهجية المخاطر ومتابعتها. أما التدقيق الداخلي فيمثّل الخط الثالث، يقدّم تأكيدًا ومشورةً موضوعيين ومستقلّين، ويعتمد في تخطيطه على ما يفرزه السجل من معلومات. مجلس الإدارة، عبر لجنة التدقيق، يمارس الإشراف والمساءلة على مدى نضج إدارة المخاطر.

المتطلبات ذات الصلة في GIAS

المعيار 9.4 (خطة التدقيق الداخلي): يُلزم رئيس التدقيق الداخلي بأن تكون خطة التدقيق مبنية على المخاطر، وأن تأخذ في الحسبان تقييم المخاطر على مستوى المؤسسة. عمليًا، السجل الجيد هو المُدخل الأهم لهذه الخطة؛ فالمخاطر ذات القيمة الأعلى توجّه نطاق المهام وأولوياتها.

المبدأ 9 (التخطيط الاستراتيجي): يضع على عاتق الوظيفة فهم عمليات الحوكمة وإدارة المخاطر والرقابة في المؤسسة، وهو فهم لا يكتمل دون سجلٍ موثوق يعكس صورة المخاطر الفعلية لا المتخيَّلة.

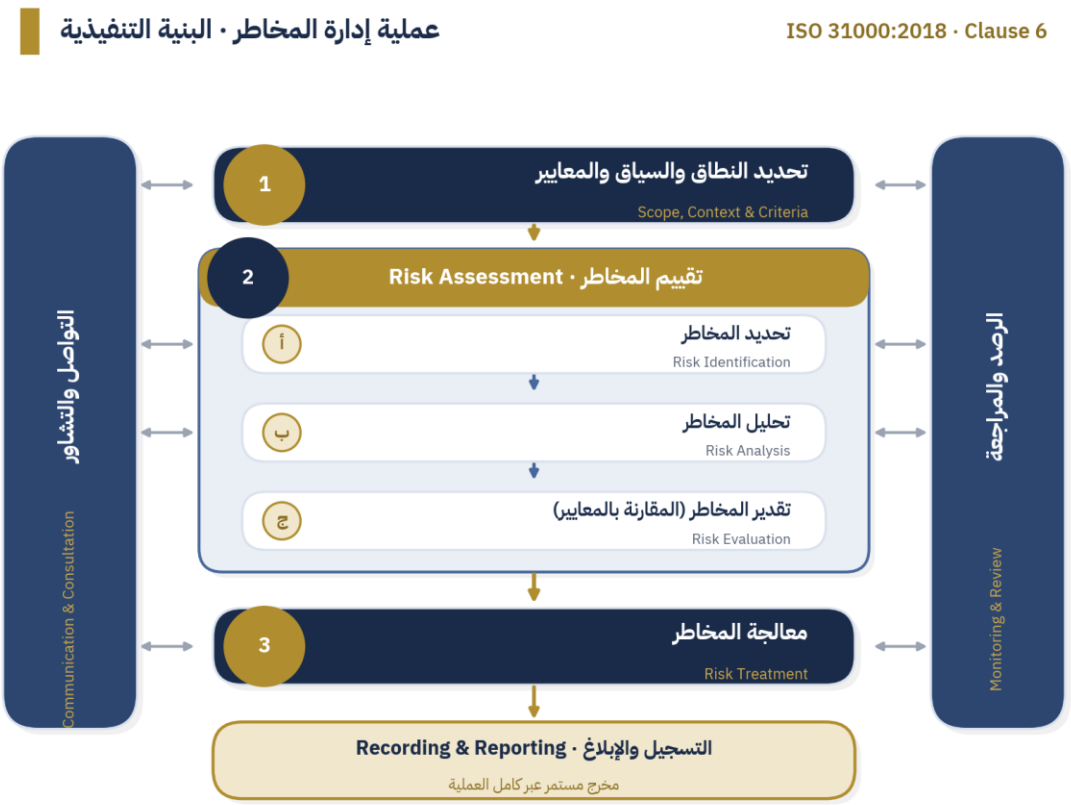
المعيار 13.2 (تقييم مخاطر المهمة): يتطلب عند التخطيط لكل مهمة إجراء تقييمٍ لمخاطرها يستند إلى السجل المؤسسي ويُحدِّثه في الوقت ذاته. هكذا تتغذّى المهمة من السجل، وتردّ إليه ما تكتشفه من مخاطر أو تغيّرات.

