

بسم الله الرحمن الرحيم



جامعة ميداووشن

كلية الإدارة - برنامج إدارة المخاطر

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

رسالة مقدمة لاستكمال متطلبات درجة الماجستير في إدارة المخاطر

إعداد الطالب:

الرقم الجامعي:

إشراف: د.

العام الجامعي ١٤٤٨هـ - ٢٠٢٦م

الملخص :

هدفت الدراسة إلى قياس أثر حوكمة مخاطر الطرف الثالث في تعزيز المرونة التشغيلية لدى شركات التأمين في المملكة العربية السعودية، مع اختبار الدور الوسيط لجاهزية الأمن السيبراني. وانطلقت الدراسة من اتساع اعتماد شركات التأمين على مزودي الأنظمة السحابية، ومنصات إدارة المطالبات، ومراكز الاتصال، ومقدمي خدمات الأمن السيبراني والتحليلات والوساطة الرقمية؛ الأمر الذي جعل استمرارية الخدمات الحيوية مرتبطة بقدرة الشركة على إدارة المخاطر الممتدة خارج حدودها التنظيمية. واعتمدت الدراسة المنهج الوصفي التحليلي، وطُورت استبانة من (٣٠) عبارة موزعة على ثلاثة محاور: حوكمة مخاطر الطرف الثالث، وجاهزية الأمن السيبراني، والمرونة التشغيلية.

ولأغراض بناء نموذج تحليلي كامل، طُبقت إجراءات التحليل على عينة محاكاة قوامها (٢١٤) مفردة تعكس التوزيع المتوقع للعاملين في إدارات المخاطر والالتزام وتقنية المعلومات والأمن السيبراني والعمليات والمطالبات والمراجعة الداخلية والتعاقدات. أظهرت النتائج النموذجية أن مستوى حوكمة مخاطر الطرف الثالث جاء مرتفعاً بمتوسط (٣,٦٩)، وأن جاهزية الأمن السيبراني جاءت مرتفعة بمتوسط (٣,٧٧)، كما جاءت المرونة التشغيلية مرتفعة بمتوسط (٣,٧٦). وتبين وجود ارتباطات موجبة ذات دلالة إحصائية بين المتغيرات، وبلغ معامل الارتباط بين حوكمة مخاطر الطرف الثالث والمرونة التشغيلية (٠,٧٠٣)، وبين الحوكمة والجاهزية السيبرانية (٠,٦٠٣)، وبين الجاهزية السيبرانية والمرونة التشغيلية (٠,٦٥٧).

وأظهر تحليل الوساطة أن حوكمة مخاطر الطرف الثالث تؤثر في المرونة التشغيلية تأثيراً مباشراً وغير مباشر عبر جاهزية الأمن السيبراني؛ إذ بلغ الأثر غير المباشر (٠,٢٢١)، وكانت فترة الثقة بالتمهيد المعلمي Bootstrap لا تشمل الصفر. وبناءً على ذلك، أوصت الدراسة بتأسيس إطار مؤسسي موحد لدورة حياة الأطراف الثالثة، وتصنيف المزودين وفق الأهمية والحرجية، وإدراج متطلبات الأمن السيبراني والمرونة وحقوق التدقيق وخطط الخروج في العقود، وربط مؤشرات أداء المزودين بحدود تحمل الأثر للخدمات الحيوية، وتنفيذ اختبارات مشتركة للاستجابة والتعافي.

الكلمات المفتاحية: حوكمة المخاطر، مخاطر الطرف الثالث، المرونة التشغيلية، جاهزية الأمن السيبراني، شركات التأمين، المملكة العربية السعودية.

Abstract:

This study examines the effect of third-party risk governance on operational resilience in Saudi insurance companies and tests the mediating role of cybersecurity readiness. The study responds to insurers' growing reliance on cloud platforms, claims administrators, contact centers, digital intermediaries, analytics providers, and cybersecurity service providers. A descriptive-analytical design was adopted, using a 30-item questionnaire covering third-party risk governance, cybersecurity readiness, and operational resilience.

Because the source proposal did not include field responses, this complete analytical draft uses a clearly disclosed simulated dataset of 214 observations. The illustrative results indicate high levels of third-party risk governance ($M = 3.69$), cybersecurity readiness ($M = 3.77$), and operational resilience ($M = 3.76$). Third-party risk governance was positively associated with operational resilience ($r = 0.703$) and cybersecurity readiness ($r = 0.603$); cybersecurity readiness was also positively associated with operational resilience ($r = 0.657$). Mediation analysis showed a statistically significant indirect effect of 0.221, indicating that cybersecurity readiness partially transmits the effect of third-party risk governance to operational resilience.

The study recommends an enterprise-wide third-party lifecycle framework, risk-based criticality classification, enforceable cybersecurity and resilience clauses, auditable service-level indicators, tested exit strategies, and joint disruption exercises with critical providers.

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

المحتويات :

٢	الملخص :
٣	Abstract :
٨	قائمة الجداول :
٩	قائمة الأشكال :
٩	قائمة الاختصارات :
١٠	الفصل الأول : الإطار العام للدراسة :
١١	١,١ مقدمة الفصل :
١٢	١,٢ خلفية الدراسة وسياقها :
١٢	١,٢,١ تطور قطاع التأمين السعودي :
١٢	١,٢,٢ التحول الرقمي والاعتماد على الأطراف الثالثة :
١٣	١,٢,٣ السياق التنظيمي والسيبراني :
١٣	١,٣ مشكلة الدراسة :
١٤	١,٤ أسئلة الدراسة :
١٤	١,٥ أهداف الدراسة :
١٥	١,٦ أهمية الدراسة :
١٥	١,٦,١ الأهمية العلمية :
١٥	١,٦,٢ الأهمية التطبيقية :
١٥	١,٦,٣ الأهمية التنظيمية والمجتمعية :
١٦	١,٧ مبررات اختيار الموضوع :
١٦	١,٨ حدود الدراسة :
١٧	١,٩ مصطلحات الدراسة وتعريفاتها الإجرائية :
١٨	١,١٠ متغيرات الدراسة والنموذج المفاهيمي :
١٩	١,١١ فرضيات الدراسة :
٢٠	١,١٢ هيكل الرسالة :
٢١	١,١٣ خلاصة الفصل :
٢٢	الفصل الثاني : الإطار النظري والدراسات السابقة :
٢٣	٢,١ مقدمة الفصل :
٢٣	٢,٢ المنطلقات النظرية للدراسة :
٢٣	٢,٢,١ نظرية الاعتماد على الموارد :
٢٤	٢,٢,٢ نظرية القدرات الديناميكية :
٢٤	٢,٢,٣ إدارة مخاطر المؤسسة والحوكمة المتكاملة :
٢٥	٢,٢,٤ المنظور الاجتماعي-التقني :
٢٥	٢,٣ حوكمة مخاطر الطرف الثالث :
٢٥	٢,٣,١ المفهوم والنطاق :
٢٥	٢,٣,٢ دورة حياة العلاقة مع الطرف الثالث :
٢٧	٢,٣,٣ مخاطر الأطراف الثالثة في شركات التأمين :
٢٨	٢,٣,٤ البعد الأول: العناية الواجبة قبل التعاقد :
٢٩	٢,٣,٥ البعد الثاني: حوكمة العقود ومستويات الخدمة :
٢٩	٢,٣,٦ البعد الثالث: الرقابة والمتابعة المستمرة :
٣٠	٢,٣,٧ البعد الرابع: مخاطر البيانات والأمن السيبراني لدى الطرف الثالث :

