

أثر حوكمة مخاطر الطرف الثالث في تعزيز المرونة التشغيلية لدى شركات التأمين في المملكة العربية السعودية: الدور الوسيط لجاهزية الأمن السيبراني

The Impact of Third-Party Risk Governance on Operational Resilience in Saudi Insurance Companies: The Mediating Role of Cybersecurity Readiness

اسم الباحث:

رقم الأوركيذ:

التخصص - الكلية - جامعة ميدأوشن - الدولة

البريد الإلكتروني:

الملخص:

الأهداف: قياس أثر حوكمة مخاطر الطرف الثالث في المرونة التشغيلية، واختبار الدور الوسيط لجاهزية الأمن السيبراني لدى شركات التأمين السعودية. مكان الدراسة: قطاع التأمين وإعادة التأمين والخدمات التأمينية في المملكة العربية السعودية. المنهجية: اعتمدت الدراسة منهجاً وصفيًا تحليليًا بتصميم كمي مقطعي، واستبانة من ٣٠ عبارة موزعة على حوكمة الطرف الثالث، والجاهزية السيبرانية، والمرونة التشغيلية. ولأن الملف الأصلي لا يتضمن استجابات ميدانية، استخدمت ٢١٤ مشاهدة محاكاة معلنة لاختبار النموذج إيضاحيًا، وحُللت بالمتوسطات والارتباط والانحدار والوساطة باستخدام Bootstrap. النتائج: بلغت متوسطات الحوكمة والجاهزية والمرونة ٣.٦٩ و ٣.٧٧ و ٣.٧٦ على التوالي، وارتبطت الحوكمة بالمرونة عند ٠.٧٠٣ وبالجاهزية عند ٠.٦٠٣، وارتبطت الجاهزية بالمرونة عند ٠.٦٥٧. كما بلغ الأثر غير المباشر للحوكمة عبر الجاهزية ٠.٢٢١، وكانت فترة الثقة ٩٥٪ بين ٠.١٤٣ و ٠.٣٠٤، بما يدعم وساطة جزئية في النموذج المحاكى. التوصيات: إنشاء إطار موحد لدورة حياة الأطراف الثالثة، وتصنيف المزودين بحسب الحرجية، وإدراج متطلبات الأمن والمرونة وحقوق التدقيق وخطط الخروج في العقود، وتنفيذ اختبارات تعافٍ مشتركة. ولا يجوز اعتماد النتائج بوصفها دليلًا ميدانيًا قبل استبدال البيانات المحاكاة باستجابات فعلية. الكلمات المفتاحية: حوكمة مخاطر الطرف الثالث، المرونة التشغيلية، جاهزية الأمن السيبراني، شركات التأمين، المملكة العربية السعودية.

Abstract:

Objectives: To examine the effect of third-party risk governance on operational resilience and test the mediating role of cybersecurity readiness in Saudi insurance companies. **Study setting:** The insurance, reinsurance, and insurance-services sector in Saudi Arabia. **Methodology:** A descriptive-analytical cross-sectional design was used with a 30-item questionnaire covering third-party risk governance, cybersecurity readiness, and operational resilience. Because the source file contained no field responses, 214 explicitly disclosed simulated observations were used solely to illustrate model testing through descriptive statistics, correlation, regression, and bootstrap mediation. **Results:** Mean scores for governance, readiness, and resilience were 3.69, 3.77, and 3.76. Governance correlated with resilience at 0.703 and readiness at 0.603, while readiness correlated with resilience at 0.657. The indirect effect through readiness was 0.221, with a 95% confidence interval of 0.143 to 0.304, supporting partial mediation in the simulated model. **Recommendations:** Insurers should establish an enterprise-wide third-party lifecycle framework, classify providers by criticality, embed cybersecurity, resilience, audit, and exit requirements in contracts, and conduct joint recovery exercises. The simulated results must be replaced with verified field data before any empirical publication claim.

Keywords: Third-party risk governance; operational resilience; cybersecurity readiness; insurance companies; Saudi Arabia.

١. المقدمة:

أعادت الرقمنة تشكيل نموذج تشغيل شركات التأمين؛ بإصدار الوثائق، وتسوية المطالبات، والدفع، وخدمة العملاء، والتحليلات الاكتوارية، وحفظ البيانات أصبحت تعتمد على منظومة من المزودين تشمل المنصات السحابية ومراكز الاتصال ومقدمي الأمن السيبراني وشبكات الخدمة. ويمنح هذا الاعتماد الشركات سرعة في الوصول إلى قدرات متخصصة، لكنه ينقل جزءاً من استمرارية الخدمة إلى جهات لا تخضع للسيطرة التنظيمية المباشرة، ويزيد مخاطر التعطل وتسرب البيانات وضعف الالتزام والتركيز لدى عدد محدود من المزودين.

تزداد أهمية الموضوع في السوق السعودي مع اتساع حجم الأعمال الرقمية؛ فقد بلغ إجمالي أقساط التأمين المكتتبة خلال عام ٢٠٢٥ نحو ٨٤.٣ مليار ريال، بزيادة ١٠.٧٪ عن عام ٢٠٢٤، بما يعكس نمو عدد المعاملات والبيانات والخدمات التي يجب أن تبقى متاحة وآمنة (هيئة التأمين، ٢٠٢٦). ولا يقتصر أثر تعطل الطرف الثالث على علاقة تعاقدية، بل قد يمتد إلى تأخر التعويضات، وتراكم المطالبات والشكاوى، والإضرار بثقة المستفيدين والالتزامات النظامية.

لهذا انتقلت الأطر الحديثة من مفهوم التعهيد الضيق إلى إدارة مخاطر جميع علاقات الطرف الثالث والأطراف اللاحقة طوال دورة الحياة. ويؤكد مجلس الاستقرار المالي أن الإدارة الفعالة تبدأ بتحديد الخدمات الحرجة والتبعيات، ثم العناية الواجبة والتعاقد والمراقبة والاستجابة والخروج، مع مراعاة مخاطر التركيز والاعتماد النظامي (Financial Stability Board, 2023). كما تضع الضوابط السعودية الأمن السيبراني للأطراف الخارجية والحوسبة السحابية ضمن نطاق الحوكمة والحماية والاستجابة والتعافي (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤، ٢٠٢٤ ب). تبحث الدراسة العلاقة بين حوكمة مخاطر الطرف الثالث والمرونة التشغيلية، وتقرح أن جاهزية الأمن السيبراني تمثل قناة وسيطة تحول السياسة والعقد والتقييم إلى قدرات فعلية على الحماية والكشف والاستجابة والتعافي. وتتمثل القيمة المضافة في دمج ثلاثة متغيرات غالباً ما تعالجها الأدبيات بصورة منفصلة، وتطبيق النموذج على سياق شركات التأمين السعودية مع بناء إطار تنفيذي يمكن استخدامه في تصميم برنامج الحوكمة وقياسه.

ويكتسب البحث أهمية إضافية من التحول الرقابي الجاري في قطاع التأمين السعودي؛ إذ يدفع الانتقال إلى أطر أكثر اعتماداً على المخاطر الشركات إلى توسيع نظرتها من الملاءة المالية المنعزلة إلى ترابط المخاطر المالية والتشغيلية والسيبرانية. فقرار الاستعانة بمزود سحابي أو منصة مطالبات قد يخفف التكلفة الرأسمالية، لكنه يخلق في الوقت نفسه مخاطر تركّز وتوافر وخصوصية والالتزام يجب أن تظهر في شهية المخاطر وتقارير الإدارة العليا وخطط التعافي.

كما أن حماية المستفيد تفرض منظوراً قائماً على نتائج الخدمة. فإذا ظل النظام التقني متاحاً جزئياً لكن العميل لم يستطع تقديم المطالبة أو استلام التعويض في الزمن المقبول، فإن المؤسسة لم تحقق المرونة المطلوبة. لذلك تربط الدراسة الحوكمة بمفهوم الخدمات الحيوية وحدود تحمل الأثر، وتتعامل مع أداء الطرف الثالث بوصفه جزءاً من نتيجة الخدمة النهائية لا مجرد التزام تعاقدية منفصل.

١-١ الآثار العلمية والتطبيقية:

علمياً، يميز النموذج بين الحوكمة بوصفها نظام قرار ومساءلة، والجاهزية السيبرانية بوصفها قدرة تنفيذية، والمرونة بوصفها نتيجة خدمة. ويمنح هذا الفصل المفاهيمي اختزال حوكمة الطرف الثالث في استبانة أمنية، أو اختزال المرونة في وجود خطة استمرارية. كما يوضح أن الجاهزية لا تستبدل الحوكمة، بل تنقل جزءاً من أثرها، وأن المسار المباشر يظل ضرورياً لتفسير المخاطر غير السيبرانية.