النطاق الثالث (حوكمة وظيفة التدقيق): يكرّس مسؤولية الإشراف لدى المجلس، ومن ذلك متابعة كيفية إدارة المخاطر والإبلاغ عنها. تقرير المخاطر المنبثق من السجل هو أحد أهم ما يُرفع للجنة التدقيق.

الخلاصة أن بناء سجل مخاطر متين ليس ترفًا تنظيميًا، بل التزامٌ يخدم المدقق في خطته، وفي مهامه، وفي تقاريره للمجلس. السجل الضعيف ينعكس ضعفًا في كل حلقةٍ تالية.

4. ما قبل البناء: السياق والنطاق والمعايير وتقبّل المخاطر

الخطأ الأكثر شيوعًا أن يبدأ الفريق بتعداد المخاطر مباشرة. هذا يقود إلى سجلٍ مشتّت بلا مرجعية. المنهج السليم وفق ISO 31000 يبدأ بتأسيس الأرضية: تحديد السياق، وحدود النطاق، ومعايير المخاطر، وبيان تقبّل المخاطر. هذه الأسس هي التي تجعل التقييم لاحقًا متّسقًا وقابلًا للدفاع عنه.



الشكل (3): عملية إدارة المخاطر وفق البند السادس من ISO 31000:2018.

تحديد السياق الداخلي والخارجي

السياق الخارجي يشمل البيئة التنظيمية والاقتصادية والتقنية والتنافسية التي تعمل فيها المؤسسة، وتوقعات أصحاب المصلحة والجهات الرقابية. والسياق الداخلي يشمل الأهداف الاستراتيجية، والهيكل التنظيمي، والثقافة، والموارد، والأنظمة. تحليل السياق ليس تمرينًا أكاديميًا؛

فهو ما يحدد أي المخاطر ذات صلة بهذه المؤسسة بالذات. أداة مثل PESTLE تساعد على مسح العوامل الخارجية، بينما يكشف تحليل SWOT عن مواطن الضعف الداخلية التي قد تتحول إلى مخاطر.

رسم حدود النطاق

النطاق يحدد ما الذي يغطّيه السجل: المؤسسة بأكملها، أم وحدة أعمال، أم عملية بعينها، أم مشروع. كلما اتسع النطاق ازدادت الحاجة إلى تصنيف المخاطر في فئات منطقية، مثل المخاطر الاستراتيجية والتشغيلية والمالية والامتثالية ومخاطر السمعة والمخاطر التقنية والسيبرانية. هذا التصنيف يجعل السجل قابلًا للقراءة والتجميع والمقارنة عبر الوحدات.

معايير المخاطر: مقياس الاحتمالية والأثر

معايير المخاطر هي المسطرة التي نقيس بها. يجب الاتفاق مسبقًا على سُلَّم للاحتمالية (مثلًا من «نادر» إلى «شبه مؤكد») وسُلَّم للأثر (من «ضئيل» إلى «جسيم»)، مع وصفٍ كميّ أو نوعيّ لكل درجة. الأثر لا يُقاس ماليًا فقط؛ فقد يكون أثرًا على السمعة أو على الالتزام التنظيمي أو على سلامة الأفراد. توحيد هذه المعايير عبر المؤسسة شرطٌ لأي مقارنة عادلة بين المخاطر.

بيان تقبّل المخاطر وحدود التحمل

هنا يدخل مفهوم محوري كثيرًا ما يُهمل. تقبّل المخاطر (Risk Appetite) هو مقدار المخاطر الذي تكون المؤسسة مستعدة لقبوله سعيًا وراء أهدافها، بينما حدود التحمل (Risk Tolerance) هي الانحراف المسموح حول هذا المستوى. هذان المفهومان، اللذان يفصّلهما إطار COSO لإدارة مخاطر المؤسسة، هما ما يحوّل التقييم إلى قرار. فالخطر لا يُعالَج لأنه «مرتفع» فحسب، بل لأنه يتجاوز ما قرّر المجلس أنه مستعد لتحمّله. من دون هذا الخط الفاصل يصبح ترتيب الأولويات اجتهادًا بلا مرساة.

