insights

التهديدات السيبرانية

ومخاطر الذكاء الاصطناعي:
هل التدقيق الداخلي الخاص بك جاهز؟

2025

"إعادة تعريف دور التدقيق الداخلي في الحد من إساءة استخدام الذكاء الاصطناعي والثغرات الأمنية السيبرانية"

مجلد III

العمل وفق معايير معهد المدققين الداخليين ٢٠٢٤
وأولويات رؤية السعودية ٢٠٣٠

www.insightss.co/ar

شركة إنسايتس للإدارة والاستشارا المالية

التدقيق الداخلي ٢٠٢٥

التوافق مع المعايير العالمية الجديدة والمخاطر الناشئة لعام 2025

الجدول الزمني لنشر الرؤى:

الفصل I

معايير التدقيق الداخلي العالمية الجديدة الصادرة عن معهد المدققين الداخليين (IIA) – ما يجب أن تعرفه الشركات السعودية

13 مايو 2025

الفصل II

إدارة المخاطر – دمجها في عملية التدقيق الداخلي

28 مايو 2025

الفصل III

الأمن السيبراني والذكاء الاصطناعي – أهم المخاطر التي تواجه المدققين الداخليين

يونيو 2025

الفصل IV

الحوكمة والأخلاقيات والحوكمة البيئية والاجتماعية والمؤسسية – الركائز الأساسية للمدقق المستقبلي

يوليو 2025

الفصل V

الابتكار في التدقيق الداخلي وتحليلات البيانات، Agile – والأتمتة

يوليو 2025

التدقيق الداخلي في مواجهة المخاطر الرقمية

تُصنّف معايير التدقيق الداخلي العالمية لعام ٢٠٢٤ الأمن السيبراني كأولوية أساسية في التدقيق. ويُتوقع من المدققين الداخليين الآن تقييم مدى كفاية حوكمة الأمن السيبراني (بما يتماشى مع المجال الخامس: أداء خدمات التدقيق الداخلي – المبدآن ١٣ و١٤)، واختبار فعالية الضوابط، وتقييم الاستعداد للحوادث، بما يضمن توافق هذه الجهود مع أهداف إدارة المخاطر المؤسسية وأطر الأمن السيبراني الوطنية.

في بيئة اليوم، تُعد التهديدات السيبرانية ديناميكية ومتشابكة بشكل وثيق مع الاستراتيجية والامتثال والسمعة. بالنسبة للمؤسسات الناشئة في ظل رؤية المملكة العربية السعودية ٢٠٣٠، تلعب وظيفة التدقيق الداخلي دورا محوريا في تعزيز الثقة الرقمية والحد من المخاطر السيبرانية وضمان المرونة في الأنظمة الحيوية، وذلك على النحو التالي:

الأمن السيبراني كخطر استراتيجي
التوافق مع رؤية السعودية ٢٠٣٠
دور التدقيق الداخلي في بناء الثقة الرقمية

يوضح هذا الجزء كيفية استجابة إدارات التدقيق الداخلي لمتطلبات الأمن السيبراني في ظل المعايير الجديدة. ندرس التخطيط القائم على المخاطر والكفاءة السيبرانية وتوقعات حماية البيانات، مما يُمكّن فرق التدقيق من تقديم ضمانات فعّالة في عالم رقمي متزايد.

نحن في إنسايتس ندعم المؤسسات في دمج الأمن السيبراني في استراتيجية التدقيق الداخلي من خلال أطر عمل مُصممة خصيصا وبناء المهارات وحلول استشارية مبنية على أحدث المعايير العالمية والوطنية.

ثلاثة محاور رئيسية للتركيز

التركيز على المخاطر:
يجب على المدققين التعامل مع الأمن السيبراني باعتباره خطرا استراتيجيا على المؤسسة - مما يضمن دعم الحوكمة والضوابط ومناهضتها للتهديدات القادمة.

النزاهة المدعومة بالمهارة:
تتطلب عمليات التدقيق السيبراني معرفة حالية بالمخاطر وتنفيذًا غير متحيز، وخاليا من المنازعات أو الصراعات السابقة.

المرونة والثقة:
تقييم جاهزية الاختراق مع ضمان سرية البيانات والامتثال طوال المشاركات.