ويقدم البحث تشغيلاً قياسياً ملائماً لقطاع التأمين؛ إذ يربط أبعاد الحوكمة ببيئة المطالبات والبيانات الصحية والمالية ومراكز الاتصال والمنصات الرقمية، وقياس المرونة من خلال استمرار الخدمة والتعافي وتقليل التوقف والأثر المالي والسمعي. ويمكن أن يدعم هذا التشغيل بناء مقياس أكثر نصجاً في الدراسات اللاحقة، بشرط زيادة عدد الفقرات لكل بعد والتحقق من الصدق التقاربي والتمييزي على بيانات فعلية.

تطبيقياً، يساعد النموذج على توزيع المسؤولية وفق خطوط الدفاع. يملك خط الأعمال الخدمة والعلاقة ونتائجها اليومية، وتضع وظائف المخاطر والالتزام والأمن المعايير وتراقب التجاوزات، وتقدم المراجعة الداخلية تأكيداً مستقلاً على كفاية التصميم والفاعلية. ويجب أن يكون لكل خدمة حيوية مالك أعمال قادر على قبول المخاطر أو رفضها، لا أن تظل القرارات موزعة بين المشتريات والتقنية دون جهة مسؤولة عن الأثر على المستفيد.

كما تقترح النتائج الانتقال من المتابعة الدورية الثابتة إلى مراقبة قائمة على الأحداث. فتغير ملكية المزود، أو نقل موقع البيانات، أو تعيين طرف لاحق، أو تدهور المركز المالي، أو حادث سيبراني، أو ارتفاع الشكاوى ينبغي أن يؤدي إلى إعادة تقييم فوري. ويسمح ذلك بتوجيه الاهتمام إلى الإشارات المبكرة بدل انتظار مراجعة سنوية قد تأتي بعد تراكم الخطر.

وعلى مستوى مجلس الإدارة، ينبغي ألا يقتصر التقرير على عدد الموردين أو نسبة العقود السارية، بل يعرض الخدمات الحيوية المعتمدة على أطراف خارجية، وحالات تجاوز حدود الأثر، وتركيز المزودين، والاستثناءات المتأخرة، ونتائج الاختبارات، ومدى جاهزية خطط الخروج. فهذه المؤشرات تربط برنامج الحوكمة بشهية المخاطر والاستراتيجية وتجربة المستفيد.

٢. مشكلة الدراسة:

تتمثل المشكلة في احتمال وجود فجوة بين سرعة توسع شركات التأمين في الاعتماد على الأطراف الثالثة وبين نضج الحوكمة القادرة على استيعاب المخاطر الناتجة عن هذا الاعتماد. وقد تظهر الفجوة في عدم اكتمال سجل المزودين، أو تطبيق عناية واجبة واحدة على علاقات مختلفة الحرجية، أو ضعف بنود الإبلاغ عن الحوادث وحقوق التدقيق، أو اقتصار المتابعة على مؤشرات الأداء دون مؤشرات المخاطر، أو عدم قابلية خطط الخروج للتنفيذ والاختبار.

ولا تكفي جاهزية الشركة الداخلية عندما يحتفظ المزود ببيانات حساسة أو يملك وصولاً مرتفع الصلاحية أو يعتمد بدوره على طرف لاحق غير مرئي. كما أن العقد الجيد لا يضمن وحده استمرار الخدمة إذا لم تتوافر قدرات للكشف والتنسيق والتعافي والاختبار المشترك. وتؤكد مبادئ إدارة الطرف الثالث الحديثة ضرورة التناسب مع الحرجية، ورؤية سلسلة التوريد، وإدارة التركيز، والقدرة على الصمود والتكيف والتعافي (Basel Committee on Banking Supervision, 2025).

وتكشف مراجعة الأدبيات العربية عن تركيز أكبر على إدارة المخاطر العامة أو التشغيلية أو الإفصاح السيبراني، بينما تتناول الأدبيات الأجنبية مخاطر سلاسل التوريد أو البنوك والتقنية. ومن ثم تقل النماذج التي تجمع حوكمة الطرف الثالث والجاهزية السيبرانية والمرونة التشغيلية في قطاع التأمين السعودي وتختبر المسار غير المباشر. وعليه يمثل السؤال الرئيس في: ما أثر حوكمة مخاطر الطرف الثالث في تعزيز المرونة التشغيلية، وما الدور الوسيط لجاهزية الأمن السيبراني في هذه العلاقة؟

٣. أهمية الدراسة:

تتبع الأهمية العلمية من تطوير نموذج تفسيري يجمع نظرية الاعتماد على الموارد والقدرات الديناميكية والمنظور الاجتماعي-التقني، ويختبر كيف تنتقل قيمة الحوكمة إلى المرونة عبر الجاهزية السيبرانية. كما تقدم الدراسة تعريفات تشغيلية وأبعاداً قابلة للقياس لحوكمة الطرف الثالث في التأمين، وتسد فجوة قطاعية وجغرافية في الأدبيات العربية.

أما الأهمية التطبيقية فتتمثل في تزويد مجالس الإدارة ووظائف المخاطر والأمن والتقنية والعمليات والمشتريات والقانونية بخريطة متكاملة لدورة حياة العلاقة، وبمؤشرات تساعد على تصنيف المزودين وضبط العقود ومراقبة المخاطر واختبار البدائل. وتدعم الدراسة كذلك حماية المستفيد واستمرارية المطالبات والخدمات الحيوية، وتوفر أساساً لتطوير إرشاد قطاعي متناسق مع الضوابط الوطنية.

٤. أهداف الدراسة وأسئلتها وفرضياتها:

تهدف الدراسة إلى:

- (١) قياس مستوى حوكمة مخاطر الطرف الثالث وجاهزية الأمن السيبراني والمرونة التشغيلية في النموذج التطبيقي.
- (٢) تحليل أثر الحوكمة الكلية وأبعادها الخمسة في المرونة التشغيلية.
- (٣) اختبار أثر الحوكمة في الجاهزية السيبرانية وأثر الجاهزية في المرونة.
- (٤) اختبار الدور الوسيط لجاهزية الأمن السيبراني، وتحويل النتائج إلى توصيات وخارطة تنفيذ قابلة للقياس.

تتناظر الأهداف سبعة أسئلة فرعية تتناول مستويات المتغيرات، وأثر الحوكمة وأبعادها، ومساري الحوكمة إلى الجاهزية والجاهزية إلى المرونة، والوساطة. وتفترض الدراسة وجود آثار موجبة دالة لحوكمة الطرف الثالث وأبعادها في المرونة، وتأثير موجب للحوكمة في الجاهزية، وتأثير موجب للجاهزية في المرونة، ووساطة جزئية للجاهزية السيبرانية في العلاقة بين الحوكمة والمرونة.

٥. الأدب النظري للدراسة:

١-٥ المنطلقات النظرية:

تفسر نظرية الاعتماد على الموارد لجوء شركات التأمين إلى المزودين للحصول على التقنية والخبرة والاقتصاد في الحجم، لكنها توضح أيضًا أن المورد الخارجي قد يكتسب قوة عندما نقل البدائل أو ترتفع تكاليف الانتقال. وتخفف الحوكمة هشاشة الاعتماد من خلال التنويع، وحقوق التدقيق، وشفافية الأطراف اللاحقة، ونقل المعرفة، وخطط الخروج، والاحتفاظ بقدرة داخلية كافية للإشراف (Pfeffer & Salancik, 1978). وتصنف نظرية القدرات الديناميكية أن القيمة لا تتحقق بامتلاك الموارد فقط، بل بقدرة المنظمة على استشعار التغير، واغتنام الاستجابة المناسبة، وإعادة تشكيل الموارد والعمليات. فالسجل والتقييم المستمر يساعدان على الاستشعار، والعقد والضوابط يترجمان قرار الاستجابة، بينما تمثل خطط الخروج والتحويل وإعادة التوزيع قدرة على إعادة الهئية (Teece et al., 1997). وينسجم ذلك مع تصور المرونة بوصفها توقعًا ومواجهة وتكيفًا (Duchek, 2020).

أما المنظور الاجتماعي-التقني فيفسر الدور الوسيط للجهازية السيبرانية؛ فقد يكون العقد شاملاً، لكن غموض الأدوار أو ضعف التدريب أو عدم اختبار النسخ الاحتياطية يجعل الضمانات نظرية. وتظهر المرونة عندما تتكامل التقنية والأشخاص والإجراءات والعلاقة التعاقدية في منظومة قادرة على اكتشاف الحادث والتنسيق والتعافي والتعلم.