٣٠	٢,٣,٨ البعد الخامس: خطط الطوارئ والخروج والاستبدال:
٣١	٢,٤ جاهزية الأمن السيبراني:
٣١	٢,٤,١ المفهوم ومكونات الجاهزية:
٣١	٢,٤,٢ الحوكمة والسياسات السيبرانية:
٣١	٢,٤,٣ الحماية وإدارة الهوية والبيانات:
٣١	٢,٤,٤ الكشف والاستجابة والتعافي:
٣٢	٢,٤,٥ الوعي والتدريب والاختبار:
٣٢	٢,٥ المرونة التشغيلية:
٣٢	٢,٥,١ مفهوم المرونة التشغيلية:
٣٣	٢,٥,٢ الفرق بين المرونة واستمرارية الأعمال:
٣٣	٢,٥,٣ الخدمات الحيوية وحدود تحمل الأثر:
٣٤	٢,٥,٤ رسم خرائط التبعية:
٣٤	٢,٥,٥ أبعاد المرونة التشغيلية في الدراسة:
٣٤	٢,٦ تفسير العلاقات بين متغيرات الدراسة:
٣٤	٢,٦,١ الحوكمة والمرونة التشغيلية:
٣٥	٢,٦,٢ الحوكمة وجاهزية الأمن السيبراني:
٣٥	٢,٦,٣ الجاهزية السيبرانية والمرونة التشغيلية:
٣٥	٢,٦,٤ منطق الوساطة:
٣٦	٢,٧ السياق التنظيمي والمعياري:
٣٨	٢,٨ الدراسات السابقة:
٣٨	٢,٨,١ الدراسات العربية:
٤٠	٢,٨,٢ الدراسات الأجنبية:
٤٣	٢,٨,٣ التعقيب على الدراسات السابقة:
٤٣	٢,٩ الفجوة البحثية وإسهام الدراسة:
٤٤	٢,١٠ خلاصة الفصل:
٤٥	الفصل الثالث: منهجية الدراسة وإجراءاتها:
٤٦	٣,١ مقدمة الفصل:
٤٦	٣,٢ منهج الدراسة وتصميمها:
٤٦	٣,٣ مجتمع الدراسة:
٤٧	٣,٤ عينة الدراسة وطريقة اختيارها:
٤٧	٣,٥ مصادر البيانات:
٤٧	٣,٥,١ البيانات الثانوية:
٤٧	٣,٥,٢ البيانات الأولية:
٤٧	٣,٦ بناء أداة الدراسة:
٤٨	٣,٧ التعريفات القياسية وترميز الدرجات:
٤٩	٣,٨ صدق الأداة:
٤٩	٣,٨,١ الصدق الظاهري وصدق المحتوى:
٤٩	٣,٨,٢ صدق البناء:
٤٩	٣,٩ ثبات الأداة:
٥٠	٣,١٠ الدراسة الاستطلاعية:
٥٠	٣,١١ إجراءات جمع البيانات:
٥٠	٣,١٢ معالجة البيانات المفقودة والقيم المتطرفة:
٥١	٣,١٣ التحيز المنهجي المشترك:
٥١	٣,١٤ أساليب التحليل الإحصائي:
٥٢	٣,١٥ نموذج اختبار الوساطة:

٥٢	٣,١٦ الاعتبارات الأخلاقية:
٥٣	٣,١٧ قيود المنهج:
٥٣	٣,١٨ خلاصة الفصل:
٥٤	الفصل الرابع : عرض النتائج وتحليلها ومناقشتها
٥٥	٤,١ مقدمة الفصل:
٥٥	٤,٢ فحص البيانات الأولي:
٥٥	٤,٣ خصائص عينة الدراسة:
٥٧	٤,٤ صدق وثبات أداة القياس:
٥٧	٤,٥ النتائج الوصفية لمتغيرات الدراسة:
٥٨	٤,٥,١ أبعاد حوكمة مخاطر الطرف الثالث:
٥٩	٤,٥,٢ فقرات جاهزية الأمن السيبراني:
٦٠	٤,٥,٣ فقرات المرونة التشغيلية:
٦١	٤,٦ الارتباطات بين متغيرات الدراسة:
٦٢	٤,٧ اختبار الفرضية الرئيسة الأولى وأبعادها:
٦٣	٤,٨ اختبار H2 و H3 ونموذج الوساطة H4:
٦٤	٤,٩ اختبار الفروق وفق الخصائص التنظيمية:
٦٥	٤,١٠ ملخص قرارات اختبار الفرضيات:
٦٥	٤,١١ مناقشة النتائج:
٦٥	٤,١١,١ مستوى حوكمة مخاطر الطرف الثالث:
٦٦	٤,١١,٢ مستوى جاهزية الأمن السيبراني:
٦٦	٤,١١,٣ مستوى المرونة التشغيلية:
٦٦	٤,١١,٤ أثر الحوكمة في المرونة:
٦٧	٤,١١,٥ الدور الوسيط لجاهزية الأمن السيبراني:
٦٧	٤,١٢ خلاصة الفصل:
٦٨	الفصل الخامس: الاستنتاجات والتوصيات
٦٩	٥,١ مقدمة الفصل:
٦٩	٥,٢ ملخص النتائج الرئيسة:
٧٠	٥,٣ الاستنتاجات والإجابة عن أسئلة الدراسة:
٧٠	٥,٣,١ واقع حوكمة مخاطر الطرف الثالث:
٧٠	٥,٣,٢ مستوى جاهزية الأمن السيبراني:
٧١	٥,٣,٣ مستوى المرونة التشغيلية:
٧١	٥,٣,٤ أثر الحوكمة في المرونة:
٧١	٥,٣,٥ الدور الوسيط للجاهزية السيبرانية:
٧٢	٥,٤ التوصيات العملية:
٧٣	٥,٥ النموذج المقترح لحوكمة مخاطر الطرف الثالث:
٧٤	٥,٦ مستويات النضج المقترحة:
٧٥	٥,٧ خارطة التنفيذ المرحلية:
٧٦	٥,٨ مؤشرات الأداء والمخاطر المقترحة
٧٧	٥,٩ توصيات للجهات التنظيمية والقطاع:
٧٨	٥,١٠ حدود الدراسة:
٧٨	٥,١١ مقترحات للبحوث المستقبلية:
٧٩	٥,١٢ الخاتمة العامة :
٨٠	قائمة المراجع:
٨٠	أولاً: المراجع العربية
٨٠	ثانيًا: المراجع الأجنبية

الملاحق:.....	٨٤
الملحق (١): استبانة الدراسة.....	٨٤
الملحق (٢): نموذج الموافقة المستنيرة.....	٨٧
الملحق (٣): استمارة تحكيم الأداة.....	٨٨
الملحق (٤): قاموس الترميز والتحليل.....	٨٩

قائمة الجداول:

- جدول (١-١): المتغيرات وأبعادها وتعريفاتها الإجرائية
- جدول (٢-١): فرضيات الدراسة
- جدول (١-٢): دورة حياة إدارة مخاطر الطرف الثالث
- جدول (٢-٢): تصنيف مخاطر الأطراف الثالثة في شركات التأمين
- جدول (٣-٢): مقارنة بين استمرارية الأعمال والمرونة التشغيلية
- جدول (٤-٢): المرجعيات التنظيمية والمعيارية للدراسة
- جدول (٥-٢): ملخص الدراسات العربية السابقة
- جدول (٦-٢): ملخص الدراسات الأجنبية السابقة
- جدول (٧-٢): الفجوة البحثية واستجابة الدراسة الحالية
- جدول (١-٣): توزيع فقرات الاستبانة
- جدول (٢-٣): معايير تفسير المتوسطات
- جدول (٣-٣): إجراءات التحليل الإحصائي
- جدول (١-٤): خصائص عينة الدراسة
- جدول (٢-٤): مؤشرات الصدق والثبات
- جدول (٣-٤): المتوسطات والانحرافات المعيارية للمتغيرات
- جدول (٤-٤): نتائج أبعاد حوكمة مخاطر الطرف الثالث
- جدول (٥-٤): نتائج جاهزية الأمن السيبراني
- جدول (٦-٤): نتائج المرونة التشغيلية
- جدول (٧-٤): مصفوفة الارتباطات
- جدول (٨-٤): الانحدار المتعدد لأبعاد الحوكمة
- جدول (٩-٤): اختبار المسارات والوساطة
- جدول (١٠-٤): اختبار الفروق وفق المتغيرات التنظيمية
- جدول (١١-٤): قرار اختبار الفرضيات
- جدول (١-٥): مصفوفة التوصيات والأولوية والمسؤولية
- جدول (٢-٥): خارطة التنفيذ المرحلية المقترحة

قائمة الأشكال

شكل (١-١): النموذج المفاهيمي للدراسة

شكل (١-٢): منطق انتقال أثر الحوكمة إلى المرونة التشغيلية

شكل (١-٤): متوسطات أبعاد حوكمة مخاطر الطرف الثالث

شكل (٢-٤): نتائج نموذج الوساطة

شكل (١-٥): نموذج الحوكمة التطبيقي المقترح

قائمة الاختصارات

الاختصار	المعنى
TPRM	Third-Party Risk Management - إدارة مخاطر الطرف الثالث
ERM	Enterprise Risk Management - إدارة مخاطر المؤسسة
BCM	Business Continuity Management - إدارة استمرارية الأعمال
SLA	Service Level Agreement - اتفاقية مستوى الخدمة
KPI	Key Performance Indicator - مؤشر الأداء الرئيس
KRI	Key Risk Indicator - مؤشر المخاطر الرئيس
RTO	Recovery Time Objective - الهدف الزمني للتعافي
RPO	Recovery Point Objective - نقطة التعافي المستهدفة
NCA	National Cybersecurity Authority - الهيئة الوطنية للأمن السيبراني
SAMA	Saudi Central Bank - البنك المركزي السعودي
IA	Insurance Authority - هيئة التأمين
FSB	Financial Stability Board - مجلس الاستقرار المالي
BCBS	Basel Committee on Banking Supervision - لجنة بازل للرقابة المصرفية
IAIS	International Association of Insurance Supervisors - الجمعية الدولية لمشرفي التأمين

الفصل الأول : الإطار العام للدراسة

الخلفية، المشكلة، الأسئلة، الأهداف، الفرضيات، والمتغيرات



١,١ مقدمة الفصل:

أعادت الرقمنة تشكيل نموذج تشغيل شركات التأمين؛ فلم تعد العمليات الجوهرية تُنجز داخل الحدود التنظيمية للشركة وحدها، بل أصبحت موزعة عبر منظومة من مزودي الخدمات تشمل الحوسبة السحابية، وأنظمة إصدار الوثائق، ومنصات إدارة المطالبات، وشركات الفحص والتقييم، ومراكز الاتصال، ومقدمي التحليلات والخدمات الاكتوارية والأمن السيبراني. ويتيح هذا النموذج الوصول إلى خبرات متخصصة، وخفض بعض التكاليف، وزيادة القابلية للتوسع؛ لكنه في المقابل ينقل جزءًا من الاعتماد التشغيلي إلى جهات لا تخضع للسيطرة المباشرة للشركة، ويخلق مخاطر مرتبطة بالتوقف، وتسرب البيانات، وضعف الالتزام، وتركيز الخدمات لدى عدد محدود من المزودين.

وتزداد حساسية هذا الاعتماد في قطاع التأمين لأن الخدمة لا تتوقف عند بيع وثيقة؛ فهي تشمل استقبال المطالبة والتحقق من التغطية وتبادل الوثائق والبيانات الصحية والمالية، واتخاذ قرار التسوية، وصرف التعويض، والتواصل مع العميل. وأي تعطل لدى مزود خارجي قد يمتد سريعًا إلى سلسلة الخدمة، فيتأخر التعويض، وترتفع الشكاوى، وتتأثر الثقة والسمعة والالتزامات النظامية. لذلك أصبحت حوكمة مخاطر الطرف الثالث جزءًا من صميم إدارة المخاطر المؤسسية والمرونة التشغيلية، لا مجرد نشاط مشتريات أو متابعة عقدية (البنك المركزي السعودي، ٢٠١٧؛ الهيئة الوطنية للأمن السيبراني، ٢٠٢٤) (FSB, 2023; BCBS, 2025).

يستند مفهوم المرونة التشغيلية إلى قدرة المؤسسة على الاستمرار في تقديم خدماتها الحيوية ضمن حدود أثر مقبولة أثناء الاضطرابات، ثم التعافي والتكيف والتعلم. ولا تتحقق هذه القدرة بخطط الطوارئ الداخلية فقط؛ إذ يجب أن تشمل الخدمات المشتركة، والتبعيات التقنية، والأطراف الثالثة والأطراف اللاحقة في سلسلة التوريد. ومن هنا تفترض الدراسة أن حوكمة الطرف الثالث ترفع المرونة من خلال مسارين: مسار مباشر ناتج عن جودة العناية الواجبة والعقود والرقابة والخروج، ومسار غير مباشر يمر عبر رفع جاهزية الأمن السيبراني للكشف والاستجابة والتعافي (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤) (IAIS, 2023; NIST, 2024).

١,٢ خلفية الدراسة وسياقها:

١,٢,١ تطور قطاع التأمين السعودي:

يشهد قطاع التأمين في المملكة العربية السعودية توسعاً في الأقساط والخدمات وقنوات التوزيع الرقمية. ووفق تقرير سوق التأمين السعودي لعام ٢٠٢٥ بلغ إجمالي الأقساط المكتتبة ٨٤,٣ مليار ريال، بنمو ١٠,٧٪ مقارنة بعام ٢٠٢٤، كما تجاوز عدد المستفيدين من التأمين الصحي ١٤ مليوناً، ووصل عدد المركبات المؤمن عليها إلى ١١ مليون مركبة. وتعكس هذه المؤشرات اتساع حجم المعاملات والبيانات والعمليات اليومية التي تعتمد على بنية تقنية مترابطة ومزودين خارجيين متعددين (هيئة التأمين، ٢٠٢٦).

ولا يعني نمو القطاع زيادة الإيرادات فقط، بل يرفع كذلك كلفة التعطل المحتملة. فكلما اتسع عدد المستفيدين وتنوعت قنوات الخدمة زادت أهمية توافر الأنظمة، وسلامة البيانات، والقدرة على معالجة المطالبات دون انقطاع. كما أن الانتقال إلى إطار رقابي أكثر نضجاً، وإنشاء هيئة التأمين بوصفها الجهة المنظمة للقطاع، يفرضان على الشركات تطوير أطر الحوكمة الداخلية بما يتناسب مع طبيعة الاعتماد على مزودي الخدمات وتقنيات التأمين الحديثة.