دور التدقيق الداخلي في الأمن السيبراني وفقا لمعايير معهد المدققين الداخليين

تُعيد معايير التدقيق الداخلي العالمية الصادرة عن معهد المدققين الداخليين لعام ٢٠٢٤ تعريف دور التدقيق الداخلي في الأمن السيبراني، مُعترفةً به كخطر استراتيجي محوري للأداء والمرونة والثقة. يجب على المدققين الداخليين الانتقال من التأكيد التفاعلي إلى التقييم الاستباقي، ودمج المخاطر السيبرانية في الحوكمة وضمان الرقابة الفعالة.

وبموجب المعايير الجديدة، يلعب التدقيق الداخلي دورا رئيسيا في دعم القيادة من خلال تقييم مدى شمولية حوكمة وممارسات الأمن السيبراني وديناميكيتها وتوافقها الاستراتيجي.

مراجعة أبعاد المخاطر في الابتكار الرقمي:
مراجعة الضوابط الخاصة بالمخاطر الناشئة في مشاريع الذكاء الاصطناعي والأتمتة وإنترنت الأشياء والسحابة.

تطوير الخبرة السيبرانية الداخلية والاستراتيجية:
تعمل المراجعة على بناء الخبرة السيبرانية أو الوصول إليها لتقييم الضوابط الحرجة بشكل فعال.

دمج الأمن السيبراني في هياكل الحوكمة:

يقوم التدقيق بتقييم كيفية دمج الأمن السيبراني في الحوكمة وإدارة المخاطر، وضمان إعطاء الأولوية للمخاطر والإبلاغ عنها إلى القيادة.

تُشجّع معايير معهد المدققين الداخليين لعام ٢٠٢٤ على اتباع مناهج تدقيق مرنة قائمة على التكنولوجيا لمعالجة مخاطر الإنترنت والذكاء الاصطناعي سريعة التطور. ويُتوقع من المدققين الداخليين استخدام أدوات مثل استخبارات التهديدات وتحليلات الأمن والاختبار الآلي لتقديم ضمانات آنية.

يجب على إدارات التدقيق الداخلي ضمان توافق تقييماتها للأمن السيبراني مع المتطلبات النظامية للمملكة العربية السعودية، بما في ذلك أطر عمل الهيئة الوطنية للأمن السيبراني والتزامات قانون حماية البيانات الشخصي. وإلى جانب الضمانات، يلعب المدققون الداخليون دورا استشاريا من خلال ترجمة قضايا المخاطر السيبرانية المعقدة إلى توصيات عملية، مما يُساعد مجالس الإدارة والمديرين التنفيذيين على اتخاذ قرارات مدروسة لحماية الأصول الحيوية.

عمليات تدقيق حوكمة الذكاء الاصطناعي: إدارة مخاطر الرقابة والتحيز والأخلاقيات

تُقرّ معايير التدقيق الداخلي العالمية لعام ٢٠٢٤ الصادرة عن معهد المدققين الداخليين بالذكاء الاصطناعي كقوة تحويلية، ومجال مخاطر معقد يتطلب إشرافا استباقيا. يُتوقع من التدقيق الداخلي الآن تقييم مدى استناد أطر حوكمة الذكاء الاصطناعي إلى أسس أخلاقية وخضوعها لرقابة جيدة وإدارتها بشفافية. ويشمل ذلك تقييم المخاطر المرتبطة بسلامة البيانات وتحيز النماذج والمساءلة في اتخاذ القرارات. مع تسارع المؤسسات في التحول الرقمي، يلعب التدقيق الداخلي دورا رئيسيا في ضمان مواءمة أنظمة الذكاء الاصطناعي مع الغرض منها وحماية ثقة أصحاب المصلحة والامتثال للتوقعات التنظيمية المتطورة.

معايير معهد المدققين الداخليين لعام ٢٠٢٤ تعزز الرقابة على حوكمة الذكاء الاصطناعي والمخاطر الأخلاقية:

تكامل أخلاقيات الذكاء الاصطناعي	ومن المتوقع أن تقوم المراجعة الداخلية بمراجعة ما إذا كانت المبادئ الأخلاقية للذكاء الاصطناعي مثل العدالة والمساءلة والشفافية مدمجة في السياسات والممارسة، وما إذا كانت توجه تصميم نموذج الذكاء الاصطناعي ونشره.
وسائل مراقبة التحز	ينبغي للمراجعين تقييم وجود وفعالية الضوابط المصممة للكشف عن التحيز الخوارزمي والتخفيف منه، والتأكد من أن القرارات لا تؤدي إلى إلحاق الضرر بشكل غير عادل بأفراد أو مجموعات معينة.
حوكمة البيانات في الذكاء الاصطناعي	يجب على التدقيق الداخلي تقييم مدخلات البيانات المستخدمة في نماذج الذكاء الاصطناعي من حيث الجودة والدقة والملاءمة والامتثال لقوانين خصوصية البيانات (مثل قانون حماية البيانات الشخصية السعودي)، حيث تؤدي البيانات الضعيفة إلى مخرجات غير موثوقة ومخاطر
هياكل المسائلة	يقع على عاتق المدققين الداخليين مسؤولية التحقق من أن المسؤوليات المتعلقة بالذكاء الاصطناعي محددة بوضوح عبر فرق الأعمال وتكنولوجيا المعلومات والامتثال، وأن ملكية مخاطر الذكاء الاصطناعي يمكن تتبعها في جميع المراحل.
قابلية التدقيق والشفافية	ينبغي أن يقوم التدقيق الداخلي بتقييم ما إذا كانت أنظمة الذكاء الاصطناعي قابلة للتفسير وما إذا كانت مخرجاتها قابلة للتتبع لضمان إمكانية تدقيق النماذج وتبرير القرارات والحفاظ على الحوكمة حتى في البيئات الآلية.

يتماشى إشراف التدقيق الداخلي على حوكمة الذكاء الاصطناعي مع نموذج الخطوط الثلاثة لمعهد المدققين الداخليين ، مما يعزز دوره كمستشار استراتيجي في مواجهة مخاطر التكنولوجيا الناشئة. في المملكة العربية السعودية، حيث تُسرّع رؤية ٢٠٣٠ من تبني الذكاء الاصطناعي والابتكار الرقمي، يُعدّ التدقيق الداخلي بالغ الأهمية لضمان عمل أنظمة الذكاء الاصطناعي ضمن الأطر الأخلاقية والرقابية والتنظيمية. تُشدد معايير معهد المدققين الداخليين لعام ٢٠٢٤ على المراقبة المستمرة والضمان الاستشرافي، مما يُمكّن المدققين من تحديد ومعالجة المخاطر المتعلقة بالذكاء الاصطناعي، مثل التحيز وسلامة البيانات والشفافية. يدعم هذا التوافق التحول الرقمي والإصلاحات التنظيمية في المملكة العربية السعودية من خلال التأكيد على قوة وفعالية ممارسات حوكمة الذكاء الاصطناعي. يعمل التدقيق الداخلي كمراجع مستقل، حيث يُصادق على ضوابط الإدارة ويوصي بالتحسينات في المجالات التي لا تزال أطر حوكمة الذكاء الاصطناعي قيد التطوير. من خلال هذا الدور، يُساعد التدقيق الداخلي المؤسسات على تحقيق التوازن بين الابتكار والمسؤولية الأخلاقية والامتثال للوائح السعودية، مثل قانون حماية البيانات الشخصية ومعايير الأمن السيبراني للهيئة الوطنية للأمن السيبراني.

إدارة المخاطر السيبرانية للجهات الخارجية (البائع)

لإدارة المخاطر السيبرانية الناتجة عن جهات خارجية بفعالية، يجب أن يتكامل التدقيق الداخلي بشكل وثيق مع إدارة مخاطر المؤسسة للحصول على رؤية شاملة للتهديدات المتعلقة بالموردين. يعزز هذا التعاون تركيز التدقيق على المخاطر الحرجة للجهات الخارجية، ويحسّن الرقابة على ضوابط أمن الموردين ويساعد المؤسسات على الاستجابة السريعة لثغرات سلسلة التوريد. تدعم إنسايتس العملاء في تطوير برامج تدقيق فعّالة للمخاطر السيبرانية للجهات الخارجية، مما يضمن الامتثال للمعايير التنظيمية ويعزز حوكمة الموردين. فيما يلي أهم مجالات التركيز لإدارة المخاطر السيبرانية للجهات الخارجية:

المخاطر السيبرانية الناشئة الرئيسية التي تتطلب اهتمام التدقيق		
فئة المخاطر	الوصف	التركيز على التدقيق الداخلي
إدارة دخول الموردين	المخاطر المتعلقة بكيفية وصول الأطراف الأخرى إلى الأنظمة والبيانات.	• مراجعة ضوابط الوصول • إدارة الامتيازات • التحقق من المصادقة
حماية وسرية البيانات	مخاطر خرق البيانات أو عدم الامتثال لقوانين خصوصية البيانات.	• فحوصات الامتثال للخصوصية • تدقيقات معالجة البيانات • ضمانات السرية
الاستجابة للحوادث والتعافي منها	المخاطر المرتبطة باستعداد الموردين للحوادث الإلكترونية.	• تقييم التأهب للأزمات • اختبار الاستجابة للحوادث • تدقيق الاتصالات
بنود الأمن التعاقدي	المخاطر الناجمة عن عدم كفاية متطلبات الأمن في عقود الموردين.	• تدقيق شروط العقد • الامتثال لاتفاقيات مستوى الخدمة • مراقبة التنفيذ
الرقابة الدائمة	المخاطر الناجمة عن عدم وجود مراقبة مستمرة لوضع أمن الموردين.	• مراجعات تقييم المخاطر • جداول تدقيق الأمن • تتبع الأداء
نقاط ضعف سلسلة التوريد	المخاطر الناجمة عن النظم البيئية المترابطة مع أطراف ثالثة.	• رسم خرائط مخاطر سلسلة التوريد • تحليل الترابط • مراجعة ضوابط التخفيف
الامتثال النظامي	مخاطر عدم امتثال الموردين لقوانين الأمن السيبراني المحلية.	• مراجعة الالتزام باللوائح التنظيمية • تقارير الامتثال • فحوصات توافق السياسات
مخاطر التكنولوجيا والأدوات	المخاطر المرتبطة بالبرمجيات أو الأجهزة التي يوفرها الموردون.	• تدقيقات التحقق من التكنولوجيا • اختبارات الأمان • التحقق من إدارة الدفعات

قائمة مراجعة الأمن السيبراني بناءً على معايير الهيئة الوطنية للأمن السيبراني المملكة العربية السعودية

تُحفّز رؤية السعودية ٢٠٣٠ تحوّلا رقميا كبيرا، مما يُشكّل بيئةً مُعقّدةً لمخاطر الأمن السيبراني. ومع تبنّي المؤسسات للتقنيات المُتقدّمة ومواجهة متطلبات تنظيمية أكثر صرامة من الهيئة الوطنية للأمن السيبراني، يجب أن تتطوّر وظائف التدقيق الداخلي لتوفير رقابة مُحدّدة. يُعدّ فهم إطار عمل الهيئة الوطنية للأمن السيبراني ومتطلبات الامتثال المحلية أمراً بالغ الأهمية لتقديم ضمان أمن سيبراني فعّال وقائم على المخاطر، بما يتماشى مع الأهداف الاستراتيجية للمملكة.

الامتثال لمعايير الأمن السيبراني الصادرة عن الهيئة الوطنية للاتصالات

مع تطور البنية التحتية الرقمية في المملكة العربية السعودية، يُعدّ الامتثال لمعايير الأمن السيبراني الصادرة عن الهيئة الوطنية للاتصالات أمرا بالغ الأهمية لحماية المصالح الوطنية والأصول الحيوية. ويلعب التدقيق الداخلي دورا محوريا في التحقق من الالتزام بهذه المتطلبات، مما يضمن التزام المؤسسات بضوابط أمنية صارمة. ولا يقتصر هذا الامتثال على حماية المعلومات الحساسة فحسب، بل يعزز أيضا ثقة أصحاب المصلحة في وضع المؤسسة فيما يتعلق بالأمن السيبراني وتوافقها مع اللوائح التنظيمية.

تقييم الرقابة القائمة على المخاطر

في مواجهة التهديدات السيبرانية المتطورة، يجب على التدقيق الداخلي إعطاء الأولوية للضوابط القائمة على تقييمات مخاطر ديناميكية تعكس طبيعة التهديدات الفريدة للمؤسسة. من خلال التركيز على أهم نقاط الضعف والتدابير الأمنية، يُسهم المدققون في تحسين تخصيص الموارد وجهود التخفيف من المخاطر. يُعزز هذا النهج المُستهدف المرونة ويُوائم ممارسات الأمن السيبراني مع الأهداف الاستراتيجية لإدارة المخاطر في المملكة العربية السعودية.

الاستجابة للحوادث والإبلاغ عنها

يُعد الكشف عن حوادث الأمن السيبراني وإدارتها في الوقت المناسب أمرا بالغ الأهمية للحد من آثارها ودعم الشفافية التنظيمية. ويضمن التدقيق الداخلي متانة أطر الاستجابة للحوادث، واختبارها، وامتثالها لمتطلبات الإبلاغ الصادرة عن الهيئة الوطنية للأمن السيبراني، ويعزز الإشراف الفعال على هذه العمليات مرونة المؤسسة، ويضمن لأصحاب المصلحة إدارة المخاطر بشكل استباقي ومسؤول.