٢-٥ حوكمة مخاطر الطرف الثالث وأبعادها:

تشير حوكمة مخاطر الطرف الثالث إلى النظام الذي يحدد اختيار الأطراف الخارجية، وتصنيف حرجية الخدمات، وملكية قرار المخاطر، ومتطلبات العقد، والمراقبة، والتعامل مع الحوادث، وإنهاء العلاقة. وهي أوسع من إدارة الموردين التقليدية؛ لأنها تشمل المخاطر التشغيلية والسيبرانية والخصوصية والالتزام والمالية والسمعة والتركيز والأطراف اللاحقة، وتمتد من التخطيط حتى حذف البيانات وإلغاء الوصول بعد الخروج (Financial Stability Board, 2023).

الجدول (١) : أبعاد حوكمة مخاطر الطرف الثالث ومخرجاتها

البعد	مجال التركيز	المخرج الحاكم
العناية الواجبة قبل التعاقد	القدرة المالية والفنية والأمنية والامتثال والسمعة وسلسلة التوريد	تقرير فجوات ومخاطر متبقية وقرار قبول موثق
حوكمة العقود ومستويات الخدمة	SLA و KRI والإخطار وحقوق التدقيق والبيانات والاستمرارية	التزامات قابلة للقياس والإنفاذ والتصعيد
المراقبة والمتابعة المستمرة	الأداء والمخاطر والحوادث والتغيرات والأطراف اللاحقة	لوحة مؤشرات وإجراءات تصحيح وإعادة تصنيف
مخاطر البيانات والأمن السيبراني	الوصول والتشفير والموقع والسجلات والثغرات والاستجابة	ضوابط متناسبة وأدلة اختبار ومراجعة صلاحيات
الطوارئ والخروج والاستبدال	نقل الخدمة والبيانات والبدايل وإلغاء الوصول والتعلم	خطة انتقال مختبرة ضمن حدود تحمل الأثر

المصدر: إعداد الباحث بالاستناد إلى الأدبيات والمرجعيات التنظيمية الواردة في الدراسة.

الجدول (٢) : تصنيف مخاطر الأطراف الثالثة في شركات التأمين

نوع الخطر	مثال قطاعي	الأثر المحتمل	الضابط الحاكم
تشغيلي	تعطل منصة المطالبات أو مركز الاتصال	تأخر التسوية وتراكم الطلبات	SLA وسعة بديلة واختبار تعافٍ
سيبراني	اختراق حساب دعم لمزود تقني	وصول غير مصرح وتسرب أو توقف	أقل صلاحية وMFA وسجلات وإخطار
خصوصية وبيانات	معالجة بيانات صحية لدى طرف لاحق	انتهاك السرية والتزامات نظامية	تصنيف وتشفير وموقع وحذف موثق
التزام وقانوني	غياب حقوق التدقيق والوصول	تعذر التحقق ومعالجة المخالفة	بنود واضحة وحقوق وصول وإنهاء
مالي	تعثر المزود أو ارتفاع تكلفة الخدمة	توقف أو تكلفة انتقال مرتفعة	تقييم مالي وضمانات وخيارات انتقال
تركيز	اعتماد خدمات متعددة على مزود واحد	نقطة فشل مشتركة وامتداد الأثر	تحليل تركّز وتنويع وبدائل
سمعة	ضعف جودة مركز خدمة خارجي	فقد الثقة وتصاعد الشكاوى	معايير سلوك ورقابة جودة وتصعيد
طرف لاحق	مقاوّل فرعي غير معّلم	مخاطر غير مرئية وضعف السيطرة	إفصاح وموافقة وسريان الالتزامات

المصدر: إعداد الباحث في ضوء الضوابط الوطنية وأدبيات مخاطر الطرف الثالث.

يبين التصنيف أن الحادث الواحد قد يجمع أكثر من نوع من المخاطر؛ فتعطل مزود المطالبات قد يبدأ بخلل تقني، ثم يتحول إلى مخاطر التزام وسمعة وسيولة تشغيلية إذا تراكمت الطلبات. ولذلك لا ينبغي توزيع العلاقة على إدارات منفصلة دون مالك متكامل للخدمة، بل يجب ربط التقييم والعقد والمراقبة بخريطة تبعية توضح الأنظمة والبيانات والأطراف اللاحقة والبدائل ومسارات التصعيد.

وتختلف شدة الضوابط بحسب الحرجية. فالمزود الذي يقدم خدمة عامة محدودة البيانات لا يحتاج العمق نفسه المطلوب من منصة مرتبطة بالمطالبات أو البيانات الصحية. ويمنع هذا النهج الإفراط في الإجراءات منخفضة القيمة، ويوجه موارد الضمان والتدقيق والاختبار إلى العلاقات التي قد يتجاوز تعطلها حدود تحمل الأثر أو يوقف خدمة حيوية.

تبدأ الدورة بتحديد الخدمة ومالكها وحرجيتها وحدود أثرها، ثم إجراء عناية واجبة متناسبة مع مستوى المخاطر. وبعد التعاقد والتهيئة الآمنة، يجب ألا تتحول العلاقة إلى متابعة مالية أو تشغيلية فقط، بل تشمل المخاطر السيبرانية والتغيرات في سلسلة التوريد ونتائج الاختبارات. وعند الإنهاء ينبغي إثبات نقل البيانات والخدمة وإلغاء الصلاحيات ومعالجة التعلم المستفاد. وتؤكد تعليمات الإسناد السعودية مبادئ العناية الواجبة والاتفاقيات الشاملة والمراقبة وخطط الطوارئ والسجل المركزي وحقوق الوصول والتدقيق، مع ضرورة تكييف نطاق تطبيقها مع الجهة المنظمة لقطاع التأمين (البنك المركزي السعودي، ٢٠١٩).

٥-٣ جاهزية الأمن السيبراني:

الجاهزية السيبرانية قدرة مؤسسية تجمع الحوكمة والسياسات، وتقييم المخاطر، وحماية الأنظمة والبيانات، وكشف الأحداث، والاستجابة، والتعافي، والتدريب والاختبار. ويضع إطار NIST CSF 2.0 حوكمة مخاطر سلسلة التوريد ضمن وظيفة GOVERN، ويؤكد تحديد الموردين وحرجيتهم، وإبلاغ المتطلبات، ومراقبة الأداء طوال دورة الحياة (National Institute of Standards and Technology, 2024).

وفي البيئة السعودية تضع الضوابط الأساسية ECC 2-2024 وضوابط الحوسبة السحابية CCC-2:2024 حدًا أدنى لحماية الأصول والمعلومات، وتضمن متطلبات مستقلة للأطراف الخارجية والسحابية. وتكتسب الجاهزية دورها الوسيط عندما تحول التقييمات والعقود إلى قدرات على ضبط الوصول، واكتشاف الحوادث، وتبادل المعلومات، والاستجابة والتعافي والاختبار المشترك (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤، ب٢٠٢٤).

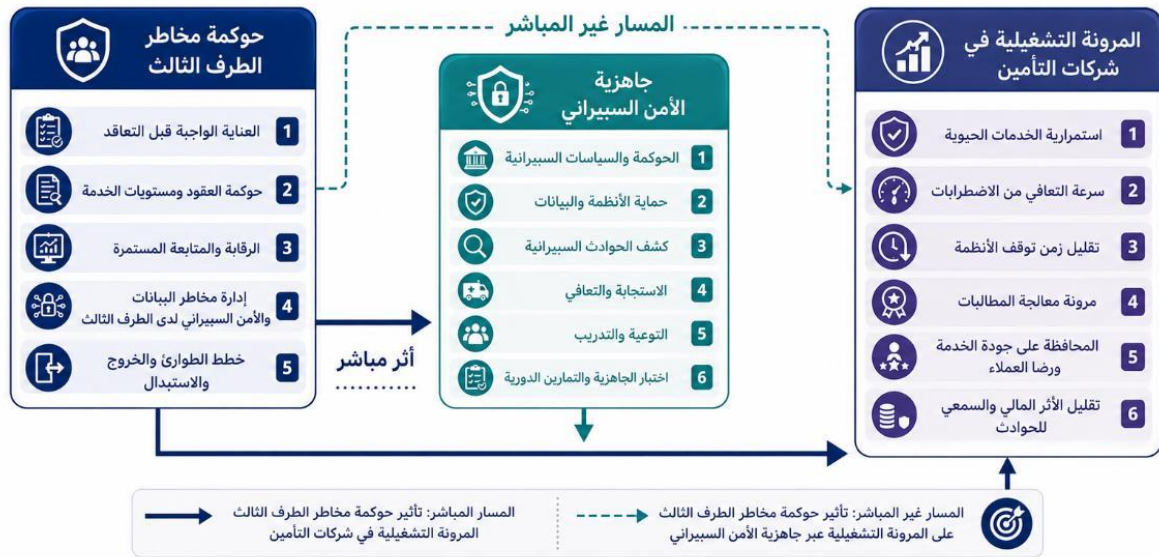
٥-٤: المرونة التشغيلية:

المرونة التشغيلية هي قدرة الشركة على الاستمرار في تقديم الخدمات الحيوية ضمن حدود أثر مقبولة أثناء الاضطراب، ثم التعافي والتكيف والتعلم. وهي أوسع من استمرارية الأعمال؛ إذ تبدأ من الخدمة التي تصل إلى المستفيد، وتحدد الموارد والتقنيات والبيانات والأشخاص والأطراف الثالثة التي تعتمد عليها، ثم تختبر السيناريوهات التي قد تقطعها (Basel Committee on Banking Supervision, 2021; International Association of Insurance Supervisors, 2023).