5. تشريح السجل الاحترافي: بنية الأعمدة

ما الذي يجعل سجلًا «احترافيًا» وآخر مجرد قائمة؟ الجواب في بنيته. السجل الاحترافي يحكي قصة كل خطر كاملة: من تعريفه وتصنيفه، إلى تحليله قبل الضوابط، إلى الضوابط القائمة، إلى ما يتبقّى بعدها، وصولًا إلى خطة معالجته ومالكها ومتابعتها. الرسم التالي يلخّص هذه البنية في خمس مجموعات.

الشكل (4): المجموعات والأعمدة الأساسية لسجل مخاطر احترافي.

المجموعة الأولى: التعريف والتصنيف

تبدأ بمرجعٍ فريد لكل خطر يسهّل الإحالة والتتبّع، ثم العملية الرئيسية والعملية الفرعية التي ينتمي إليها الخطر. بعدها يأتي قلب الصياغة: عنوان الخطر، ووصفه، وسببه الجذري. الفصل بين هذه الثلاثة ليس تجميلًا، بل ضرورة منهجية تضمن وضوح ما نتحدث عنه. ويُستحسن إضافة عمود لأفضل الممارسات أو الضابط المرجعي المرتبط بالخطر، يُبيّن ما ينبغي أن يكون عليه الوضع المثالي.

قاعدة الصياغة القائمة على الاحتمالية: اكتب كل خطر بوصفه احتمالًا لا واقعًا. الصيغة المتينة تربط ثلاثة عناصر: السبب الجذري، ثم الحدث المحتمل، ثم الأثر على الهدف. مثال: «نتيجة ضعف ضوابط الوصول المنطقي (سبب)، قد يحدث وصول غير مصرّح به لبيانات العملاء (حدث)، ما يؤدي إلى غرامات تنظيمية وضرر بالسمعة (أثر)». هذه الصياغة وحدها ترفع جودة السجل قفزة كاملة.

المجموعة الثانية: التحليل المتأصّل

هنا نقيّم الخطر قبل أثر أي ضابط، أي في صورته الخام. نسجّل الاحتمالية والأثر وفق المعايير المتّفق عليها، ثم نحسب قيمة الخطر بضربهما (الاحتمالية × الأثر). هذا هو الخطر المتأصّل أو الكامن، وهو يكشف حجم التهديد الفعلي لو غابت الرقابة.

المجموعة الثالثة: الضوابط القائمة

نوثّق هنا الضوابط الموجودة فعلًا لمواجهة الخطر، ونحكم على مدى كفاية تصميمها وفاعلية تشغيلها. الفرق جوهري: ضابط مصمَّم جيدًا لكنه لا يُطبَّق لا قيمة له. تقييم الضوابط بصدق هو ما يميّز السجل الواقعي عن السجل المتفائل.

المجموعة الرابعة: المخاطر المتبقية

بعد إنزال أثر الضوابط، نعيد تقدير الاحتمالية والأثر لنصل إلى الخطر المتبقّي (Residual Risk). هذا هو الرقم الذي يُقارَن ببيان تقبّل المخاطر. إن كان ضمن الحدّ المقبول اكتفينا بالمراقبة، وإن تجاوزه استوجب معالجة إضافية. الفرق بين المتأصّل والمتبقّي هو القيمة الفعلية التي تضيفها الرقابة، وهو في حد ذاته مؤشر على نضج بيئة الضبط.

المجموعة الخامسة: المعالجة والحوكمة

تشمل استراتيجية المعالجة، وخطة العمل، والمالك المسؤول، وتاريخ الاستحقاق، ومؤشر الخطر الرئيس المرتبط، وحالة التنفيذ. هذه المجموعة هي ما يحوّل السجل من تشخيصٍ إلى التزام. خطر بلا مالكٍ وتاريخٍ هو خطر متروك.

مبدأ غير قابل للتفاوض: كل خطر في صفٍّ مستقل، ولا دمج للخلايا إطلاقًا. الدمج يكسر إمكانية الفرز والتصفية والتجميع آليًا، ويُفسد أي تحليل لاحق للبيانات. السجل أداة بيانات قبل أن يكون مستندًا، ويجب أن يُعامَل كذلك.