الإشراف على الأمن السيبراني للجهات الخارجية

مع تزايد اعتماد المؤسسات على الموردين والشركاء، أصبحت إدارة مخاطر الجهات الخارجية السيبرانية أولوية استراتيجية. يُقيّم التدقيق الداخلي مدى كفاءة تحديد هذه المخاطر والتحكم فيها ومراقبتها طوال دورة حياة المورد. يحمي هذا الإشراف النظام البيئي الرقمي الموسّع للمؤسسة، ويعزز أمن سلسلة التوريد، ويحافظ على التوقعات التنظيمية.

المراقبة والتوعية المستمرة

يُمثل الأمن السيبراني تحديا متواترا، ويتطلب يقظةً مستمرة. ويُعد دور التدقيق الداخلي في التحقق من صحة برامج المراقبة والتدريب على الأمن السيبراني أمرا بالغ الأهمية للحفاظ على وضع أمني استباقي. ومن خلال تعزيز الوعي المستمر والكشف الفوري عن المخاطر، يُسهم التدقيق في ضمان قدرة المؤسسات على الصمود في مواجهة التهديدات الناشئة، ومواءمتها مع أهداف الأمن السيبراني الوطنية.

إن فهم مخاطر الأمن السيبراني ومتطلبات الامتثال أمر ضروري – ولكن القيمة الحقيقية تكمن في العمل الفعال. تساعد المنظمات السعودية على مواءمة ممارساتها التدقيقية مع معايير الأمن السيبراني الوطنية للسلطة المالية، وضمان الامتثال التنظيمي، وتوفير ضمان قوي على حماية البنية التحتية الرقمية الحيوية.

أمثلة واقعية على التدقيق: المخاطر السيبرانية والاستجابة لها في شركات المملكة العربية السعودية

مع التطور السريع للتهديدات السيبرانية، تواجه المؤسسات في المملكة العربية السعودية تحديات متزايدة في حماية أصولها الرقمية. ويلعب التدقيق الداخلي دورا حيويا في تحديد هذه المخاطر وتقييمها والتخفيف من حدتها، مع ضمان الامتثال للوائح الوطنية للأمن السيبراني. ومن خلال دراسة نتائج التدقيق الواقعية وردود أفعاله، يمكن للشركات تعزيز وضع الأمن السيبراني لديها وتعزيز قدرتها على مواجهة التهديدات الناشئة. فيما يلي أهم المخاطر السيبرانية التي تواجهها الشركات في المملكة العربية السعودية، بالإضافة إلى إجراءات التدقيق الداخلي النموذجية المتخذة لمعالجتها:

01 التصيد الاحتيالي واختراق البريد الإلكتروني

أوصت لجنة التدقيق الداخلي باستخدام المصادقة متعددة العوامل وتدريب مُحاكي على التصيد الاحتيالي. واستجابةً لذلك، اعتمدت المؤسسة نهجا قائما على مبدأ الثقة الصفرية للتحقق من البريد الإلكتروني، وطرحت جلسات توعية إلزامية، مما أدى إلى انخفاض كبير في معدلات النقر على رسائل البريد الإلكتروني الضارة.

02 أخطاء تكوين أمان السحابة

كشف التدقيق عن أن سياسات حوكمة السحابة قديمة. قامت الشركة بمراجعة حقوق الوصول وتطبيق عمليات فحص تكوين آلية ومواءمة بنية السحابة مع ضوابط الأمن السيبراني السحابي التابعة للهيئة الوطنية للأمن السيبراني منع تسرب البيانات والانتهاكات التنظيمية.

03 انتهاكات الموردين الخارجيين

بعد التدقيق، وضعت المؤسسة إطارا لإدارة المخاطر من جهات خارجية. شمل ذلك عمليات تدقيق دورية للموردين الأساسيين وتقييم مخاطر التكامل واتفاقيات مستوى الخدمة السيبرانية. مكّنت هذه الخطوة من الكشف عن التهديدات بشكل أسرع وضمنت مساءلة الموردين بما يتماشى مع التزامات قانون حماية البيانات الشخصية.