١,٢,٢ التحول الرقمي والاعتماد على الأطراف الثالثة:

أصبح الطرف الثالث في شركة التأمين يؤدي وظائف قد تمس كل حلقة في سلسلة القيمة. فقد يدير المزود منصة الوثائق أو بوابة الدفع، وقد يحفظ البيانات في بنية سحابية، أو يقدم خدمة المطالبات، أو يربط الشركة بمقدمي الرعاية الصحية والورش والمقيمين. وهذه التبعيات تمنح الشركة سرعة في الوصول إلى القدرات المتخصصة، لكنها توسع سطح الهجوم السيبراني وتقلل الرؤية المباشرة على الضوابط التشغيلية لدى المزود، خصوصاً عندما يستخدم المزود بدوره مقاولين فرعيين أو منصات تقنية مشتركة.

لهذا وسّعت الأطر الحديثة مفهوم التعهيد التقليدي إلى مفهوم أشمل هو ترتيبات الأطراف الثالثة، بحيث يشمل كل علاقة تقدم خدمة أو نشاطاً أو عملية تدعم وظيفة حرجية، سواء عُدّت تعهيداً قانونياً أم لا. كما أبرزت الأطر مخاطر الأطراف اللاحقة وتركيز الاعتماد على مزود واحد أو منطقة جغرافية أو منصة سحابية مشتركة، وهو ما يجعل الحوكمة الفعالة عملية ممتدة طوال دورة حياة العلاقة. (FSB, 2023; BCBS, 2025)

١,٢,٣ السياق التنظيمي والسيبراني:

توفر البيئة السعودية مرتكزات مهمة للدراسة. فالدليل التنظيمي لأمن المعلومات في القطاع المالي يربط متطلبات الأمن بالمؤسسة وفروعها وموظفيها وأطرافها الثالثة وعملائها، ويخصص محوراً لتنظيم وتنفيذ ومراقبة متطلبات الأمن السيبراني مع مقدمي خدمات تقنية المعلومات والتعهد والحوسبة السحابية والموردين. كما تؤكد الضوابط الأساسية للأمن السيبراني ECC 2-2024 حماية الأصول المعلوماتية والتقنية، وتضم مكوناً مستقلاً للأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (البنك المركزي السعودي، ٢٠١٧؛ الهيئة الوطنية للأمن السيبراني، ٢٠٢٤).

وتؤكد تعليمات إسناد المهام إلى طرف ثالث مبادئ العناية الواجبة، وتحليل أثر الإسناد في سجل المخاطر، والاتفاقيات الشاملة، والمراقبة المستمرة، وخطط الطوارئ، والسجل المركزي، وحقوق الوصول والتدقيق. وعلى الرغم من أن بعض النصوص التنظيمية صيغت أصلاً لقطاعات مالية بعينها، فإن مبادئها تقدم مرجعية عملية قابلة للتكييف مع شركات التأمين ضمن اختصاص هيئة التأمين، وبما لا يتعارض مع اللوائح القطاعية السارية (البنك المركزي السعودي، ٢٠١٩؛ هيئة التأمين، ٢٠٢٦).

١,٣ مشكلة الدراسة:

تتمثل المشكلة في وجود فجوة محتملة بين سرعة توسع شركات التأمين في الاعتماد على الأطراف الثالثة وبين نضج الحوكمة القادرة على استيعاب المخاطر الناتجة عن ذلك الاعتماد. وقد تظهر الفجوة في عدم اكتمال سجل المزودين، أو تطبيق عناية واجبة موحدة لا تراعي حرجية الخدمة، أو ضعف بنود الإبلاغ عن الحوادث وحقوق التدقيق، أو اقتصار المتابعة على مؤشرات الأداء دون مؤشرات المخاطر، أو غياب خطط خروج قابلة للتنفيذ. وتزداد آثار الفجوة عندما يكون الطرف الثالث متصلاً بأنظمة المطالبات والبيانات الشخصية أو عندما يمثل نقطة اعتماد مشتركة لعدة خدمات حيوية.

لا يكفي أن تكون الشركة نفسها مجهزة تقنياً إذا كان المزود لا يطبق ضوابط مماثلة أو لا يشارك معلومات الحوادث في الوقت المناسب. كذلك لا تضمن العقود القوية وحدها المرونة إذا لم تتوافر لدى الشركة قدرات الكشف والاستجابة والتعافي والاختبار المشترك. ومن ثم تصبح جاهزية الأمن السيبراني آلية تفسيرية محتملة توضح كيف تتحول حوكمة الطرف الثالث إلى قدرة فعلية على استمرار الخدمات والتعافي من الاضطرابات.

وعلى الصعيد البحثي، تركز غالبية الدراسات العربية المتاحة على إدارة المخاطر العامة أو المخاطر التشغيلية أو الإفصاح السيبراني بصورة منفصلة، بينما تقل الدراسات الميدانية التي تدمج حوكمة مخاطر الطرف الثالث والجاهزية السيبرانية والمرونة التشغيلية في نموذج واحد داخل قطاع التأمين السعودي. وهذا النقص النظري والتطبيقي هو جوهر الفجوة التي تعالجها الدراسة.

السؤال الرئيس:

ما أثر حوكمة مخاطر الطرف الثالث في تعزيز المرونة التشغيلية لدى شركات التأمين في المملكة العربية السعودية، وما الدور الوسيط لجاهزية الأمن السيبراني في هذه العلاقة؟

١,٤ أسئلة الدراسة:

١. ما مستوى تطبيق حوكمة مخاطر الطرف الثالث لدى شركات التأمين في المملكة العربية السعودية؟
٢. ما مستوى جاهزية الأمن السيبراني لدى شركات التأمين محل الدراسة؟
٣. ما مستوى المرونة التشغيلية لدى شركات التأمين محل الدراسة؟
٤. ما أثر حوكمة مخاطر الطرف الثالث وأبعادها في المرونة التشغيلية؟
٥. ما أثر حوكمة مخاطر الطرف الثالث في جاهزية الأمن السيبراني؟
٦. ما أثر جاهزية الأمن السيبراني في المرونة التشغيلية؟
٧. هل تتوسط جاهزية الأمن السيبراني العلاقة بين حوكمة مخاطر الطرف الثالث والمرونة التشغيلية؟
٨. هل توجد فروق في استجابات أفراد العينة تُعزى إلى جهة العمل والإدارة والخبرة وحجم الشركة ومستوى التعامل مع الأطراف الخارجية؟

١,٥ أهداف الدراسة:

١. قياس مستوى تطبيق حوكمة مخاطر الطرف الثالث في شركات التأمين السعودية.
٢. قياس مستوى جاهزية الأمن السيبراني والمرونة التشغيلية في الشركات محل الدراسة.

٣. تحليل أثر العناية الواجبة، وحوكمة العقود، والرقابة المستمرة، وإدارة مخاطر البيانات والأمن، وخطط الطوارئ والخروج في المرونة التشغيلية.
٤. اختبار أثر حوكمة مخاطر الطرف الثالث في جاهزية الأمن السيبراني.
٥. اختبار أثر جاهزية الأمن السيبراني في المرونة التشغيلية.
٦. اختبار الدور الوسيط لجاهزية الأمن السيبراني في العلاقة بين الحوكمة والمرونة.
٧. فحص الفروق المرتبطة بالخصائص الوظيفية والتنظيمية للعينة.
٨. تقديم نموذج تطبيقي وخارطة تنفيذ تساعد شركات التأمين على رفع نضج إدارة مخاطر الأطراف الثالثة.

