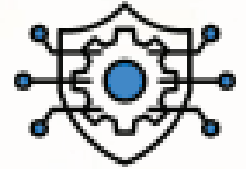


أصبح ضمان الطرف الثالث
إلزاميا الآن

ماذا يعني إطار الأمن السيبراني لعام 2026 الصادر عن البنك المركزي السعودية بالنسبة للبنوك السعودية

شركة إنسايتس للاستشارات المالية
والإدارية ، استشارات قانونية ومخاطر
الأمن السيبراني



الاستشارات التنظيمية ومخاطر
الأمن السيبراني

أصبح ضمان الطرف الثالث إلزاميا الآن

ماذا يعني إطار الأمن السيبراني لعام ٢٠٢٦ الصادر عن البنك المركزي السعودية بالنسبة للبنوك السعودية

تعمل البنوك والشركات المالية السعودية الآن على شبكة واسعة من الشركاء الخارجيين. يلعب مزودو السحابة، ومعالجو الدفع، وبائعو التكنولوجيا، وشركات الخدمات الخارجية دورا في العمليات اليومية. هذا الاعتماد ينمو بسرعة: سوق الأمن السيبراني في المملكة نفسه على الطريق الصحيح للنمو من حوالي ٤.٥٥ مليار دولار في ٢٠٢٥ إلى ٤.٩٨ مليار دولار في ٢٠٢٦، وجزء كبير من هذا الإنفاق يذهب لتأمين هذه العلاقات الخارجية تحديدا



تساعد هذه الشراكات المؤسسات على التحرك بشكل أسرع وخدمة العملاء بشكل أفضل. لكنها تفتح أيضا الباب لمخاطر إلكترونية وتشغيلية وتنظيمية جديدة، وتظهر الأرقام أن المخاطر تزداد بسرعة. على الصعيد العالمي، ارتفعت نسبة خروقات البيانات التي تشمل طرفا ثالثا من ١٥٪ قبل عامين إلى ٤٨٪ اليوم، بزيادة ٦٠٪ خلال العام الماضي فقط. لسنوات، أدارت معظم المؤسسات هذا الخطر من خلال استبيانات الموردين، وبنود العقود، والمراجعات الدورية. هذا النهج لا يزال ذا قيمة، لكنه بمفرده لم يعد يفي بمعايير اليوم. كما أن هذه الفجوة مكلفة أن تترك مفتوحة؛ فالخرق الذي يعود إلى مورد أو شريك في سلسلة التوريد يكلف الآن في المتوسط ٤.٩١ مليون دولار أمريكي ويستغرق ٢٦٧ يوما للكشف والاحتواء، وهو أطول من أي نوع اختراق آخر تم تتبعه



مع تزايد ترابط النظم البيئية المالية، يريد المنظّمون دليلا، وليس أوراقا، على أن الموردين الأساسيين يظلون آمنين. تجعل دورة تدقيق إطار عمل الأمن السيبراني الصادر عن البنك المركزي لعام ٢٠٢٦ هذا التحول رسميا. يجب على المؤسسات المنظمة الآن بناء برامج ضمان منظمة من طرف ثالث تنتج أدلة مستقلة على الأمن السيبراني للبائعين. هذا هو التغيير الذي يتوقعه البنك المركزي، ويضع الرقابة المستمرة على الموردين في صميم حوكمة البنوك



نظرة سريعة

أصبح ضمان الطرف الثالث إلزاميا من الدورة الإشرافية لإطار الأمن السيبراني الصادر عن البنك المركزي لعام ٢٠٢٦، وليس إضافة اختيارية	
يتوقع البنك المركزي من المؤسسات أن تصل على الأقل إلى مستوى النضج الثالث ("المعرف") عبر جميع مجالات الأمن السيبراني، بما في ذلك حوكمة الأطراف الثالثة	
يجب على البنوك تقديم أدلة مستقلة على أن الموردين الأساسيين يحافظون على ضوابط الأمن السيبراني المناسبة؛ لا يمكن للاستبيانات التي يتم الإبلاغ عنها ذاتيا أن تحمل هذا العبء بمفردها	
مواقيت تقارير مجالس الإدارات حول مخاطر الأمن السيبراني، بما في ذلك مخاطر الأطراف الثالثة، تنتقل من سنوية إلى نصف سنوية للمؤسسات من المستوى الأول	

Source: SAMA Cyber Security Framework, 2026 audit cycle guidance; SAMA Rulebook.