04 تكنولوجيا المعلومات الظلية والتطبيقات غير المصرح بها

حفّز التدقيق الداخلي على تطوير جرد شامل للتطبيقات على مستوى المؤسسة وتطبيق أدوات مراقبة نقاط النهاية. وضمنت الاستجابة استخدام التطبيقات التي خضعت للتدقيق فقط، مما قلل من احتمالية وقوع هجمات، وعزز الامتثال للسياسات.

05 خطط الاستجابة للحوادث القديمة

سلط فريق التدقيق الضوء على ثغرات في اختبارات الاستجابة للأزمات والتوثيق. قامت الإدارة بتحديث خطة الاستجابة للحوادث لتتوافق مع معايير الهيئة الوطنية للأمن السيبراني ، وأجرت تمارين نظرية وأسندت المسؤولية إلى فرق محددة، مما أدى إلى تحسين السرعة والوضوح في حالات الاختراق.

06 التهديدات الداخلية وإساءة استخدام الوصول المتميز

كشف التدقيق أن العديد من المستخدمين يتمتعون بصلاحيات إدارية غير ضرورية، مما يزيد من خطر إساءة الاستخدام المتعمدة أو غير المقصودة. استجابت الشركة بتطبيق التحكم في الوصول القائم على الأدوار، وتسجيل جميع الأنشطة ذات الصلاحيات، ودمج أدوات تحليل سلوك المستخدم للكشف عن أي خلل. أدت هذه الإجراءات إلى تقليل تعرض المستخدمين لمخاطر المعلومات الداخلية بشكل كبير، مع تعزيز المساءلة.

عمليات تدقيق أمان السحابة: معالجة المخاطر في البنية التحتية عن بُعد

مع تسارع تبني المؤسسات السعودية للسحابة، يلعب التدقيق الداخلي دورا حاسما في ضمان أمن البنية التحتية عن بُعد، وامتثالها للمعايير، ومرونتها. يساعد تدقيق بيئات السحابة وفقا للمعايير الوطنية، مثل ضوابط الأمن السيبراني السحابي التابعة للهيئة الوطنية للاتصالات، على تحديد أخطاء التكوين وتقييم مخاطر الجهات الخارجية والتحقق من المراقبة المستمرة.

فيما يلي أهم مجالات التركيز للتدقيق الداخلي عند تقييم أمن السحابة في بيئات البنية التحتية عن بُعد.

01

تحليل إطار عمل إدارة مخاطر السحابة الخاص بالمنظمة للتأكد من أنه يحدد بشكل شامل ويعطي الأولوية للمخاطر المرتبطة بالبنية التحتية عن بعد ومناظر التهديدات المتطورة.

02

تقييم فعالية تصميم وتشغيل عناصر التحكم في أمان السحابة، بما في ذلك إدارة الهوية والوصول وتشفير البيانات وتقسيم الشبكة وبروتوكولات الاستجابة للحوادث.

03

مراجعة تنفيذ آليات المراقبة المستمرة واكتشاف التهديدات، مثل التنبيهات الآلية ومسح الثغرات الأمنية، للتحقق من التعرف في الوقت المناسب على الحوادث الأمنية.

04

تقييم مدى صرامة عمليات إدارة المخاطر الخاصة بالموردين الخارجيين للتأكد من امتثال مزودي الخدمات السحابية لمتطلبات الأمن التعاقدية واللوائح الوطنية ذات الصلة.

05

فحص هياكل الحوكمة لضمان المساءلة الواضحة وإنفاذ السياسات والتدريب المنتظم على التوعية بأمن السحابة، وهي مضمنة في جميع أنحاء المؤسسة.

06

فحص عملية إدارة التكوين للتأكد من توفير موارد السحابة بشكل آمن، وصيانتها وفقا لأفضل الممارسات، ومراجعتها بانتظام بحثا عن التكوينات الخاطئة التي قد تكشف عن نقاط الضعف.

07

التحقق من صحة خطط التعافي من الكوارث واستمرارية الأعمال المتعلقة بالبنية التحتية السحابية لضمان توفر البيانات ومرونة النظام في حالة انقطاع الخدمة أو الحوادث الإلكترونية.

التخطيط الاستراتيجي للتدقيق بخصوص التهديدات السيبرانية والذكاء الاصطناعي الناشئة

للامتثال لمعايير معهد المدققين الداخليين لعام ٢٠٢٤، والتصدي بفعالية للتهديدات السيبرانية والذكاء الاصطناعي الناشئة، يجب على إدارات التدقيق الداخلي تطبيق نهج تخطيط تدقيق مرن وقائم على المخاطر. يُمكّن هذا من ضمان الجودة في الوقت المناسب، والتوافق الاستراتيجي، وتعزيز الاستجابة للمخاطر المتغيرة.