١,٦ أهمية الدراسة:

١,٦,١ الأهمية العلمية:

تنبع الأهمية العلمية من دمج ثلاثة مجالات غالبًا ما تدرس منفصلة: حوكمة مخاطر الطرف الثالث، وجاهزية الأمن السيبراني، والمرونة التشغيلية. ويتيح إدخال المتغير الوسيط تفسيرًا أعمق من العلاقة المباشرة؛ إذ يختبر ما إذا كانت الحوكمة تتحول إلى نتائج تشغيلية أفضل لأنها ترفع قدرة المؤسسة على الحماية والكشف والاستجابة والتعافي. كما تقدم الدراسة تشغيلًا قياسيًّا للأبعاد في بيئة التأمين السعودية، وتدعم الأدبيات العربية بمقياس يمكن التحقق من خصائصه السيكمومترية وتطويره في دراسات لاحقة.

١,٦,٢ الأهمية التطبيقية:

توفر الدراسة للإدارات العليا والمخاطر والالتزام والأمن السيبراني والمشتريات والمراجعة الداخلية إطارًا مشتركًا يربط قرارات التعاقد بخريطة الخدمات الحيوية وحدود تحمل الأثر. كما تساعد نتائجها في تحديد الأبعاد الأقل نضجًا وترتيب الاستثمار في السجل المركزي، والتقييمات الأمنية، ومؤشرات المخاطر، وخطط الخروج والتمارين المشتركة. وتفيد الجهة المنظمة في تصميم أدوات قياس نضج تتناسب مع حجم الشركة وحرية الخدمات ومخاطر التركيز القطاعي.

١,٦,٣ الأهمية التنظيمية والمجتمعية:

تمتد آثار المرونة التشغيلية إلى حماية حقوق حملة الوثائق والمستفيدين، لأن تعطل أنظمة التأمين قد يؤخر معالجة مطالبات صحية أو مالية أو يضعف الوصول إلى الخدمة. لذلك فإن الحوكمة الفعالة للأطراف الثالثة تسهم في حماية البيانات والثقة واستمرارية

التعويضات، وتدعم أهداف تطوير قطاع تأمين مستدام وموثوق ومتوافق مع رؤية السعودية ٢٠٣٠ (هيئة التأمين، ٢٠٢٦).

١,٧ مبررات اختيار الموضوع:

جدول (١-٠): مبررات اختيار موضوع الدراسة

المبرر	التوضيح
حادثة الموضوع	انتقال الرقابة عالميًا من التعهيد المحدود إلى منظومة شاملة لمخاطر الأطراف الثالثة والأطراف اللاحقة.
ملاءمته لتخصص إدارة المخاطر	يجمع التحديد والتقييم والمعالجة والمراقبة واستمرارية الأعمال في دورة واحدة.
حساسية قطاع التأمين	تتعامل شركات التأمين مع بيانات شخصية وصحية ومالية وخدمات مطالبات ذات أثر مباشر على العملاء.
التوسع الرقمي	زيادة الاعتماد على السحابة والمنصات والربط الإلكتروني ومقدمي الأمن والتحليلات.
القابلية للقياس	يمكن قياس الأبعاد من خلال العاملين في الإدارات ذات العلاقة واختبار الروابط إحصائيًا.
القيمة التنظيمية	يساعد النموذج المقترح في تحويل المتطلبات المتفرقة إلى إطار نضج قابل للتطبيق والرقابة.

المصدر: إعداد الباحث في ضوء مشكلة الدراسة وأهدافها.

١,٨ حدود الدراسة:

- **الحدود الموضوعية:** العلاقة بين حوكمة مخاطر الطرف الثالث، وجاهزية الأمن السيبراني، والمرونة التشغيلية، دون التوسع في مخاطر الاكتتاب والاستثمار والاحتياطيات إلا بقدر اتصالها باستمرارية التشغيل.

- **الحدود البشرية:** العاملون في المخاطر والالتزام وتقنية المعلومات والأمن السيبراني والعمليات والمطالبات والمراجعة الداخلية والقانونية والتعاقدات واستمرارية الأعمال.
- **الحدود المكانية:** شركات التأمين وإعادة التأمين والخدمات التأمينية ذات العلاقة العاملة في المملكة العربية السعودية.
- **الحدود الزمنية:** العام الجامعي ٢٠٢٦ م، مع استخدام أحدث المراجع التنظيمية المتاحة حتى تاريخ إعداد النسخة.
- **الحدود المنهجية:** تصميم مقطعي يعتمد الإدراك الوظيفي للمستجيبين؛ ومن ثم يفسر الارتباطات والآثار الإحصائية ضمن حدود التصميم غير التجريبي.

١,٩ مصطلحات الدراسة وتعريفاتها الإجرائية:

جدول (١-١): المتغيرات وأبعادها وتعريفاتها الإجرائية

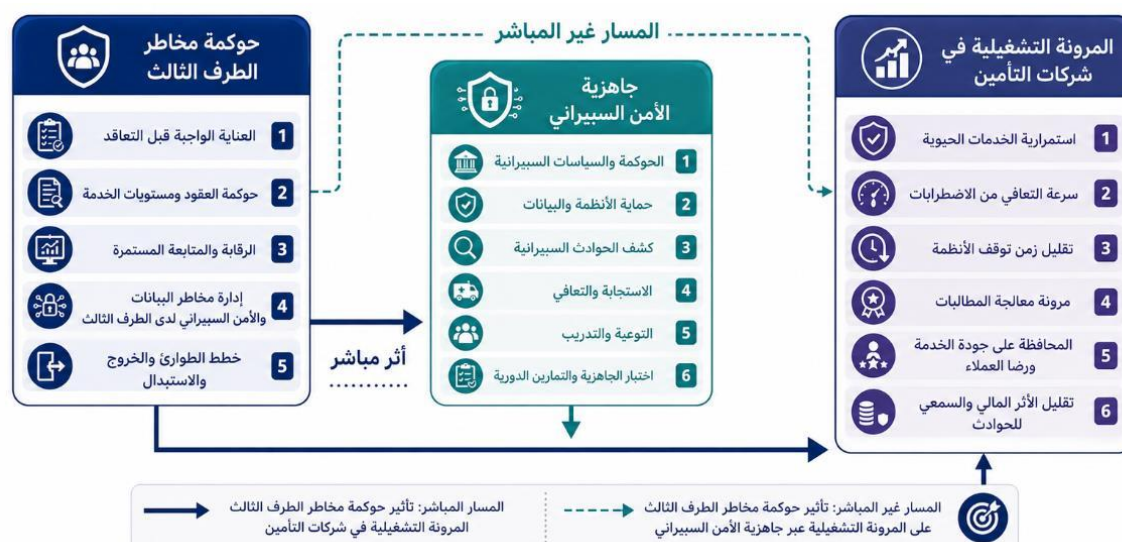
المصطلح	التعريف العلمي	التعريف الإجرائي في الدراسة
حوكمة مخاطر الطرف الثالث	منظومة السياسات والأدوار والعمليات التي تدير مخاطر العلاقات الخارجية طوال دورة حياتها.	الدرجة الكلية لاستجابات العينة عن العناية الواجبة، والعقود، والرقابة، ومخاطر البيانات والأمن، والطوارئ والخروج.
الطرف الثالث	كيان أو فرد يقدم للمؤسسة خدمة أو نشاطاً أو عملية بموجب ترتيب مباشر.	مقدمو التقنية والسحابة والمطالبات والاتصال والتحليلات والأمن والوساطة والخدمات المهنية المتصلة بعمليات شركة التأمين.
جاهزية الأمن السيبراني	قدرة تنظيمية وتقنية وبشرية على الحوكمة والحماية والكشف والاستجابة والتعافي والتعلم.	متوسط الاستجابات عن السياسات والحماية والكشف والحوادث والتدريب والاختبارات وإدارة الصلاحيات والبيانات.