لماذا لم تعد استبيانات الموردين كافية؟

لا تزال العديد من المؤسسات تدير مخاطر الأطراف الثالثة بشكل رئيسي من خلال الاستبيانات السنوية، وإعلانات الامتثال، والبنود الأمنية القياسية في العقود. تظل هذه الأدوات مفيدة، لكنها تؤكد فقط أن المعلومات قد جمعت. لا يذكرون الكثير عما إذا كانت ضوابط البائع تعمل فعليا يوميا مع تزايد تعقيد ترتيبات الاستعانة بمصادر خارجية، تحتاج البنوك إلى معرفة أكثر مما إذا كان لدى البائع سياسة أمنية مكتوبة. يحتاجون إلى معرفة ما إذا كانت هذه السياسة تطبق وتراقب باستمرار وتخضع للتحقق من قبل طرف مستقل. باختصار، التركيز التنظيمي ينتقل من الامتثال للبائعين إلى ضمان الموردين

كيف تحرك المؤشر

توقعات إطار الأمن السيبراني للبنك المركزي	المنطقة	قبل عام ٢٠٢٦
تقارير الضمان المستقلة والاختبارات الخارجية	الدليل الرئيسي	استبيانات الموردين والتصريحات الذاتية
المراقبة المستمرة عبر دورة حياة البائع	دورة المراجعة	سنوي، وغالبا ما يكون تمرينا لمرة واحدة
من المتوقع تقديم تقارير نصف سنوية للمؤسسات من المستوى الأول	تقارير مجالس الإدارات	التحديثات السنوية في معظم الحالات
مدمجة في إدارة المخاطر المؤسسية وإشراف مجلس الإدارة	ملكية المخاطر	تدار بشكل رئيسي فرق المشتريات
المتطلبات الإلزامية بموجب دورة تدقيق إطار الأمن السيبراني	الوضع التنظيمي	ممارسة جيدة موصى بها

الجدول ١: كيف تغيرت توقعات البنك المركزي من الأطراف الثالثة مع اقتراب دورة التدقيق لعام ٢٠٢٦

Source: SAMA Cyber Security Framework, 2026 audit cycle guidance; SAMA CSF 2026 compliance analysis, InfoSec4TC, June 2026.

أربع أولويات للمديرين التنفيذيين

يمكن لمجالس الإدارات الاستجابة لهذا التحول بأربع خطوات عملية

١. تحديد الموردين الأكثر أهمية

ليس كل مورد يحمل نفس مستوى المخاطر. يجب على المؤسسات تصنيف الموردين بناءً على أهمية الخدمة، وحساسية البيانات التي يلمسونها، والتأثير إذا تعطلت تلك الخدمة

٢. تجاوز الاستبيان

يجب ألا تكون التقييمات الذاتية بعد الآن في صميم برنامج الضمان الخاص بالبنك. يجب على المؤسسات ربط الاستبيانات بتقارير ضمان مستقلة، واختبارات خارجية، وشهادات، ومراقبة مستمرة لبناء صورة أكثر شمولاً وموضوعية لأمان الموردين

٣. دمج مخاطر الطرف الثالث في إدارة مخاطر المؤسسات

يجب ألا تظل مخاطر البائعين منفصلة كمهمة شراء. ينتمي هذا المجال إلى إدارة مخاطر المؤسسات، حوكمة الأمن السيبراني، تخطيط استمرارية الأعمال، وتقارير مجلس الإدارة، لذا ترى القيادة صورة واحدة مترابطة لمخاطر المنظمة

٤. الاستمرار في المتابعة بعد توقيع العقد

الضمان ليس فحصاً لمرة واحدة. يجب على المؤسسات إعادة تقييم الموردين الحيويين بشكل منتظم، وتتبع التغيرات في ملف المخاطر لديهم، ومراجعة التقارير المستقلة عند إصدارها، والتأكد من إصلاح أي نقاط ضعف

وجهة نظر الرؤى

لا تزال العديد من فرق المخاطر تطرح سؤالاً صيقاً

”هل أكمل موردونا استبيان الأمن؟“



سؤال أكثر فائدة لغرفة الاجتماعات هو

”هل يمكننا إثبات، بأدلة مستقلة، أن موردنا الأساسيين لا يزالون صامدين اليوم؟“



الفرق مهم. الامتثال يظهر أن المعلومات تم جمعها. الضمان يظهر أن المخاطر مفهومة ومتتبعة ومدارة بنشاط

الأرقام وراء التحول

الدفع نحو الضمان المستقل لا يحدث بمعزل عن غيره. وهذا يندرج ضمن اتجاه أوسع: الشركاء الخارجيون هم الآن المصدر الأسرع نمواً للمخاطر السيبرانية، والسعودية تستثمر وفقاً لذلك لمواجهة ذلك