في إنسايتس، نصمم وننفذ نماذج تخطيط تدقيق استراتيجي مصممة خصيصا لملف المخاطر الخاص بكم وأهداف مؤسستكم.

١. يجب أن يكون التخطيط متماشياً مع المخاطر وديناميكياً

ينبغي أن تركز خطة التدقيق على المخاطر السيبرانية والذكاء الاصطناعي الناشئة، وليس على الجداول الزمنية القديمة. وهذا يتطلب:

- مواءمة عمليات التدقيق مع تقييمات المخاطر السيبرانية والذكاء الاصطناعي الحالية واستراتيجية المؤسسة.
- تحديث تقييمات المخاطر بانتظام (مثلاً، ربع سنوي أو بعد الحوادث الكبرى).
- إعطاء الأولوية لعمليات التدقيق على المجالات ذات التأثير المحتمل الأكبر.

٢. يجب أن يكون التخطيط متماشياً مع المخاطر وديناميكياً

يتطلب التخطيط الفعال للتدقيق التعاون مع فرق الأمن السيبراني وحوكمة الذكاء الاصطناعي وإدارة المخاطر. ويشمل ذلك:

- مواءمة عمليات التدقيق مع تقييمات المخاطر السيبرانية والذكاء الاصطناعي الحالية واستراتيجية المؤسسة.
- تحديث تقييمات المخاطر بانتظام (مثلاً، ربع سنوي أو بعد الحوادث الكبرى)
- إعطاء الأولوية لعمليات التدقيق على المجالات ذات التأثير المحتمل الأكبر.

٣. المرونة والتدقيق المُعتمد على التكنولوجيا

يجب أن تتسم خطط التدقيق بالمرونة والاستفادة من التقنيات المتقدمة. ويشمل ذلك:

- استخدام أدوات الذكاء الاصطناعي وتحليل البيانات لتعزيز فعالية التدقيق
- دمج تحليل السيناريوهات والمحاكاة لاختبار المرونة
- مراعاة اعتبارات الحوكمة والأخلاقيات والتحيز المتعلقة بالذكاء الاصطناعي

كيف لإنسايتس مساعدتك

نحن في شركة إنسايتس للإدارة المالية والاستشارات، نتجاوز التوجيه إلى قيادة التحول. تُمكّن خدماتنا الاستشارية إدارات التدقيق الداخلي من التحول من التركيز على الرقابة إلى التركيز على الاستراتيجية، بما يتماشى بسلاسة مع معايير معهد المدققين الداخليين لعام ٢٠٢٤، ويدعم الأهداف الاستراتيجية لرؤية المملكة العربية السعودية ٢٠٣٠.