6. خارطة الطريق: خمس خطوات للبناء من الصفر

بعد أن فهمنا البنية، ننتقل إلى التنفيذ. بناء السجل ليس حدثًا لمرة واحدة بل دورة متكررة. الرسم التالي يلخّص الرحلة في خمس خطوات، تُغذّي كلٌّ منها ما يليها، وتعود الحلقة لتبدأ من جديد مع كل دورة مراجعة.

الشكل (5): خارطة طريق بناء السجل في خمس خطوات.

الفصول الخمسة التالية تتناول كل خطوة بالتفصيل العملي: ماذا نفعل فيها، وبأي أدوات، وما المخرج المتوقّع منها. اتبعها بالترتيب في أول دورة، ثم ستجد إيقاعك الخاص في الدورات اللاحقة.

7. الخطوة الأولى: تحديد المخاطر وصياغتها

لا يمكن إدارة ما لا نراه. هدف هذه الخطوة مسحٌ منهجي يكشف المخاطر التي قد تعرقل أهداف المؤسسة، بأكبر قدر من الشمول. الاعتماد على شخصٍ واحد أو على قائمة جاهزة يترك ثغرات خطيرة. الأسلوب الأنضج يجمع بين مصادر متعددة.

أدوات التحديد

ورش العمل التشاركية مع أصحاب العمليات تستخرج المخاطر من أقرب الناس إليها. المقابلات الفردية مع القيادات تكشف الهواجس الاستراتيجية. مراجعة البيانات التاريخية والحوادث السابقة وسجلات الشكاوى تكشف أنماطًا متكررة. أدوات المسح البيئي مثل PESTLE وتحليل SWOT تضمن تغطية العوامل الخارجية والداخلية. وتقييم الرقابة الذاتية (RCSA) يُشرك الإدارة في تشخيص مخاطرها وضوابطها معًا.

تحليل ربطة العنق لفهم الخطر بعمق

من أقوى الأدوات البصرية لتفكيك خطرٍ مهم تحليل ربطة العنق (Bow-Tie). يضع الحدث المحوري في المنتصف، ويصطفّ على يساره مصادر التهديد والضوابط الوقائية التي تمنع وقوعه، وعلى يمينه العواقب المحتملة وضوابط التخفيف والتعافي التي تحدّ من أثرها بعد الوقوع. هذه الصورة تكشف بوضوح أين تتركّز ضوابطنا وأين توجد الفجوات.

الشكل (6): مثال تطبيقي على تحليل ربطة العنق لخطر تسرّب بيانات العملاء.

لاحظ في المثال كيف أن الضوابط الوقائية (إدارة الهويات والصلاحيات، التوعية ومحاكاة التصيّد، تشفير الأجهزة) تعمل على منع الحدث، بينما ضوابط التعافي (خطة الاستجابة للحوادث، إشعار الجهات والعملاء، النسخ الاحتياطي) تعمل على احتواء الأثر بعد وقوعه. الفصل بين النوعين يساعد على بناء خطة معالجة متوازنة لا تركّز على المنع وتُهمل التعافي.

نتيجة الخطوة: قائمة مخاطر أولية مصاغة بطريقة قائمة على الاحتمالية (سبب ثم حدث ثم أثر)، مصنّفة في فئاتها، ومسجّلة كلٌّ منها في صفٍّ مستقل، جاهزة للانتقال إلى التحليل.

8. الخطوة الثانية: التحليل (المتأصّل والمتبقّي)

بعد التحديد، نحلّل. التحليل يجيب عن سؤالين: ما حجم الخطر لو غابت الرقابة؟ وما حجمه بعد الرقابة القائمة؟ الفرق بينهما هو ما يكشف فاعلية بيئة الضبط ويوجّه قرار المعالجة.

التقدير المتأصّل قبل الضوابط

نقدّر لكل خطر احتماليته وأثره وفق السلالم المتّفق عليها في معايير المخاطر، ثم نحسب قيمته المتأصّلة بضربهما. من المهم أن يكون التقدير مستندًا إلى أدلة قدر الإمكان لا إلى انطباعٍ فردي، وأن يشارك فيه أكثر من خبير لتقليل التحيّز. تسجيل المنطق وراء كل تقدير يرفع شفافية السجل ويسهّل مراجعته.