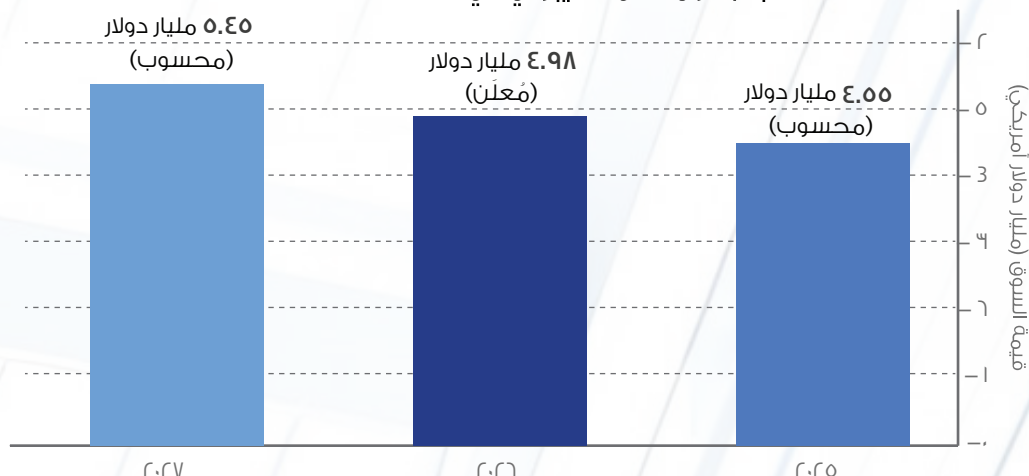
نقطة البيانات	الشكل	المصدر
القيمة السوقية السعودية للأمن السيبراني ٢٠٢٥	٤.٥٥ مليار دولار أمريكي	ماركتس آند ماركتس، فبراير ٢٠٢٦
القيمة السوقية للأمن السيبراني في السعودية ٢٠٢٦	٤.٩٨ مليار دولار أمريكي	ماركتس آند ماركتس، فبراير ٢٠٢٦
القيمة السوقية للأمن السيبراني في السعودية ٢٠٢٧ (التوقعات)	٥.٤٥ مليار دولار أمريكي	ماركتس آند ماركتس، فبراير ٢٠٢٦

نقطة البيانات	الشكل	المصدر
معدل نمو سنوي مركب في السوق ٢٠٢٦-٢٠٣١ (يصل إلى ٧.٨١ مليار دولار امريكي بحلول ٢٠٣١)	٩.٤%	ماركتس آند ماركتس، فبراير ٢٠٢٦
انتهاكات تتعلق بطرف ثالث ٢٠٢٤ تقرير التحقيق في اختراق البيانات	١٥%	تقرير تحقيقات خرق بيانات فيريزون، طبعة ٢٠٢٤
انتهاكات تتعلق بطرف ثالث ٢٠٢٥ تقرير التحقيق في اختراق البيانات	٣٠%	تقرير تحقيقات خرق بيانات فيريزون، طبعة ٢٠٢٥
انتهاكات تتعلق بطرف ثالث ٢٠٢٦ تقرير التحقيق في اختراق البيانات (الحالي)	٤٨%	تقرير تحقيقات خرق بيانات فيريزون، طبعة ٢٠٢٦
الزيادة السنوية في تورط اختراق الأطراف الثالثة (تقرير التحقيق في اختراق البيانات ٢٠٢٦)	٦٠%	تقرير تحقيقات خرق بيانات فيريزون، طبعة ٢٠٢٦
متوسط تكلفة اختراق سلسلة التوريد/طرف ثالث	٤.٩١ مليار دولار أمريكي	تقرير تكلفة اختراق أمن البيانات ٢٠٢٥
الوقت المتوسط لتحديد واحتواء مثل هذا الخرق	٢٦٧ يوم	تقرير تكلفة اختراق أمن البيانات ٢٠٢٥

الجدول ٢: أرقام السوق والاختراقات المؤكدة ذات الصلة بمخاطر الأمن السيبراني من الأطراف الثالثة في السعودية وعلى الصعيد العالمي ٢٠٢٥-٢٠٢٧ يتم حساب قيم السوق لعامي ٢٠٢٥ و ٢٠٢٧ بناء على معدل نمو سنوي مركب معلن من المصدر البالغ ٩.٤%؛ جميع الأرقام الأخرى* يتم الإبلاغ عنها مباشرة

Source: MarketsandMarkets (Feb 2026); Verizon Data Breach Investigations Report, 2024-2026 editions; IBM Cost of a Data Breach Report, 2025.