في التأمين تشمل الخدمات الحيوية استقبال المطالبة والتحقق من التغطية والوصول إلى البيانات واتخاذ قرار التسوية والدفع والتواصل. لذلك تقاس المرونة بقدرة الشركة على استمرار هذه النتائج أو استعادتها بسرعة، وتقليل زمن التوقف والأثر المالي والسمعي، والحفاظ على جودة الخدمة، ونقل العمل إلى بديل عندما يفشل المزود.

٥-٥: النموذج المفاهيمي ومنطق الوساطة:

يفترض النموذج مسارًا مباشرًا من حوكمة الطرف الثالث إلى المرونة ناتجًا عن جودة الاختيار والعقود والمراقبة والبدايل، ومسارًا غير مباشر يمر عبر جاهزية الأمن السيبراني. فالسياسة والعقد والتقييم لا يخلقان المرونة تلقائيًا؛ بل يرفعان وضوح الأدوار وضبط الوصول والكشف والتنسيق والاختبار، ثم تترجم هذه القدرات إلى استمرار الخدمة وتعافٍ أسرع وأثر أقل. ويظل الأثر المباشر قائمًا لأن فشل المزود قد يكون ماليًا أو تشغيليًا أو قانونيًا لا سيبرانيًا فقط.



الشكل (١) : النموذج المفاهيمي للعلاقة بين متغيرات الدراسة

المصدر: إعداد الباحث بالاستناد إلى النموذج النظري للدراسة.

تُختبر العلاقات السابقة من خلال الفرضيات الآتية:

- H1: تؤثر حوكمة مخاطر الطرف الثالث وأبعادها الخمسة تأثيرًا موجبًا في المرونة التشغيلية.
- H2: تؤثر حوكمة مخاطر الطرف الثالث تأثيرًا موجبًا في جاهزية الأمن السيبراني.
- H3: تؤثر جاهزية الأمن السيبراني تأثيرًا موجبًا في المرونة التشغيلية بعد ضبط أثر الحوكمة.
- H4: تتوسط جاهزية الأمن السيبراني جزئيًا العلاقة بين الحوكمة والمرونة التشغيلية.
- H5: توجد فروق في تقدير المرونة وفق الخصائص الوظيفية والتنظيمية.

٦. مراجعة الدراسات السابقة والفجوة البحثية:

تؤكد الدراسات العربية الصلة العامة بين إدارة المخاطر والأداء في التأمين؛ فقد خلصت دراسة بوداود (2021) إلى أن الإدارة المنظمة للمخاطر تساعد شركات التأمين على التنبؤ بالمخاطر وتحسين الأداء، وأبرزت طرطاق (2019) ضرورة إدماج المخاطر التشغيلية في الحوكمة والرقابة. كما أوضحت دراسة يعقوب وآخرين (2022) أهمية الإفصاح عن حوكمة الأمن والحماية والاستراتيجية، وأكدت حشمان وحدي (2024) تكامل الحوكمة والتوعية والتقنية في مواجهة المخاطر السيبرانية. ومع ذلك لم تجمع هذه الدراسات بين حوكمة الطرف الثالث والجاهزية والمرونة في نموذج وساطة واحد.

أما الأدبيات الأجنبية فانقلبت من التركيز على المورد المباشر إلى مخاطر السلسلة والتبعيات. بينت (2014) Boyson أهمية الرؤية والمعايير المشتركة والتحكم الاستراتيجي، وأظهرت (2019) Colicchia et al. أن التعاون والحوكمة عبر الحدود التنظيمية عنصران أساسيان لإدارة مخاطر المعلومات. وقدمت (2020) Duchek بناءً للمرونة يتكون من التوقع والمواجهة والتكيف، بينما دعمت (2023) Gani et al. العلاقة بين ممارسات إدارة السلسلة السيبرانية والأداء الأمني. وأظهرت (2023) Crosignani et al. انتقال أثر الهجمات عبر الروابط التجارية، وطورت (2025) Slapničar et al. نظرية عملية لتقييم مخاطر الموردين بالاعتماد على ٣٣ مقابلة و ٥٣ استبانة لخبراء أمن.

الجدول (٣) : خلاصة الدراسات السابقة وصلتها بالدراسة الحالية

الدراسة	المنهج/المجال	أبرز النتيجة	صلة الدراسة الحالية
بوداود (٢٠٢١)	دراسة حالة في التأمين	إدارة المخاطر المنظمة تحسن التنبؤ والأداء	لا تختبر الطرف الثالث أو الوساطة
طرطاق (٢٠١٩)	تحليل مخاطر تشغيلية في التأمين	الحوكمة الاستراتيجية ضرورية للمخاطر التشغيلية	لا تتناول الجاهزية السيبرانية
Colicchia et al (٢٠١٩)	تحليل استكشافي لسلاسل التوريد	التكامل والتعاون والرؤية ضرورية	يدعم الرقابة عبر الأطراف
Duchek (2020)	دراسة مفاهيمية	المرونة قدرة من التوقع والمواجهة والتكيف	توصل المتغير التابع
Gani et al (٢٠٢٣)	دراسة كمية لسلسلة التوريد السيبرانية	الممارسات المنظمة تحسن الأداء الأمني	يدعم مسار الحوكمة إلى الجاهزية
Slapničar et al (٢٠٢٥)	مختلط: ٣٣ مقابلة و ٥٣ استبانة	السياق والمعلومات والمراقبة تحدد نضج التقييم	أقرب الدراسات لمخاطر الموردين

المصدر: إعداد الباحث من الدراسات المشار إليها.

تتمثل الفجوة الموضوعية في ندرة الجمع بين الحوكمة والجاهزية والمرونة، والفجوة القطاعية في غلبة البنوك وسلاسل التوريد العامة، والفجوة الجغرافية في قلة الأدلة السعودية، والفجوة المنهجية في ندرة اختبار الوساطة. وتستجيب الدراسة بنموذج واحد يحدد خمسة أبعاد للحوكمة، ويختبر المسارين المباشر وغير المباشر، ويقترح مؤشرات وخارطة تنفيذ لقطاع التأمين.

وتكشف المقارنة أن الأدبيات العربية تمنح الدراسة أساساً قطاعياً مهماً، لكنها غالباً تقيس إدارة المخاطر بمستوى عام، بينما تقدم الدراسات الأجنبية تفصيلاً أكبر لمخاطر الموردين وسلاسل التوريد. ومع ذلك تظل قابلية نقل نتائج الصناعات التقنية أو المصرفية إلى التأمين محدودة؛ لأن دورة المطالبة والبيانات الصحية وشبكات مقدمي الخدمة تخلق تبعيات مختلفة من حيث الزمن والخصوصية وحقوق المستفيد.

كما أن كثيرًا من الدراسات يربط الحوكمة بالأداء الأمني أو يربط القدرات بالمرونة دون اختبار الآلية بينهما. ويتيح نموذج الوساطة التمييز بين أثر الحوكمة المباشر، مثل البدائل والعقد والملاءة، وبين الأثر الذي يتحقق من خلال جاهزية الكشف والاستجابة والتعافي. وهذا التمييز مهم عمليًا؛ لأنه يوضح لماذا قد تمتلك الشركة وثائق قوية لكنها لا تزال بطيئة في التعامل مع حادث لدى مزود حرج.

٧. المنهجية:

اعتمدت الدراسة المنهج الوصفي التحليلي بتصميم كمي مقطعي. ويصف الجانب الأول مستويات المتغيرات، بينما يختبر الجانب التحليلي الارتباطات والآثار المباشرة والوساطة. ويستخدم مستوى دلالة ٠.٠٥، مع عرض معاملات الأثر وفترات الثقة بدل الاقتصار على قيمة p .

يتكون المجتمع المستهدف من العاملين في شركات التأمين وإعادة التأمين والخدمات التأمينية في المملكة، ممن ترتبط وظائفهم بالمخاطر أو الالتزام أو تقنية المعلومات أو الأمن السيبراني أو العمليات أو المطالبات أو المراجعة الداخلية أو الشؤون القانونية والتعاقدات واستمرارية الأعمال. وتستخدم الدراسة عينة قصدية طبقية وظيفيًا لضمان مشاركة الأدوار الأكثر معرفة بدور الطرف الثالث.