تقييم كفاية الضوابط وفاعليتها

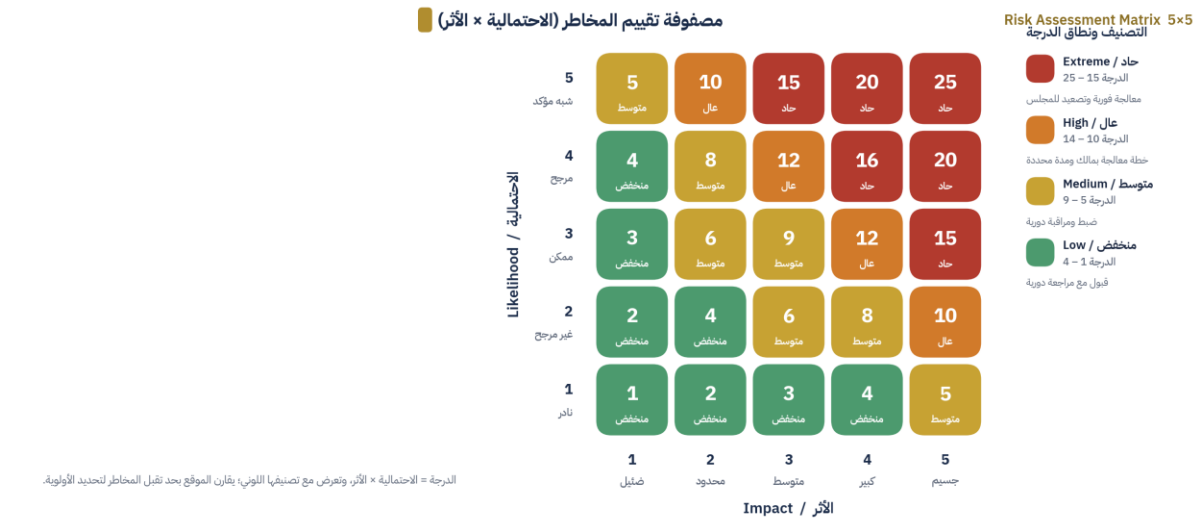
نفحص الضوابط القائمة من زاويتين. كفاية التصميم: هل الضابط مصمَّم بحيث يعالج الخطر فعلًا لو طُبِّق كما ينبغي؟ وفاعلية التشغيل: هل يُطبَّق باستمرار وباتساق على أرض الواقع؟ إطار COSO للرقابة الداخلية الصادر عام 2013 يقدّم مرجعية مفيدة لتقييم مكوّنات الرقابة. ضابطٌ ضعيف التصميم أو متقطّع التشغيل لا يُخفّض الخطر بالقدر المفترض، وهذا ما يجب أن ينعكس في التقدير المتبقّي.

التقدير المتبقّي بعد الضوابط

في ضوء تقييم الضوابط، نعيد تقدير الاحتمالية والأثر لنصل إلى الخطر المتبقّي. هذا الرقم هو الأهم عمليًا، لأنه يعبّر عن وضع المؤسسة الحقيقي اليوم. إن كانت الضوابط قوية انخفض المتبقّي كثيرًا عن المتأصّل، وإن كانت هشّة بقي الرقمان متقاربين، وهذه إشارة إنذار. تذكّر أن الهدف ليس تصفير الخطر، فذلك مستحيل ومكلف، بل إنزاله إلى ما دون حدّ التقبّل.

9. الخطوة الثالثة: التقييم وترتيب الأولويات

التحليل أعطانا أرقامًا، والتقييم يحوّلها إلى قرارات. هنا نقارن كل خطر متبقٍّ ببيان تقبّل المخاطر، ونرتّب الأولويات بناءً على من يتجاوز الحدّ ومن يقترب منه. الأداة الأشهر لهذا الغرض هي مصفوفة تقييم المخاطر، أو الخريطة الحرارية.



الشكل (7): مصفوفة تقييم المخاطر (الاحتمالية × الأثر) بأربعة تصنيفات.