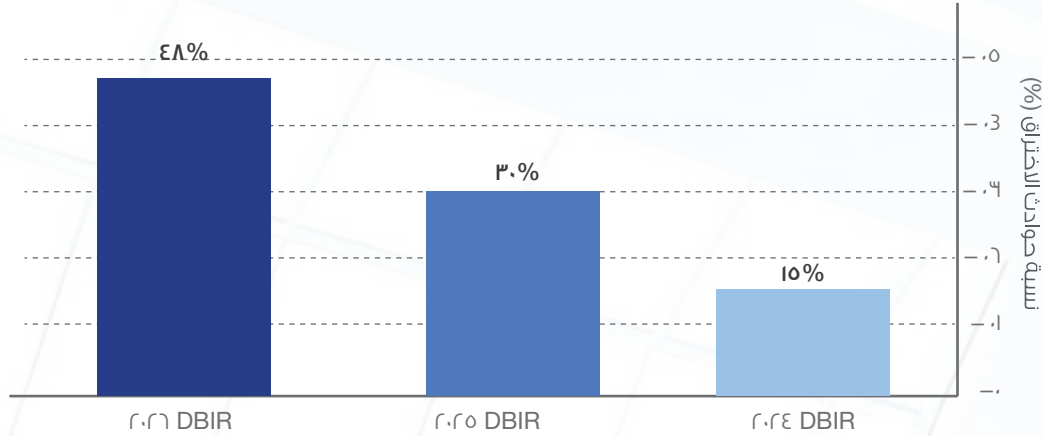
حجم سوق الأمن السيبراني في المملكة ٢٠٢٥-٢٠٢٧



الرسم البياني أ: من المتوقع أن ينمو سوق الأمن السيبراني في السعودية من حوالي ٤.٥٥ مليار دولار في عام ٢٠٢٥ إلى ٥.٤٥ مليار دولار بحلول عام ٢٠٢٧. على أساس مبلغ ٤.٩٨ مليار دولار في عام ٢٠٢٦.

Source: MarketsandMarkets, Kingdom of Saudi Arabia Cybersecurity Market Report, February 2026

نسبة حالات اختراق البيانات التي تشمل طرفاً ثالثاً



الرسم البياني ٢: ارتفع تورط الأطراف الثالثة في اختراقات البيانات العالمية من ١٥% إلى ٤٨% خلال ثلاث إصدارات متتالية من تقرير تكلفة اختراق أمن البيانات

Source: Verizon Data Breach Investigations Report, 2024, 2025, and 2026 editions

تشير هذه الأرقام إلى اتجاه واحد. مع إنفاق المؤسسات السعودية أكثر على الأمن السيبراني واعتمادها بشكل أكبر على الموردين الخارجيين، تستمر نسبة الحوادث التي تعود إلى طرف ثالث في الارتفاع. برنامج ضمان منظم ومثبت بشكل مستقل أصبح بسرعة الفرق بين اكتشاف بائع ضعيف مبكراً ومعرفة الموضوع بعد حدوث اختراق

كيف تساعد إنسايتس المؤسسات

نحن في إنسايتس للاستشارات المالية والإدارية، نساعد المؤسسات على تعزيز الحوكمة الخارجية من خلال

- تقييمات المخاطر من طرف ثالث
- مراجعات ضمان البائعين
- تصميم إطار عمل المخاطر من طرف ثالث
- تقييمات نضج المؤسسة من خلال إطار الأمن السيبراني للبنك المركزي
- مراجعات حوكمة الأمن السيبراني
- تقييمات المرونة التشغيلية
- تكامل إدارة المخاطر المؤسسية

يساعد نهجنا المؤسسات المالية على بناء برامج ضمان عملية قائمة على المخاطر تتماشى مع توقعات البنك المركزي المتطورة مع تعزيز القدرة على الصمود عبر منظومة الموردين

الخلاصة الأساسية

ومع اعتماد المؤسسات المالية السعودية بشكل أكبر على مزودي الخدمات الخارجيين، أصبحت مخاطر الأطراف الثالثة واحدة من أكبر المحركات للمرونة التشغيلية. المؤسسات التي تبني الآن قدرة الضمان المهيكلة ستكون في وضع أفضل لتلبية التوقعات التنظيمية، وتعزيز الحوكمة، والحفاظ على ثقة الجهات التنظيمية والعملاء على حد سواء

لم يعد بإمكان علاقات البائعين الاعتماد على العقود فقط. هم بحاجة إلى ضمان مستقل خلفهم

المصادر

Source: SAMA Cyber Security Framework and 2026 audit cycle guidance, SAMA Rulebook.