المصطلح	التعريف العلمي	التعريف الإجرائي في الدراسة
المرونة التشغيلية	قدرة المؤسسة على تقديم الخدمات الحيوية ضمن حدود أثر مقبولة أثناء الاضطراب والتعافي والتكيف بعده.	متوسط الاستجابات عن الاستمرارية وسرعة التعافي وتقليل التوقف ومرونة المطالبات وجودة الخدمة وتقليل الأثر المالي والسمعي.
الخدمة الحيوية	خدمة يؤدي تعطيلها إلى ضرر مادي للعملاء أو التزامات المؤسسة أو سلامة السوق.	الخدمات التي تعدها شركة التأمين لازمة لاستمرار إصدار الوثائق أو خدمة العملاء أو معالجة المطالبات أو الوفاء بالمتطلبات النظامية.

المصدر: إعداد الباحث استنادًا إلى الأطر التنظيمية والمعيارية (البنك المركزي السعودي، ٢٠١٧؛ الهيئة الوطنية للأمن السيبراني، ٢٠٢٤). (FSB, 2023; BCBS, 2025).

١,١٠ متغيرات الدراسة والنموذج المفاهيمي:

يمثل حوكمة مخاطر الطرف الثالث المتغير المستقل، ويتكون من خمسة أبعاد: العناية الواجبة قبل التعاقد، وحوكمة العقود ومستويات الخدمة، والرقابة والمتابعة المستمرة، وإدارة مخاطر البيانات والأمن السيبراني لدى الطرف الثالث، وخطط الطوارئ والخروج والاستبدال. وتمثل جاهزية الأمن السيبراني المتغير الوسيط، في حين تمثل المرونة التشغيلية المتغير التابع. يفترض النموذج مسارًا مباشرًا من الحوكمة إلى المرونة، ومسارًا غير مباشر ينتقل عبر الجاهزية السيبرانية.



شكل (١-١): النموذج المفاهيمي المقترح للدراسة

المصدر: العرض المبدئي المرفق، مع مراجعة الباحث للمرجعيات التنظيمية (البنك المركزي السعودي، ٢٠١٧؛ الهيئة الوطنية للأمن السيبراني، ٢٠٢٤)، (FSB, 2023; BCBS, 2025).

١,١١ فرضيات الدراسة

جدول (٢-١): فرضيات الدراسة

الرمز	نص الفرضية
H1	يوجد أثر ذو دلالة إحصائية لحوكمة مخاطر الطرف الثالث في المرونة التشغيلية لدى شركات التأمين السعودية.
H1.1	يوجد أثر ذو دلالة إحصائية للعناية الواجبة قبل التعاقد في المرونة التشغيلية.
H1.2	يوجد أثر ذو دلالة إحصائية لحوكمة العقود ومستويات الخدمة في المرونة التشغيلية.
H1.3	يوجد أثر ذو دلالة إحصائية للرقابة والمتابعة المستمرة في المرونة التشغيلية.
H1.4	يوجد أثر ذو دلالة إحصائية لإدارة مخاطر البيانات والأمن السيبراني لدى الطرف الثالث في المرونة التشغيلية.

الرمز	نص الفرضية
H1.5	يوجد أثر ذو دلالة إحصائية لخطط الطوارئ والخروج والاستبدال في المرونة التشغيلية.
H2	يوجد أثر ذو دلالة إحصائية لحوكمة مخاطر الطرف الثالث في جاهزية الأمن السيبراني.
H3	يوجد أثر ذو دلالة إحصائية لجاهزية الأمن السيبراني في المرونة التشغيلية.
H4	تؤدي جاهزية الأمن السيبراني دوراً وسيطاً ذا دلالة إحصائية في العلاقة بين الحوكمة والمرونة.
H5	توجد فروق ذات دلالة إحصائية في استجابات العينة تُعزى إلى الخصائص الوظيفية والتنظيمية.

المصدر: إعداد الباحث في ضوء النموذج المفاهيمي.

١,١٢ هيكل الرسالة:

- الفصل الأول: الإطار العام للدراسة، ويتناول الخلفية والمشكلة والأسئلة والأهداف والأهمية والحدود والمصطلحات والنموذج والفرضيات.
- الفصل الثاني: الإطار النظري والدراسات السابقة، ويعرض الأسس النظرية والمتغيرات والسياق التنظيمي والفجوة البحثية.
- الفصل الثالث: منهجية الدراسة، ويتضمن التصميم والمجتمع والعينة والأداة والصدق والثبات والإجراءات الأخلاقية والأساليب الإحصائية.
- الفصل الرابع: عرض النتائج وتحليلها ومناقشتها، ويشمل الخصائص الوصفية واختبار القياس والفرضيات والوساطة والفروق.
- الفصل الخامس: الخاتمة والاستنتاجات والتوصيات والنموذج التطبيقي ومقترحات البحوث المستقبلية.

١,١٣ خلاصة الفصل :

حدد الفصل الأول منطلقات الدراسة ومشكلتها المتمثلة في الحاجة إلى حوكمة متكاملة للاعتماد الخارجي داخل قطاع تأميني سريع النمو والتحول الرقمي. وصيغت الأسئلة والأهداف والفرضيات ضمن نموذج يربط الحوكمة بالمرونة مباشرة وعبر جاهزية الأمن السيبراني. ويبيئ ذلك للانتقال إلى الفصل الثاني الذي يبني الأساس النظري ويحلل الأدلة السابقة والمرجعيات التنظيمية التي تدعم العلاقات المقترحة.

الفصل الثاني : الإطار النظري والدراسات السابقة

حوكمة الطرف الثالث، الجاهزية السيبرانية، المرونة التشغيلية، والفجوة البحثية



٢,١ مقدمة الفصل:

يبني هذا الفصل الأساس النظري للعلاقات التي تختبرها الدراسة. ويبدأ بالمنطلقات المفسرة، ثم يعرض مفهوم حوكمة مخاطر الطرف الثالث ودورة حياتها وأبعادها ومخاطرها في بيئة التأمين. وبعد ذلك يناقش جاهزية الأمن السيبراني بوصفها قدرة مؤسسية وسيطة، ويحلل المرونة التشغيلية بوصفها نتيجة تتجاوز استمرارية الأعمال التقليدية. ويتناول الفصل كذلك البيئة التنظيمية السعودية والمعايير الدولية، ثم يستعرض الدراسات السابقة العربية والأجنبية بصورة نقدية لاستخلاص الفجوة البحثية.

وتقوم الفكرة المركزية على أن الطرف الثالث لا يصبح مصدرًا للمرونة أو للخطر بذاته؛ بل تتحدد النتيجة بحسب جودة الحوكمة التي تضبط العلاقة، ومدى دمج الأمن السيبراني في القرارات، وقدرة الشركة على رؤية التبعيات واختبارها والتعامل معها. لذلك لا تُفهم الحوكمة بوصفها وثائق ثابتة، وإنما بوصفها مجموعة قدرات متكررة لاستشعار المخاطر، وتقييمها، وصياغة شروط ملزمة، ومراقبة السلوك، وإعادة التهيئة عند تغير التهديد أو الخدمة.