في هذه المصفوفة، يقع كل خطر في خليةٍ تتحدد بدرجة احتماليته (المحور الرأسي) ودرجة أثره (المحور الأفقي). حاصل ضربهما يعطي درجة الخطر التي تصنَّف لونيًا في أربع فئات: منخفض (1 إلى 4) باللون الأخضر، ومتوسط (5 إلى 9) بالكهرماني، وعالٍ (10 إلى 14) بالبرتقالي، وحادّ (15 إلى 25) بالأحمر. عرض التصنيف بالكلمة واللون معًا، لا بالرقم وحده، يجعل المصفوفة مفهومة لغير المختصين في المجلس واللجان.

من اللون إلى القرار

التصنيف اللوني ليس غاية بل توجيه. الخطر الحادّ يستدعي معالجة فورية وتصعيدًا للمجلس. والعالي يحتاج خطة معالجة بمالكٍ ومدّةٍ محددة. والمتوسط يُضبط ويُراقب دوريًا. والمنخفض يُقبَل مع مراجعة دورية للتأكد من بقائه كذلك. لكن الحاكم النهائي يبقى موقع الخطر من حدّ التقبّل المعتمد؛ فقد تقرر مؤسسةٌ ما أن خطرًا «متوسطًا» في مجال حسّاس كالامتثال يستحق معالجةً تفوق ما يوحي به لونه. المصفوفة ترشد، وبيان التقبّل يحكم.

10. الخطوة الرابعة: المعالجة وخطط العمل

وصلنا إلى حيث تتحول الإدارة من فهمٍ إلى فعل. لكل خطر يتجاوز حدّ التقبّل، نختار استراتيجية معالجة. توفّر ISO 31000 أربعة خيارات رئيسية، تُعرف عمليًا بالـ«T» الأربع.

الخيارات الأربعة للمعالجة

التجنّب (Avoid): الامتناع عن النشاط المسبّب للخطر أصلًا، حين يفوق خطره أي عائد محتمل. مثل التوقف عن خط منتجٍ عالي المخاطر أو الانسحاب من سوقٍ غير مستقر.

التخفيض (Reduce): الخيار الأكثر شيوعًا، ويعني تعزيز الضوابط لخفض الاحتمالية أو الأثر أو كليهما. مثل إضافة المصادقة الثنائية لتقليل احتمالية الاختراق.

المشاركة أو التحويل (Share / Transfer): نقل جزء من عبء الخطر إلى طرفٍ آخر، عبر التأمين أو التعاقد الخارجي أو شروط تعاقدية. لا ينقل المسؤولية كاملة، لكنه يوزّع الأثر المالي.

القبول (Accept): الإبقاء على الخطر عن وعيٍ وقرار، حين يكون ضمن حدّ التقبّل أو حين تفوق كلفة معالجته فائدتها. القبول قرارٌ موثّق لا إهمالٌ صامت.

من الاستراتيجية إلى خطة عمل قابلة للتنفيذ

اختيار الاستراتيجية وحده لا يكفي. كل معالجة تحتاج خطة عملٍ محددة المعالم: ماذا سيُنفَّذ بالضبط، ومن يملك التنفيذ بالاسم لا بالمسمّى، وما تاريخ الاستحقاق، وما المؤشر الذي نعرف به أن المعالجة أثمرت. بعد تنفيذ المعالجة يُعاد تقدير الخطر المتبقّي مجددًا، للتأكد من أنه نزل فعلًا إلى ما دون حدّ التقبّل. هذه الحلقة المغلقة هي ما يمنع تحوّل خطط المعالجة إلى وعودٍ معلّقة.

تنبيه عملي: احذر «المعالجة الورقية»، أي تسجيل إجراءٍ في السجل دون موازنةٍ ولا مالكٍ حقيقي ولا متابعة. هذه أخطر من ترك الخطر دون معالجة، لأنها توهم بأن الأمر تحت السيطرة.

11. الخطوة الخامسة: الرصد والمراجعة والإبلاغ

السجل ليس وثيقةً نُنجزها ثم نغلقها. المخاطر تتغير، وتظهر مخاطر جديدة، وتتآكل فاعلية الضوابط مع الوقت. هذه الخطوة هي ما يبقي السجل حيًّا ومفيدًا، وهي مسؤولية مشتركة بين الخطوط الثلاثة.