SAMA CSF 2026 compliance analysis, InfoSec4TC, June 2026.

Verizon Data Breach Investigations Report, 2024, 2025, and 2026 editions.

IBM Cost of a Data Breach Report, 2025.

MarketsandMarkets, Kingdom of Saudi Arabia Cybersecurity Market Report, February 2026.

تواصل معنا

لمزيد من المعلومات والتوضيح والمناقشة بشأن المحتويات، يرجى الاتصال

أمير عباس

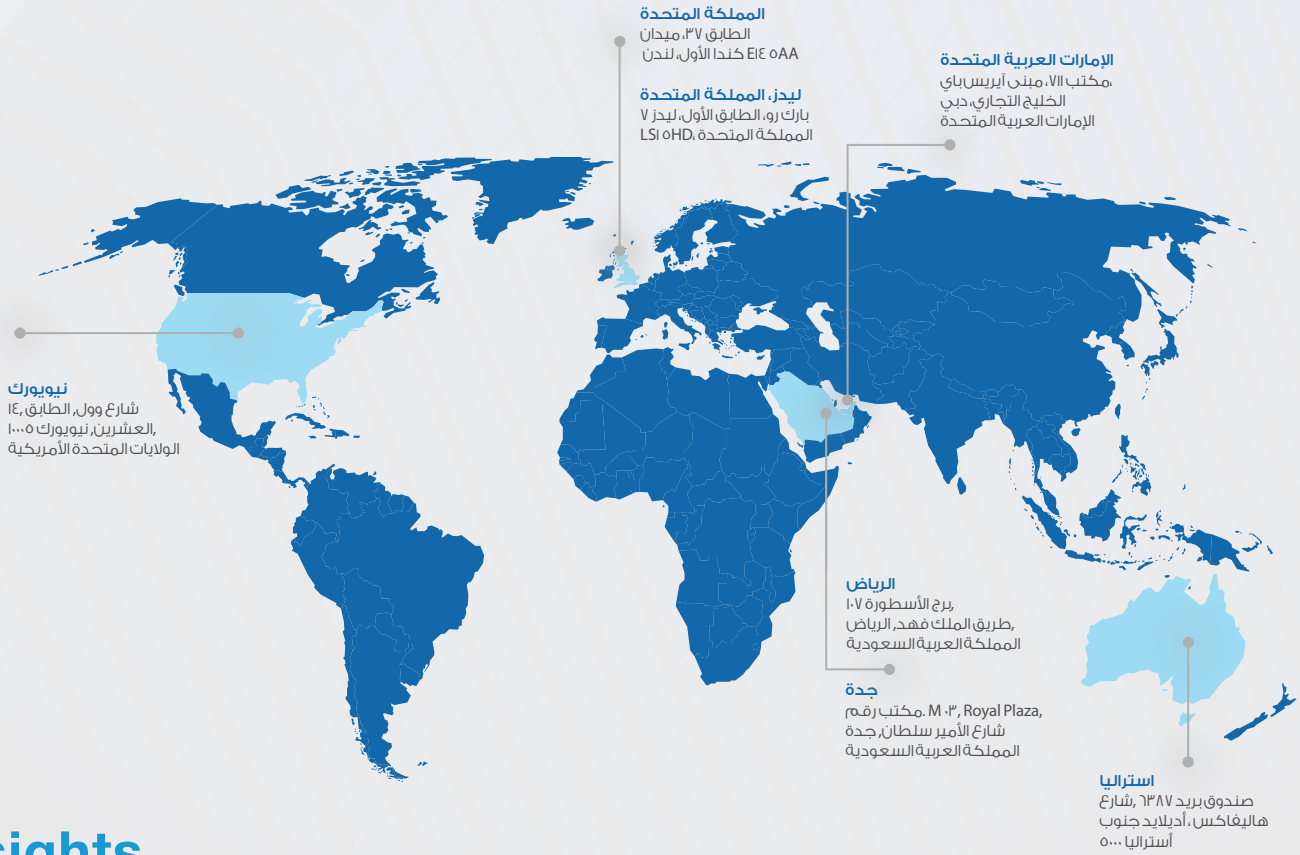
نائب الرئيس – الاستشارات المالية
aabbas@insightss.co ✉

نيك ويتفورد

نائب الرئيس أول – لنمو اعمال
nwhitford@insightss.co ✉

خواجه سوها بت

شريك – الإستشارات المالية
sbutt@insightss.co ✉



Insights

☎ : +966 53 775 0075

✉ : info@insightss.co

🌐 : www.insightss.co/ar