طريق التحول

01 مراجعات نضج إدارة مخاطر المؤسسة

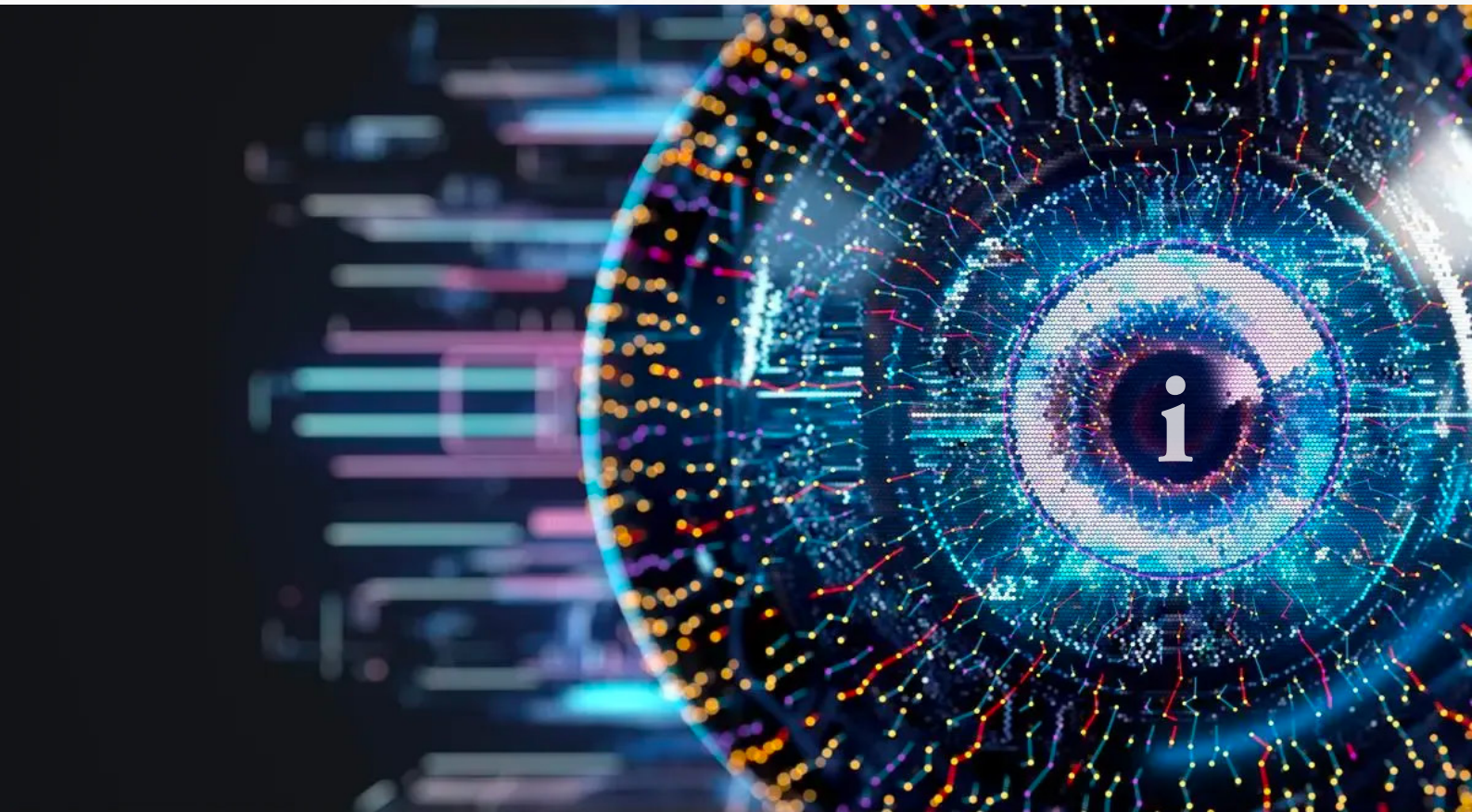
02 تقييمات جاهزية التدقيق الداخلي (بما يتماشى مع معايير التدقيق الداخلي لعام ٢٠٢٤)

03 ورش عمل مجلس الإدارة ولجنة التدقيق حول الرقابة على الحوكمة

04 نماذج وأدوات تخطيط التدقيق الرشيقة

05 عمليات تدقيق الامتثال التنظيمي (البنك المركزي السعودي، هيئة السوق المالية، هيئة الحكومة

06 أطر تدقيق مخاطر الحوكمة البيئية والاجتماعية والمؤسسية والأمن السيبراني والذكاء الاصطناعي



تواصل معنا

لمزيد من المعلومات والتوضيح والمناقشة بشأن المحتويات، يرجى الاتصال

خواجه سوها بت
شريك - الإستشارات المالية
sbutt@insightss.co :

احتشام مالك
نائب الرئيس الأول – الاستشارات المالية والمخاطر
emalik@insightss.co :

نيك ويتفورد
نائب الرئيس اول– لنمو اعمال
nwhitford@insightss.co :

مكتب الرياض:
107 برج الأسطورة, طريق الملك فهد, الرياض,المملكة العربية السعودية

مكتب جدة:
رويال بلازا، شارع الأمير سلطان، جدة 23615 – المملكة العربية السعودية

مكتب دبي:
مكتب 711، مبنى آيريس باي، الخليج التجاري، دبي – الإمارات العربية المتحدة

مكتب المملكة المتحدة:
الطابق 37، ميدان كندا الأول، لندن E14 5AA

مكتب استراليا:
صندوق بريد 6387 ,شارع هاليفاكس ، أديلايد جنوب أستراليا 5000

مكتب نيويورك:
شارع وول, الطابق العشرين, نيويورك ,14 10005, الولايات المتحدة الأمريكية

Insights
: +966 53 963 3882
: + 966 11 2930 665
: info@insightss.co
: www.insightss.co/ar

insights

التعامل مع التعقيد وتبسيط النجاح