مؤشرات المخاطر الرئيسة

مؤشرات المخاطر الرئيسة (KRIs) هي إشارات إنذار مبكر تنبّه إلى تصاعد خطرٍ ما قبل أن يقع. اختيار مؤشر جيد لكل خطرٍ مهم، مع تحديد عتبة للتنبيه، يحوّل الرصد من ردّ فعلٍ متأخر إلى استباقٍ منضبط. مثلًا، ارتفاع نسبة محاولات الدخول الفاشلة قد يكون مؤشرًا مبكرًا على خطرٍ سيبراني متصاعد.

دورية المراجعة

تُحدَّد وتيرة مراجعة منتظمة تتناسب مع طبيعة كل خطر؛ فالمخاطر عالية التقلب تُراجَع أكثر من المستقرة. وإلى جانب الدورية المجدولة، تستوجب الأحداث الكبرى كالتغيّرات التنظيمية أو إطلاق منتجٍ جديد أو حادثٍ جسيم مراجعةً فورية. كل مراجعة تعيد تقدير المخاطر، وتُحدّث الضوابط، وتغلق المعالَج، وتفتح ما استجدّ.

الإبلاغ للجنة التدقيق والمجلس

القيمة النهائية للسجل تظهر في الإبلاغ. تقرير المخاطر الذي يُرفع للجنة التدقيق ينبغي أن يكون مركّزًا وبصريًا، يبرز المخاطر الحادّة والعالية وحالة معالجتها واتجاهها صعودًا أو هبوطًا. هذا الإبلاغ يخدم مسؤولية الإشراف المنصوص عليها في معايير GIAS ضمن النطاق الثالث، ويغذّي مبدأ التواصل الفعّال. السجل الذي لا يصل إلى صانع القرار في صورةٍ مفهومة يفقد نصف قيمته.

12. أخطاء شائعة وكيف تتجنّبها

بعد بناء عدّة سجلات تتكرر أمامك الأخطاء ذاتها. الوعي بها مسبقًا يوفّر عليك دوراتٍ من التصحيح.

الصياغة الفضفاضة: كتابة الخطر ككلمةٍ واحدة مثل «السيولة» أو «السمعة» دون سبب ولا حدث ولا أثر. العلاج صياغة قائمة على الاحتمالية تفصل العناصر الثلاثة.

النسخ من القوالب: تبنّي قائمة مخاطر جاهزة لا تعكس سياق المؤسسة. العلاج البدء من تحليل السياق والنطاق الخاصّين بك.

الخلط بين المتأصّل والمتبقّي: تقييم الخطر مرة واحدة دون تمييز ما قبل الضوابط عمّا بعدها. العلاج عمودان منفصلان للتقدير، يفصل بينهما تقييم صريح للضوابط.

غياب المالك والتاريخ: تسجيل المعالجة دون مسؤولٍ محدد ولا موعد. العلاج إلزام كل معالجة بمالكٍ بالاسم وتاريخ استحقاق ومؤشر متابعة.

دمج الخلايا والجمع بين المخاطر في صفّ واحد: ما يكسر الفرز والتحليل. العلاج قاعدة صارمة: خطر واحد لكل صفّ، ولا دمج إطلاقًا.

السجل الميت: إعداده مرة ثم إهماله. العلاج دورية مراجعة معتمدة، ومؤشرات إنذار، وإبلاغ منتظم للجنة التدقيق.

تجاهل تقبّل المخاطر: ترتيب الأولويات باللون وحده دون مرجعية. العلاج اعتماد بيان تقبّل وحدود تحمّل يقارَن بهما كل خطر متبقٍّ.

13. قائمة تحقق عملية لبناء السجل

استخدم هذه القائمة كمرجعٍ سريع للتأكد من اكتمال سجلك قبل اعتماده. كل بندٍ يلخّص فكرة أصّلناها في هذا الدليل.

1. حُدّد السياق الداخلي والخارجي وتوقعات أصحاب المصلحة بوضوح.
2. رُسمت حدود نطاق السجل (مؤسسة / وحدة / عملية / مشروع) وصُنّفت المخاطر في فئات منطقية.
3. اعتُمدت معايير المخاطر: سلالم للاحتمالية والأثر بأوصاف كمية أو نوعية موحّدة.