طورت استبانة من ٣٠ عبارة على مقياس ليكرت الخماسي: عشر عبارات لحوكمة الطرف الثالث، وعشر للجاهزية السيبرانية، وعشر للمرونة التشغيلية. واستندت الصياغة إلى الضوابط السعودية وأطر FSB و BCBS و NIST و IAIS، وركزت كل عبارة على ممارسة قابلة للملاحظة. وتحقق صدق البناء باستخدام KMO و Bartlett، والثبات باستخدام كرونباخ ألفا.

ولأن الملف الأصلي لا يحتوي على ردود استبانة فعلية، استخدمت هذه الصيغة ٢١٤ مشاهدة محاكاة معلنة لتعكس التوزيع المتوقع للوظائف المستهدفة وتوضح طريقة الاختبار. ولذلك لا تمثل النتائج تقديرات ميدانية عن شركات بعينها، ويجب استبدال قاعدة البيانات وإعادة التحليل كاملاً قبل تقديم المقال بوصفه دراسة تجريبية. خللت البيانات بالتكرارات والمتوسطات والانحرافات، وارتباط بيرسون، والانحدار البسيط والمتعدد، وتحليل الوساطة بـ ٥,٠٠٠ عينة Bootstrap وفق منطق Hayes (2022).

راعى التصميم الطوعية والسرية وعدم جمع أسماء الأشخاص أو الشركات أو أسرار الحوادث، وعرض النتائج مجمعة، وحفظ البيانات في بيئة مقيدة الوصول. كما فُحص التحيز المنهجي المشترك، وأظهر اختبار العامل الواحد أن العامل الأول يفسر ٣٥.٦٪ من التباين، وهي نسبة دون ٥٠٪ لكنها لا تلغي الحاجة إلى مصادر بيانات متعددة في التطبيق الفعلي.

الجدول (٤) : ملخص التصميم المنهجي

العنصر	الوصف
التصميم	وصفي تحليلي، كمي مقطعي
المجتمع	وظائف المخاطر والأمن والتقنية والعمليات والرقابة في قطاع التأمين السعودي
قاعدة الاختبار	٢١٤ مشاهدة محاكاة معلنة لأغراض إيضاح النموذج
الأداة	٣٠ عبارة: ١٠ للحوكمة، ١٠ للجاهزية، ١٠ للمرونة
التحليل	وصفي، بيرسون، انحدار بسيط ومتعدد، وساطة Bootstrap = 5,000
معياري القرار	$\alpha = 0.05$ ، وفترة ثقة الأثر غير المباشر لا تشمل الصفر

المصدر: إعداد الباحث بالاستناد إلى تصميم الدراسة.

الجدول (٥) : التوزيع الوصفي للمشاهدات المحاكاة

المتغير	الفئة	التكرار	النسبة
جهة العمل	شركة تأمين	١٥٤	٧٢.٠٪
جهة العمل	إعادة تأمين/خدمات تأمينية/أخرى	٦٠	٢٨.٠٪
الإدارة	المخاطر	٤٢	١٩.٦٪

المتغير	الفئة	التكرار	النسبة
الإدارة	تقنية المعلومات	٣٦	١٦.٨%
الإدارة	الالتزام والأمن السيبراني	٦٠	٢٨.٠%
الإدارة	العمليات والمطالبات	٤٧	٢٢.٠%
الإدارة	المراجعة والقانونية والتعاقدات	٢٩	١٣.٦%
الخبرة	أقل من ٦ سنوات	٨٥	٣٩.٧%
الخبرة	٦ سنوات فأكثر	١٢٩	٦٠.٣%
حجم الشركة	صغيرة	٣٣	١٥.٤%
حجم الشركة	متوسطة	٧٣	٣٤.١%
حجم الشركة	كبيرة	١٠٨	٥٠.٥%
التعامل مع الأطراف	منخفض	١٨	٨.٤%
التعامل مع الأطراف	متوسط	٧٢	٣٣.٦%
التعامل مع الأطراف	مرتفع	١٢٤	٥٧.٩%

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة؛ لا تمثل استجابات ميدانية فعلية.

صُمم التوزيع الإيضاحي بحيث تمثل شركات التأمين المباشر النسبة الأكبر، مع حضور وظائف المخاطر والتقنية والأمن والالتزام والعمليات والمطالبات والرقابة. كما روعي أن تكون غالبية الحالات ذات خبرة ست سنوات فأكثر، وأن تمثل الشركات الكبيرة ومستويات التعامل المرتفعة حصة أكبر، لأن أثر التبعيات الخارجية يكون أوضح عادة في المنشآت الأكثر رقمنة وكثافة في العلاقات. ولا يجوز تفسير هذا التوزيع بوصفه وصفًا فعليًا لسوق العمل أو للشركات.

٨. النتائج:

١-٨ فحص جودة القياس:

الجدول (٦) : مؤشرات الصدق والثبات في البيانات المحاكاة

المؤشر	القيمة	المعيار	الحكم
KMO	٠.٩٣٢	≤ 0.60	ملاءمة مرتفعة
Bartlett χ^2	٢٧١٥.٧٧	$p < 0.001$ ؛ $df = 435$	دال إحصائيًا
ألفا - حوكمة الطرف الثالث	٠.٨٠٦	≤ 0.70	ثبات جيد
ألفا - جاهزية الأمن السيبراني	٠.٩٠٣	≤ 0.70	ثبات مرتفع
ألفا - المرونة التشغيلية	٠.٨٨١	≤ 0.70	ثبات مرتفع
العامل الواحد	٣٥.٦%	> 0.50	لا يفسر معظم التباين

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

تشير القيم إلى ملائمة مصفوفة الارتباطات للتحليل وإلى اتساق داخلي مقبول للمقاييس. وجاء ثبات الحوكمة أقل من المحورين الآخرين لأن عشر فقرات فقط تغطي خمسة أبعاد مختلفة، لكنه يتجاوز الحد المقبول. ويبرر ذلك استخدام الدرجات المركبة في النموذج الإيضاحي، مع توصية بتوسيع عدد الفقرات لكل بعد عند التطبيق الميداني.

٨-١ النتائج الوصفية:

الجدول (٧) : المتوسطات والانحرافات المعيارية للمتغيرات وأبعاد الحوكمة

المتغير/البعد	المتوسط	الانحراف	المستوى	الترتيب
جاهزية الأمن السيبراني	٣.٧٦٦	٠.٦٤٧	مرتفع	١
المرونة التشغيلية	٣.٧٦١	٠.٦١١	مرتفع	٢
حوكمة مخاطر الطرف الثالث	٣.٦٩١	٠.٥٢٣	مرتفع	٣
العناية الواجبة	٣.٨٥٥	٠.٧٢٤	مرتفع	١ ضمن الحوكمة
حوكمة العقود	٣.٧٦٩	٠.٧٥٩	مرتفع	٢ ضمن الحوكمة
مخاطر البيانات والأمن	٣.٧١٧	٠.٧٣٧	مرتفع	٣ ضمن الحوكمة
الرقابة المستمرة	٣.٦٩٦	٠.٧٣٧	مرتفع	٤ ضمن الحوكمة
الطوارئ والخروج والاستبدال	٣.٤١٨	٠.٨٣٢	مرتفع	٥ ضمن الحوكمة

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

جاءت المتغيرات الثلاثة في المستوى المرتفع، وتقدمت الجاهزية بمتوسط ٣.٧٧، ثم المرونة ٣.٧٦، فالحوكمة ٣.٦٩. وداخل الحوكمة جاءت العناية الواجبة أولاً بمتوسط ٣.٨٦، بينما كانت خطط الطوارئ والخروج والاستبدال الأدنى بمتوسط ٣.٤٢. ويشير هذا النمط إلى أن الاختيار والتقييم الأولي أكثر نضجاً من اختبار الفشل ونقل الخدمة، وهي فجوة مهمة لأن المرونة لا تثبت إلا عندما يكون البديل قابلاً للتنفيذ ضمن حدود الأثر.

٨-٣ اختبار العلاقات والوساطة:

الجدول (٨) : نتائج الارتباط والانحدار والوساطة

العلاقة/المسار	المعامل	الدلالة/التفسير	القرار
الحوكمة ↔ المرونة	$r = 0.703$	$p < 0.001$	ارتباط موجب قوي
الحوكمة ↔ الجاهزية	$r = 0.603$	$p < 0.001$	ارتباط موجب
الجاهزية ↔ المرونة	$r = 0.657$	$p < 0.001$	ارتباط موجب
الأثر الكلي للحوكمة في المرونة (c)	$\beta = 0.703$	$R^2 = 0.494$	دال
الحوكمة ← الجاهزية (a)	$\beta = 0.603$	$R^2 = 0.364$	دال
الجاهزية ← المرونة مع ضبط الحوكمة (b)	$\beta = 0.366$	$p < 0.001$	دال
الأثر المباشر للحوكمة (c')	$\beta = 0.482$	$p < 0.001$	دال
الأثر غير المباشر (a×b)	٠.٢٢١	٩٥% CI [0.143, 0.304]	وساطة جزئية

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة؛ Bootstrap = 5,000 عينة.