٢,٢ المنطلقات النظرية للدراسة:

٢,٢,١ نظرية الاعتماد على الموارد:

تفترض نظرية الاعتماد على الموارد أن المنظمة لا تملك جميع الموارد والقدرات اللازمة لإنجاز أهدافها، فتدخل في علاقات مع جهات خارجية للحصول على المعرفة والتقنية والمرونة والاقتصاد في الحجم. غير أن الحصول على المورد يخلق اعتمادًا، وقد يتحول الاعتماد إلى مصدر قوة للطرف المزود عندما تكون البدائل محدودة أو تكاليف الانتقال مرتفعة أو تكون الخدمة شديدة التخصص. وفي شركات التأمين يتجسد ذلك في الاعتماد على منصة مطالبات أو مزود سحابي أو شبكة طبية أو محرك تسعير يصعب استبداله في وقت قصير. تفسر النظرية لماذا لا ينبغي تقييم مزود الخدمة من منظور السعر والجودة فقط. فقرار الإنسان يعيد توزيع السيطرة على موارد وعمليات حيوية، ويخلق مخاطر تركّز ومعلومات غير متماثلة. وتعمل الحوكمة على تخفيف اختلال القوة من خلال تنويع البدائل، وحقوق التدقيق، وشفافية سلسلة التوريد، ونقل المعرفة، وخطط الخروج، والاحتفاظ بقدرة داخلية كافية للإشراف. وبذلك ترتبط العناية الواجبة وحوكمة العقود وخطط الاستبدال مباشرة بخفض هشاشة الاعتماد.

٢,٢,٢ نظرية القدرات الديناميكية:

توضح نظرية القدرات الديناميكية أن التفوق في البيئات المتغيرة لا يعتمد على امتلاك الموارد فقط، بل على قدرة المنظمة على استشعار التحولات، واغتنام الفرص، وإعادة تشكيل الموارد والعمليات. ويمكن تطبيق المنطق على إدارة الأطراف الثالثة؛ فالسجل المحدث والتقييم المستمر يساعدان في استشعار المخاطر، والقرارات التعاقدية والضوابط تمثل اغتنامًا منظمًا، بينما تجسد خطط الخروج وتحويل الخدمة وإعادة توزيعها القدرة على إعادة التهيئة.

وتنسجم النظرية مع تصور المرونة كقدرة عليا تشمل الاستباق والمواجهة والتكيف. فقد قدم (Duchek, 2020) نموذجًا يرى المرونة قدرة مركبة تتكون من التوقع والتعامل والتكيف؛ وهي مراحل يمكن موازاتها مع تقييم الطرف الثالث قبل التعاقد، وإدارة الحادث أثناء التشغيل، والتعلم وإعادة التصميم بعد الاضطراب. ومن ثم فإن حوكمة الطرف الثالث ليست إجراء امتثال، بل قدرة ديناميكية ترفع قابلية الشركة للتكيف مع فشل المزود أو تغير بيئة التهديد.

٢,٢,٣ إدارة مخاطر المؤسسة والحوكمة المتكاملة:

يربط إطار إدارة مخاطر المؤسسة بين المخاطر والاستراتيجية والأداء، ويؤكد أن قرارات الأعمال يجب أن تُتخذ ضمن شهية مخاطر واضحة ومعلومات متكاملة. وتبعًا لذلك ينبغي أن تكون استراتيجية استخدام الأطراف الثالثة مرتبطة بالخدمات الحيوية والأهداف ومستويات المخاطر المقبولة، وأن تتوزع المسؤوليات بين مجلس الإدارة والإدارة التنفيذية ومالكي الخدمات ووظائف الرقابة. كما يجب أن تدخل مخاطر المزود في سجل المخاطر المؤسسي، لا أن تبقى ضمن ملفات المشتريات أو تقنية المعلومات فقط (COSO, 2017; ISO, 2018).

يوفر نموذج خطوط الدفاع تفسيرًا عمليًا: يملك خط الأعمال العلاقة والمخاطر اليومية؛ وتضع وظائف المخاطر والالتزام والأمن المعايير وتراقب الالتزام؛ وتقدم المراجعة الداخلية تأكيدًا مستقلًا على كفاية التصميم والفاعلية. وتفشل الحوكمة عندما تتشتت البيانات بين هذه الوظائف أو لا يوجد مالك واضح للمخاطر أو تعتمد قرارات التجديد على الأداء التجاري وحده.

٢,٢,٤ المنظور الاجتماعي-التقني:

الأمن السيبراني والمرونة التشغيلية ناتجان عن تفاعل الإنسان والإجراء والتقنية والعلاقة التعاقدية. فقد تكون الضوابط التقنية متقدمة، لكن ضعف الإبلاغ أو غموض المسؤولية يطيل زمن اكتشاف الحادث. وقد يكون العقد شاملاً، لكن عدم اختبار النسخ الاحتياطية أو صلاحيات الوصول يجعل الضمانات نظرية. لذلك تتطلب الجاهزية مزيجاً من الحوكمة والمهارات والثقافة والتقنية والتمارين، وهو ما يبرر دورها الوسيط بين تصميم الحوكمة والنتيجة التشغيلية.

٢,٣ حوكمة مخاطر الطرف الثالث:

٢,٣,١ المفهوم والنطاق:

تشير حوكمة مخاطر الطرف الثالث إلى النظام الذي يحدد كيف تختار المؤسسة الأطراف الخارجية، وكيف تقيم المخاطر، ومن يملك قرار القبول، وما المتطلبات التي تُدرج في العقود، وكيف تُراقب الخدمة، ومتى وكيف تنتهي العلاقة. ويشمل المفهوم العلاقات المباشرة، وقد يمتد إلى الأطراف اللاحقة التي يعتمد عليها المزود لتقديم الخدمة. ويختلف بذلك عن إدارة الموردين التقليدية التي تركز غالباً على السعر والتسليم والجودة؛ إذ يضيف منظور الحوكمة المخاطر السيبرانية والقانونية والتنظيمية والمالية والسمعية والاستمرارية والتركيز.

ويرى مجلس الاستقرار المالي أن إدارة مخاطر الطرف الثالث عملية قائمة على المخاطر تمتد طوال دورة حياة العلاقة وتُعنى بتحديد الخدمات الحرجة والتبعيات النظامية. كما تؤكد مبادئ بازل النهائية لعام ٢٠٢٥ التناسب والحرجية والتركيز والأطراف اللاحقة، وتربط جودة الإدارة بالقدرة على الصمود والتكيف والتعافي من الاضطراب. (FSB, 2023; BCBS, 2025) ورغم أن مبادئ بازل موجهة للبنوك، فإن منطقتها قابل للاستفادة في التأمين مع مراعاة الإطار القطاعي.

٢,٣,٢ دورة حياة العلاقة مع الطرف الثالث:

تبدأ الحوكمة قبل اختيار المزود بتحديد الحاجة، وتحليل البدائل، وبيان ما إذا كانت الخدمة حيوية وما البيانات التي ستعالجها. ثم تجري العناية الواجبة على المزود المختار، ويصاغ العقد بحسب مستوى المخاطر، ويخضع المزود لتهيئة آمنة قبل التشغيل. بعد ذلك تبدأ المراقبة المستمرة التي تجمع الأداء والمخاطر والحوادث والتغيرات، وتنتهي الدورة بإنهاء

مخطط أو طارئ ونقل البيانات والخدمة. والدورة ليست خطية تمامًا؛ فقد تدفع واقعة أثناء التشغيل إلى إعادة التقييم أو تعديل العقد أو رفع التصنيف.