4. صدر بيان تقبّل المخاطر وحدود التحمّل من مستوى الحوكمة المناسب.
5. حُدّدت المخاطر من مصادر متعددة (ورش، مقابلات، بيانات تاريخية، RCSA، SWOT، PESTLE).
6. صيغ كل خطر بطريقة قائمة على الاحتمالية: سبب جذري ثم حدث محتمل ثم أثر على الهدف.
7. قُدّر الخطر المتأصّل (الاحتمالية × الأثر) قبل أثر أي ضابط.
8. وُثّقت الضوابط القائمة، وقُيّمت كفاية تصميمها وفاعلية تشغيلها بصدق.
9. أُعيد تقدير الخطر المتبقّي بعد الضوابط وقورن ببيان التقبّل.
10. اختيرت استراتيجية معالجة لكل خطر متجاوز (تجنّب / تخفيض / مشاركة / قبول).
11. لكل معالجة خطة عمل بمالكٍ بالاسم وتاريخ استحقاق ومؤشر متابعة.
12. حُدّدت مؤشرات مخاطر رئيسة (KRIs) بعتبات تنبيه للمخاطر المهمة.
13. اعتُمدت دورية مراجعة منتظمة، مع مراجعة فورية عند الأحداث الكبرى.
14. صُمّم تقرير مخاطر بصري للجنة التدقيق والمجلس يبرز الحادّ والعالي واتجاهه.
15. طُبّقت قاعدة: خطر واحد لكل صفّ، ولا دمج للخلايا، والسجل قابل للفرز والتحليل.

14. خاتمة

سجل المخاطر الاحترافي ليس إنجازًا تقنيًا بقدر ما هو تعبير عن نضج المؤسسة في التفكير في مستقبلها. حين تُبنى كل خانةٍ فيه بوعي، من صياغة الخطر إلى تقدير المتبقّي إلى متابعة المعالجة، يتحول السجل من عبءٍ امتثالي إلى أداةٍ للقيادة الرشيدة. والمدقق الداخلي الذي يتقن قراءة هذا السجل وبناءه يضع يده على المُدخل الأهم لخطته ومهامه وتقاريره.

ابدأ بسيطًا ومتينًا، ثم طوّر مع كل دورة. سجلٌ متواضع الحجم لكنه صادق ومحدَّث وحيّ، خيرٌ من جدولٍ ضخم منسوخ لا يقرأه أحد. القيمة ليست في عدد الصفوف، بل في صدق ما تحمله وفي القرارات التي تنبثق منه.

حول الكاتب

أحمد أبو منيع

CIA · FMVA · CBCA · CFM · CRCM · FTIP

راكم أحمد خبرة عملية ممتدّة في حوكمة الشركات وإدارة المخاطر المؤسسية والرقابة الداخلية والامتثال التنظيمي، عبر مؤسساتٍ متنوعة في دول الخليج والأردن. ينصبّ اهتمامه على تحويل الأطر النظرية إلى أدواتٍ عملية قابلة للتطبيق، وعلى بناء مخرجاتٍ مهنية عالية الجودة تخدم صانع القرار فعلًا لا شكلًا.

يجمع بين عمقٍ في حوكمة المخاطر والامتثال (GRC) وإدارة المخاطر المؤسسية (ERM)، وخبرةٍ في تدقيق نظم المعلومات والمراجعات التنظيمية أمام الجهات الرقابية في المنطقة. ويستند في عمله إلى المعايير والأطر الدولية المعتمدة، من ISO 31000 وإطار COSO إلى المعايير الدولية للتدقيق الداخلي الصادرة عن معهد المدققين الداخليين، مع حرصٍ على مواءمتها مع البيئة التنظيمية المحلية في كل بلد.

يحمل عددًا من الشهادات المهنية الدولية، من بينها شهادة المدقق الداخلي المعتمد (CIA)، ومحلل النمذجة والتقييم المالي (FMVA)، ومحلل الائتمان والمصرفية المعتمد (CBCA)، إلى جانب مؤهلاتٍ في الإدارة المالية وإدارة المخاطر والامتثال. هذا التنوّع يمنح طرحه زاويةً تكاملية تربط المخاطر بالمال وبالحوكمة في آنٍ واحد.

معلومات التواصل

البريد الالكتروني : Ahmad.abumanie@outlook.com