دعمت النتائج الإيضاحية الفرضيات الرئيسية؛ فقد فسرت الدرجة الكلية للحوكمة ٤٩.٤٪ من تباين المرونة. وفي الانحدار المتعدد فسرت الأبعاد الخمسة معاً ٥٠.١٪ من التباين، وكانت جميعها دالة: العناية الواجبة $\beta = 0.264$ ، حوكمة العقود $\beta = 0.217$ ، خطط الخروج $\beta = 0.198$ ، إدارة مخاطر البيانات $\beta = 0.130$ ، والرقابة المستمرة $\beta = 0.130$. كما لم تشمل فترة الثقة للأثر غير المباشر الصفر، ما يدعم وساطة جزئية للجاهزية السيبرانية في النموذج المحاكى.

ولم تظهر فروق دالة في المرونة وفق جهة العمل أو الإدارة أو سنوات الخبرة أو حجم الشركة أو مستوى التعامل مع الأطراف الخارجية، وكانت أحجام الأثر صغيرة. ولا يعني ذلك تطابق الشركات، بل قد يعكس طبيعة البيانات المحاكاة أو حاجة الفروق الفعلية إلى عينة ميدانية أكبر ومؤشرات موضوعية على مستوى الشركة.

٨-٤ ملخص قرارات الفرضيات:

الجدول (٩): قرارات اختبار فرضيات الدراسة

الفرضية	المضمون	القرار
H1	الحوكمة تؤثر في المرونة التشغيلية	مقبولة في النموذج المحاكى
H1.1	العناية الواجبة تؤثر في المرونة	مقبولة
H1.2	حوكمة العقود تؤثر في المرونة	مقبولة
H1.3	الرقابة المستمرة تؤثر في المرونة	مقبولة
H1.4	مخاطر البيانات والأمن تؤثر في المرونة	مقبولة
H1.5	الطوارئ والخروج تؤثر في المرونة	مقبولة
H2	الحوكمة تؤثر في الجاهزية السيبرانية	مقبولة
H3	الجاهزية تؤثر في المرونة	مقبولة
H4	الجاهزية تتوسط العلاقة	مقبولة - وساطة جزئية
H5	فروق وفق الخصائص التنظيمية	غير مقبولة في النموذج المحاكى

المصدر: إعداد الباحث من نتائج التحليل الإحصائي للبيانات المحاكاة.

تعكس القرارات اتساق المسارات مع النموذج النظري، إلا أن قبولها مقيد بطبيعة البيانات الإيضاحية. وفي التطبيق الميداني يجب فحص الافتراضات وإعادة تقدير المعاملات وفترات الثقة دون نقل أي قيمة من هذه النسخة، كما ينبغي الإفصاح عن معدل الاستجابة والاستبعادات وخصائص الشركات المشاركة بما يسمح للقارئ بتقدير حدود التعميم.

٩. الخاتمة ومناقشة النتائج:

توضح النتائج النموذجية أن حوكمة الطرف الثالث ليست وظيفة مشتريات أو التزام منفصلة، بل قدرة مؤسسية تؤثر في استمرار الخدمات الحيوية. ويتفق ارتفاع الحوكمة مع الاتجاهات التنظيمية التي تربط الإسناد بالعناية الواجبة والعقد والمراقبة والطوارئ، بينما يكشف انخفاض الخروج والاختبار عن فجوة بين جودة الترتيب في الظروف العادية والقدرة المثبتة عند فشل المزود.

يتسق تقدم العناية الواجبة والعقد مع ما توصلت إليه Slapničar et al. (2025) من أن نضج تقييم المورد يتأثر بالسياق والمعلومات والمراقبة، لا بالاستبيان الأمني وحده. كما ينسجم الأثر الموجب للحوكمة في الجاهزية مع Gani et al. (2023)، الذين أبرزوا دور ممارسات سلسلة التوريد السيبرانية في الأداء الأمني، ومع NIST CSF 2.0 الذي يجعل حوكمة السلسلة جزءاً من وظيفة GOVERN.

يدعم أثر الحوكمة في المرونة نظرية الاعتماد على الموارد؛ فالاعتماد الخارجي لا يصبح هشاشة حتمية عندما توجد آليات لاختيار المزود وفرض الشروط ومراقبة الأداء والحفاظ على البدائل. كما يدعم منطق القدرات الديناميكية؛ لأن التقييم المستمر وخطط الخروج تمكن الشركة من استشعار التدهور وإعادة تشكيل مواردها. وتتفق النتيجة مع (Boyson (2014 و Colicchia et al (2019) في أهمية الرؤية والتكامل والتحكم الاستراتيجي عبر السلسلة.

تقدم الوساطة أهم إضافة تفسيرية؛ فجزء من أثر الحوكمة يتحقق عندما ترفع قدرة الشركة على ضبط الوصول والكشف والاستجابة والتعافي والاختبار. وبقاء أثر مباشر يؤكد أن المرونة أوسع من الأمن السيبراني؛ فقد يفشل المزود ماليًا أو تشغيليًا، أو تصبح تكلفة التحويل مرتفعة، حتى مع وجود ضوابط أمنية جيدة. لذلك ينبغي أن يكون البرنامج متعدد الوظائف، تقوده المخاطر ومالكو الخدمات وتشارك فيه المشتريات والقانونية والالتزام والتقنية والأمن واستمرارية الأعمال.

وتخلص الدراسة إلى أن الطرف الثالث قد يكون خارج الهيكل القانوني لشركة التأمين، لكنه داخل سلسلة الخدمة ومسؤوليتها تجاه المستفيد والجهة المنظمة. والمرونة لا تُشتري من مزود، بل تُبنى من خلال حوكمة وبيانات وقدرات سيبرانية واختبارات واقعية وخيارات انتقال. ومع ذلك تبقى النتائج رقمية إيضاحية وليست دليلاً ميدانيًا، ويجب إعادة التحليل على استجابات فعلية قبل الاستدلال على واقع القطاع.

ومن منظور إداري، توضح النتائج أن التحسن لا يتحقق بتكثيف قوائم التحقق فقط. فإذا كانت العناية الواجبة قوية بينما لا تُعَلَق الملاحظات أو لا تُراجع الصلاحيات أو لا تُختبر خطة الخروج، تبقى المؤسسة معرضة لفجوة بين التصميم والتنفيذ. ولهذا ينبغي أن يقاس النضج بقدرة البرنامج على تغيير القرار: رفض مزود غير مناسب، أو فرض معالجة، أو خفض الوصول، أو تفعيل بديل قبل تجاوز حد الأثر.

ومن منظور رقابي، يشير النموذج إلى أهمية جمع معلومات عن التركزز والأطراف اللاحقة والحوادث المشتركة، لأن تقييم كل شركة منفردة قد لا يكشف الاعتماد القطاعي على منصة أو مزود واحد. ويمكن أن تدعم التمارين القطاعية وتبادل المؤشرات بصورة آمنة القدرة على رصد نقاط الفشل المشتركة، مع حماية سرية البيانات التجارية وحوادث العملاء.

١٠. التوصيات:

- (١) تأسيس إطار مؤسسي موحد يغطي دورة حياة الطرف الثالث من التخطيط والتصنيف إلى الخروج وإلغاء الوصول.
- (٢) إنشاء سجل مركزي لجميع المزودين والأطراف اللاحقة وربطه بالخدمات الحيوية والبيانات ومالكي المخاطر وحدود تحمل الأثر.
- (٣) تطبيق عناية واجبة متناسبة مع الحرجية، تشمل القدرة المالية والتشغيلية والسيبرانية والخصوصية والاستمرارية والتركيز.
- (٤) تطوير مكتبة بنود تعاقدية تتضمن الإخطار بالحوادث وحقوق التدقيق والوصول إلى الأدلة وقيود الطرف اللاحق وقابلية نقل البيانات وخطط الخروج.
- (٥) دمج مؤشرات الأداء KPI ومؤشرات المخاطر KRI في لوحة واحدة، مع حدود تصعيد وملاك واضحين للملاحظات والاستثناءات.
- (٦) تنفيذ اختبارات مشتركة سنوية على سيناريو تعطل مزود سحابي أو منصة مطالبات أو بوابة دفع، وقياس زمن الاستعادة والأثر على المستفيد.
- (٧) إجراء المسح الميداني الفعلي، وتوثيق إطار المعاينة والاستجابة والتنظيف، ثم إعادة جميع الاختبارات قبل إرسال الدراسة للنشر التجريبي.

الجدول (١٠) : خارطة تنفيذ مرحلية مقترحة

المرحلة	الأعمال الرئيسية	مؤشر الإنجاز
٠-٣ أشهر: التأسيس	سجل موحد، تصنيف الحرجية، سياسة وأدوار	اكتمال السجل وتعيين المالكين
٣-٦ أشهر: الضبط	عناية واجبة موحدة، مكتبة بنود، مراجعة الوصول	نسبة العقود المراجعة والاستثناءات
٦-١٢ شهرًا: الاختبار	خرائط تبعية، تمارين مشتركة، خطط خروج	نسبة الاختبارات وزمن الاستعادة
١٢-١٨ شهرًا: التكامل	تحليل التركزز، تقارير المجلس، ضمان مستقل	حدود التركزز ومستوى النضج
بعد ١٨ شهرًا: التحسين	أتمتة الرصد، سيناريوهات متقدمة، تعلم مستمر	انخفاض التعطل والخسائر وتحسن الخدمة

المصدر: إعداد الباحث في ضوء نتائج الدراسة والأطر التنظيمية.

١٠-١ مؤشرات الأداء والمخاطر المقترحة:

الجدول (١١) : لوحة استرشادية لمؤشرات أداء ومخاطر برنامج الطرف الثالث

النوع	المؤشر	طريقة القياس	الحد الاسترشادي	الدورية
KPI	تغطية التقييم	العلاقات المهمة المقيمة ÷ إجمالي العلاقات المهمة	$\leq 95\%$	شهري
KPI	اكتمال البنود	العقود المهمة المستوفية للحد الأدنى ÷ الإجمالي	$\leq 90\%$	ربع سنوي
KRI	الاستثناءات المتأخرة	استثناءات المخاطر المتجاوزة لتاريخ المعالجة	$\geq 5\%$	شهري
KRI	التركيز	الخدمات الحيوية المعتمدة على مزود واحد دون بديل	اتجاه هابط	ربع سنوي
KPI	الاختبار	الخدمات المهمة المختبرة خلال ١٢ شهرًا	100%	ربع سنوي
KPI	إغلاق الملاحظات	الملاحظات المغلقة في الموعد ÷ الإجمالي	$\leq 90\%$	شهري
KRI	زمن الإخطار	متوسط زمن إخطار الشركة بحادث لدى المزود	ضمن العقد	لكل حادث
KPI	زمن إلغاء الوصول	من قرار الانتهاء إلى إلغاء جميع الصلاحيات	≥ 24 ساعة	لكل خروج
KRI	تجاوز حد الأثر	الحوادث التي تجاوزت حد تحمل الخدمة	صفر/اتجاه هابط	ربع سنوي

المصدر: إعداد الباحث؛ تُعابير الحدود وفق شهية المخاطر وخصائص كل شركة.

تجمع اللوحة بين مؤشرات النشاط والنتيجة. فتغطية التقييم واكمال البنود تقيسان ما إذا كانت العملية نُفذت، بينما يقيس تجاوز حد الأثر والتركيز وزمن الإخطار ما إذا كان الخطر بقي ضمن المستوى المقبول. ولا ينبغي مكافأة البرنامج على ارتفاع عدد التقييمات إذا كانت الملاحظات لا تُغلق أو إذا ظل مزود واحد نقطة فشل مشتركة لخدمات متعددة.

وتحتاج المؤشرات إلى تعريفات موحدة ومصادر بيانات واضحة وملاك مسؤولين وحدود تصعيد. ويُستحسن ربطها بسجل الخدمات الحيوية ونظام الحوادث وإدارة العقود والوصول؛ لأن الاعتماد على جداول منفصلة يزيد أخطاء البيانات ويؤخر القرار. كما يجب مراجعة الحدود دوريًا بعد الحوادث والاختبارات والتغيرات التنظيمية، بحيث تصبح اللوحة أداة تعلم وتحسين لا مجرد تقرير امتثال.

وللجهة المنظمة دور مكمل من خلال تطوير إرشاد قطاعي يربط الإسناد والأمن والخصوصية والمرونة، وتشجيع تمارين مشتركة لسيناريوهات تعطل مزود سحابي أو منصة مطالبات أو بوابة دفع، وتسهيل تبادل مؤشرات المخاطر بصورة آمنة. ويساعد ذلك على كشف التبعيات المشتركة التي لا تظهر عند تقييم كل شركة أو عقد منفردًا.

١٠-٢ النموذج المؤسسي المقترح وتوزيع المسؤوليات:

يتطلب نجاح البرنامج نموذج تشغيل يحدد من يملك الخدمة، ومن يضع المعايير، ومن يراجع الالتزام، ومن يقرر قبول المخاطر أو إنهاء العلاقة. ويؤدي غموض المسؤوليات إلى تكرار التقييمات في بعض الجوانب وترك فجوات في جوانب أخرى، كما يبطئ الاستجابة عندما لا يعرف المزود نقطة الاتصال أو لا يملك فريق الحادث صلاحية اتخاذ القرار.

الجدول (١٢) : الأدوار والمسؤوليات في نموذج الحوكمة المقترح

الجهة	المسؤولية الرئيسية	المخرج المتوقع
مجلس الإدارة/لجنة المخاطر	اعتماد السياسة وشهية المخاطر وحدود التركيز	تقرير ربع سنوي عن الخدمات الحرجة والتجاوزات

الجهة	المسؤولية الرئيسية	المخرج المتوقع
الإدارة التنفيذية	تخصيص الموارد وحسم الاستثناءات الجوهرية	قرارات موثقة وخطط معالجة ممولة
مالك الخدمة في خط الأعمال	امتلاك العلاقة والنتيجة التشغيلية والمخاطر اليومية	تصنيف الحرجية ومراقبة SLA وخطة البديل
إدارة المخاطر والالتزام	وضع المنهج ومراجعة المخاطر المتبقية والالتزامات	سجل مخاطر وتقارير تصعيد ومتابعة الاستثناءات
المشتريات والشؤون القانونية	الاختيار والتفاوض وتحويل المتطلبات إلى عقد	بنود موحدة وحقوق تدقيق وإخطار وخروج
التقنية والأمن السيبراني	تقييم الضوابط والوصول والربط والكشف والاستجابة	أدلة فنية وسجلات صلاحيات ونتائج اختبارات
استمرارية الأعمال والعمليات	خرائط التبعية وحدود الأثر والتأمين والتعافي	سيناريوهات مشتركة وزمن استعادة وخطط انتقال
المراجعة الداخلية	تأكيد مستقل على التصميم والفاعلية	ملاحظات مرتبة حسب الخطر ومتابعة الإغلاق

المصدر: إعداد الباحث في ضوء نموذج خطوط الدفاع ودورة حياة الطرف الثالث.

يبدأ القرار بتصنيف الخدمة قبل البحث عن المزود؛ إذ يحدد مالك الأعمال نتيجة الخدمة وحدود أثرها والبيانات والتبعيات والبدائل، ثم تطبق وظائف الرقابة عمق العناية الواجبة المناسب. وبعد التعاقد، لا تنتقل ملكية المخاطر إلى المزود؛ فالطرف الخارجي مسؤول عن أداء التزاماته، لكن شركة التأمين تظل مسؤولة عن القرار والرقابة وحماية المستفيد وإثبات القدرة على الاستمرار.

وتحتاج الاستثناءات إلى حوكمة مستقلة عن المسار التجاري. فإذا لم يستوف المزود مطلبًا أساسيًا، يجب توثيق الخطر المتبقي والضوابط التعويضية والمالك الذي قبله وتاريخ انتهاء الاستثناء، مع منع التجديد التلقائي دون مراجعة. ويساعد ذلك على تجنب تحول الحل المؤقت إلى وضع دائم لا يظهر في تقارير المخاطر.

وعند الحادث، يجب أن تعمل قنوات التصعيد المتفق عليها قبل بدء الأزمة. فيحدد العقد زمن الإخطار والبيانات الواجب تقديمها وحقوق الوصول والتعاون، بينما تحدد الخطة الداخلية من يقود الاستجابة ومن يتواصل مع المستفيدين والجهة المنظمة ومن يقرر تفعيل البديل. وبعد التعافي تُجرى مراجعة مشتركة للأسباب والدروس، وتُحدَّث درجة المخاطر والعقد والخطة واللوحة.

أما الخروج فيجب أن يعامل كمشروع تشغيلي لا كبنود قانوني فقط. ويتضمن حصر البيانات وإعادتها أو حذفها، وإلغاء الحسابات والمفاتيح، ونقل المعرفة والتكوينات والسجلات، والتحقق من قدرة البديل، ومراقبة الخدمة خلال الفترة الانتقالية. وتزداد أهمية التشغيل المزدوج أو القدرة الداخلية الدنيا عندما تكون تكلفة الانتقال مرتفعة أو يكون المزود شديد التخصص.

١٠-٣ مستويات نضج برنامج حوكمة الطرف الثالث:

الجدول (١٣): مستويات النضج المقترحة لبرنامج حوكمة مخاطر الطرف الثالث

المستوى	الخصائص	الدليل التشغيلي	أولوية التطوير
١ - متفرق	علاقات وسجلات موزعة وقرارات تعتمد على الأفراد	قوائم غير مكتملة ومتابعة بعد وقوع المشكلة	حصر العلاقات وتعيين الملاك
٢ - أولي	سياسة عامة وتقييمات غير متجانسة	نماذج متعددة واستثناءات غير موحدة	تصنيف الحرجية وتوحيد المنهج

المستوى	الخصائص	الدليل التشغيلي	أولوية التطوير
٣ - محدد	دورة حياة وأدوار وبنود ومؤشرات موثقة	سجل مركزي وعقود معيارية وتقارير دورية	ربط الخدمات بالتبعيات والاختبارات
٤ - مُدار	مراقبة قائمة على المخاطر وقرارات مدعومة بالبيانات	KPI/KRI وحدود تصعيد وتمارين وخطط خروج	تحليل التركز والتكامل الآلي
٥ - متكيف	تنبؤ وتحسين مستمر وتعاون قطاعي	رصد أحداث وسيناريوهات متقدمة وضمنان مستقل	التعلم والمقارنة المعيارية والابتكار

المصدر: إعداد الباحث بالاستناد إلى دورة الحياة وخارطة التنفيذ المقترحة.

يساعد نموذج النضج على تحديد نقطة البداية وترتيب الاستثمار. فالشركة في المستوى الأول لا تحتاج أولاً إلى منصة تقنية معقدة، بل إلى حصر العلاقات ومالكي الخدمات والبيانات. وعندما يصبح المنهج محدداً وقابلًا للتكرار، يمكن الانتقال إلى التكامل الآلي والرصد القائم على الأحداث وتحليل التركز. ويمنع هذا التسلسل شراء أدوات لا تستند إلى بيانات وأدوار وقرارات واضحة.

وينبغي تقييم النضج لكل عنصر لا بمتوسط جملي يخفي الفجوات؛ فقد تكون الشركة في مستوى متقدم في العناية الواجبة، لكنها في مستوى أولي في الخروج أو الأطراف اللاحقة. لذلك يُعرض الملف على شكل خريطة فجوات تربط كل بعد بالخدمات الحيوية، ثم توضع خطة معالجة لها مالك وموعد ومؤشر نجاح. ويعاد التقييم بعد الحوادث والاختبارات والتغييرات الجوهرية، لا وفق دورة زمنية ثابتة فقط.

١١. حدود الدراسة ومقترحات البحوث المستقبلية:

تتمثل الحدود الأساسية في استخدام بيانات محاكاة لا تمثل استجابات بشرية فعلية، وفي التصميم المقطعي المقترح، والاعتماد على تقديرات ذاتية، والعينة القصدية، وتمثيل بعض الأبعاد بعدد محدود من الفقرات. لذلك لا يجوز تعميم المتوسطات أو معاملات الأثر على شركات التأمين السعودية قبل جمع بيانات فعلية وفق موافقة أخلاقية وإطار معاينة موثق وإعادة التحليل.

نقترح البحوث المستقبلية إجراء دراسة طولية تربط نضج الحوكمة بزمان التعطل والشكاوى والحوادث، واستخدام بيانات متعددة المصادر تشمل الموظفين والعقود وتقارير التدقيق وتمارين التعافي، ودراسة مخاطر التركز في السحابة والمنصات الصحية والدفع، ومقارنة الشركات بحسب الحجم والنضج الرقمي، وتطوير مقياس كامن متعدد الفقرات لكل بعد، واختبار متغيرات مثل ثقافة المخاطر ودعم الإدارة العليا ونضج استمرارية الأعمال.

وينبغي أن يسبق التطبيق الميداني تحديد إطار المعاينة بالتعاون مع الجهات والشركات، وتوثيق عدد الدعوات والاستجابات والاستبعايدات، وإجراء دراسة استطلاعية، والتحقق من الصدق والثبات والتحيز المنهجي. كما يستحسن ربط الاستبانة بمؤشرات موضوعية مثل عدد الحوادث وزمن الإخطار ونتائج الاختبارات ونسبة الملاحظات المتأخرة، بما يقلل الاعتماد على التصورات الذاتية ويرفع قوة الاستدلال.

ومن المهم أيضاً اختبار النموذج على مستويات متعددة؛ فبعض المتغيرات تقاس عند الموظف، بينما الحوكمة والمرونة خصائص تنظيمية. وقد تسمح عينات من عدة شركات باستخدام نماذج متعددة المستويات أو بيانات لوحية تكشف أثر الحجم والنضج الرقمي ونوع المنتج ودرجة التعهيد. ويمكن عندئذ مقارنة التأثيرات بين التأمين الصحي والمركبات والحماية والادخار وإعادة التأمين.

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

- البنك المركزي السعودي. (2017). الإطار التنظيمي للأمن السيبراني. <https://www.sama.gov.sa/ar-.sa/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf>
- البنك المركزي السعودي. (2019). تعليمات إسناد المهام إلى طرف ثالث. تعليمات-إسناد-إلى-طرف-ثالث. <https://rulebook.sama.gov.sa/ar/>
- بوداود، خ. (2021). أثر إدارة المخاطر على تحسين أداء شركات التأمين: دراسة حالة. مجلة الاقتصاد والتنمية المستدامة، ٤ (2)، ٨-٢٠.
- حشمان، س.، وحدي، ع. (2024). المخاطر السيبرانية في الصناعة المالية الإسلامية. المجلة الجزائرية للعلوم والسياسات الاقتصادية، [١٥:RLI] (عدد خاص)، [٧٢-٥٩].
- طرطاق، ر. (2019). التوجهات الاستراتيجية لإدارة المخاطر التشغيلية في شركات التأمين على ضوء متطلبات معيار الملاءة ٢. مجلة العلوم الإدارية والمالية، ٩٢-١١٠.
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٤). الضوابط الأساسية للأمن السيبراني (ECC 2-2024). <https://nca.gov.sa/ar/regulatory-documents/controls-list/ecc/>
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٤ب). ضوابط الأمن السيبراني للحوسبة السحابية (CCC-2:2024). <https://nca.gov.sa/ar/regulatory-documents/controls-list/ccc/>
- هيئة التأمين. (2026). تقرير سوق التأمين السعودي لعام ٢٠٢٥: مؤشرات ونتائج القطاع. <https://www.ia.gov.sa/ar/media-center/news/117>
- يعقوب، ا.، إ.، ووهاب، أ. م. ع.، والفرطوسي، ع. م. ح. (2022). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية وفق المتطلبات الدولية: دراسة اختبارية. <https://asjp.cerist.dz/en/article/192579>

ثانياً: المراجع الأجنبية:

- Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d516.htm>.
- Basel Committee on Banking Supervision. (2025). Principles for the sound management of third-party risk (BCBS d605). Bank for International Settlements. <https://www.bis.org/bcbs/publ/d605.htm>.
- Benaroch, M. (2021). Cybersecurity risk in IT outsourcing: Challenges and emerging realities. Journal of Cybersecurity, 7(1), tyab020. <https://doi.org/10.1093/cybsec/tyab020>.
- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353. <https://doi.org/10.1016/j.technovation.2014.02.001>.
- Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. Supply Chain Management, 24(2), 215-240. <https://doi.org/10.1108/SCM-09-2017-0289>.
- Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. Supply Chain Management, 27(1), 30-53. <https://doi.org/10.1108/SCM-02-2020-0073>.
- Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. Journal of Financial Economics, 147(2), 432-448. <https://doi.org/10.1016/j.jfineco.2022.12.002>.
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13, 215-246. <https://doi.org/10.1007/s40685-019-0085-7>.

- Financial Stability Board. (2023). Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities. <https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/>.
- Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M. L. (2023). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data Systems*, 123(3), 843-861. <https://doi.org/10.1108/IMDS-05-2022-0313>.
- Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). Guilford Press.
- Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*, 23(1), 7-44. <https://doi.org/10.1111/ijmr.12239>.
- International Association of Insurance Supervisors. (2023). Issues paper on insurance sector operational resilience. <https://www.iaisweb.org/>.
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>.
- Pfeffer, J., & Salancik, G. R. (1978). The external control of organizations: A resource dependence perspective. Harper & Row.
- Slapničar, S., Vidmar, T., & Tsen, E. (2025). Process theory of supplier cyber risk assessment. *Australasian Journal of Information Systems*, 29, 1-33. <https://doi.org/10.3127/ajis.v29.5323>.
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z).