جدول (١-٢): دورة حياة إدارة مخاطر الطرف الثالث

المرحلة	الأسئلة الحاكمة	المخرجات الرئيسية
التخطيط والتصنيف	ما الخدمة؟ ما حرجيتها؟ ما حدود الأثر؟ ما البدائل والتركيز؟	تصنيف الحرجية، مالك الخدمة، شهية المخاطر، متطلبات التقييم.
العناية الواجبة	هل يملك المزود قدرة مالية وفنية وسيبرانية وقانونية مناسبة؟	تقرير عناية واجبة، فجوات، مخاطر متبقية، قرار قبول/رفض.
التعاقد	هل حُوت المتطلبات إلى التزامات قابلة للقياس والإنفاذ؟	SLA، KRI، حقوق تدقيق، إخطار الحوادث، استمرارية خروج.
التهيئة والتشغيل	هل الوصول والربط والبيانات مضبوط؟ وهل اختُبرت الخدمة؟	إعداد آمن، قبول تشغيلي، سجل صلاحيات، خطوط اتصال. وتصعيد.
المراقبة المستمرة	هل تغير الأداء أو الخطر أو سلسلة التوريد؟	لوحات مؤشرات، تقييمات دورية، إجراءات تصحيح، تقارير الإدارة.
الإنهاء والخروج	كيف تُنقل الخدمة والبيانات دون تجاوز حدود الأثر؟	خطة انتقال، حذف/إرجاع بيانات، إلغاء صلاحيات، تعلم بعد التنفيذ.

المصدر: إعداد الباحث بالاستناد إلى (البنك المركزي السعودي، ٢٠١٩) (FSB, 2023; BCBS, 2025)

٢,٣,٣ مخاطر الأطراف الثالثة في شركات التأمين:

تتعدد المخاطر لأن الطرف الثالث قد يؤثر في سرية البيانات وتوافر النظام ودقة القرار وجودة الخدمة والامتثال في آن واحد. ويُعد الخطر التشغيلي أوسعها؛ إذ يشمل فشل العملية أو النظام أو الأشخاص أو الحدث الخارجي. وقد يؤدي توقف مزود منصة المطالبات إلى تراكم الطلبات، بينما يقود خطأ مقدم تحليل أو خدمة اكتوارية إلى قرارات غير دقيقة. كما قد تنشأ مخاطر قانونية من اختلاف مكان تخزين البيانات أو غموض مسؤولية المقاول الفرعي. أما الخطر السيبراني فينشأ عندما يوفر الربط أو حسابات الدعم أو واجهات البرمجة مسارًا غير مباشر إلى أنظمة الشركة وبياناتها. ولا يتوقف الخطر عند الاختراق؛ بل يشمل ضعف إدارة الثغرات، وتأخر الإخطار، وعدم كفاية سجلات الأحداث، وعدم إمكانية تنسيق الاستجابة. وتظهر مخاطر التركيز عندما تعتمد عدة خدمات داخل الشركة أو عدة شركات في القطاع على المزود نفسه أو على منصة سحابية مشتركة، ما يجعل حدثًا واحدًا قادرًا على إحداث أثر واسع (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤). (BCBS, 2025).

جدول (٢-٢): تصنيف مخاطر الأطراف الثالثة في شركات التأمين

نوع الخطر	مثال في قطاع التأمين	أثر محتمل	ضابط حاكم
تشغيلي	تعطل نظام المطالبات أو مركز الاتصال	تأخر التسوية وتراكم الطلبات والشكاوى	SLA، سعة بديلة، اختبار تعافٍ، مراقبة لحظية
سيبراني	اختراق حساب دعم لمزود تقني	وصول غير مصرح وتسرب بيانات وتعطل خدمة	أقل صلاحية، MFA، سجلات، إخطار واختبار استجابة
خصوصية وبيانات	معالجة بيانات صحية لدى مقاول فرعي	انتهاك السرية والتزامات نظامية وسمعية	تصنيف بيانات، تحديد الموقع، تشفير، حذف موثق

نوع الخطر	مثال في قطاع التأمين	أثر محتمل	ضابط حاكم
التزام وقانوني	عقد لا يمنح حقوق التدقيق أو الوصول	تعذر التحقق الرقابي أو معالجة المخالفات	بنود واضحة وحقوق وصول وتدقيق وإنهاء
مالي	تعثر المزود أو ارتفاع مفاجئ في تكاليف الخدمة	توقف أو تكلفة انتقال مرتفعة	تقييم مالي، ضمانات، تسعير وخيارات انتقال
تركيز	اعتماد خدمات متعددة على مزود سحابي واحد	نقطة فشل مشتركة وامتداد الأثر	تحليل تركّز، تنوع هندسة متعددة المناطق/المزودين
سمعة	سوء تعامل مركز خدمة خارجي مع العملاء	فقد الثقة وانتشار الشكاوى	معايير سلوك، رقابة جودة، تدريب وتصعيد
طرف لاحق	استخدام المزود مقاوئاً فرعياً غير معلن	مخاطر غير مرئية وضعف السيطرة	إفصاح وموافقة وسريان الالتزامات على السلسلة

المصدر: إعداد الباحث في ضوء (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤) (FSB, 2023; IAIS, 2023; BCBS, 2025).

٢,٣,٤ البعد الأول: العناية الواجبة قبل التعاقد:

العناية الواجبة هي عملية التحقق المنهجي من أهلية المزود قبل منح الاعتماد أو الوصول. ويحدد مستوى عمقها بناء على حرجية الخدمة ونوع البيانات والربط والتبعية. وتشمل الملاءة المالية والخبرة والقدرة التشغيلية والسمعة والالتزام والتأمينات المهنية والموقع الجغرافي والأمن السيبراني واستمرارية الأعمال وسلسلة التوريد. ولا تكفي الشهادات وحدها؛ إذ ينبغي التحقق من نطاقها وحداثها واستثناءاتها، وطلب أدلة تشغيلية مثل نتائج الاختبارات وتقارير التدقيق وخطط معالجة الملاحظات.

تقلل العناية الواجبة من الاختيار المعاكس والمفاجآت بعد التعاقد. لكنها تفقد قيمتها إذا كانت قائمة تحقق واحدة لجميع الموردين أو إذا لم يُربط التقييم بقرار قبول مخاطر واضح. لذلك يجب توثيق المخاطر المتبقية، والمالك الذي قبلها، وشروط القبول، وتاريخ إعادة التقييم. وفي الخدمات الحرجة يُستحسن إجراء زيارة أو مراجعة مستقلة واختبار سيناريو واقعي قبل الإطلاق.

٢,٣,٥ البعد الثاني: حوكمة العقود ومستويات الخدمة:

يحول العقد نتائج التقييم إلى التزامات قابلة للقياس. وينبغي أن يحدد نطاق الخدمة، والمسؤوليات، ومؤشرات الأداء والمخاطر، ومستويات التوافر، وأهداف التعافي، ومتطلبات النسخ الاحتياطي، وملكية البيانات وموقعها، والتشفير، وإدارة الوصول، والإبلاغ عن الحوادث، وحقوق التدقيق والوصول التنظيمي، وضوابط التعاقد الفرعي، واستمرارية الأعمال، والمساعدة عند الخروج.

ومن الأخطاء الشائعة قياس التوافر كنسبة شهرية دون ربطه بفترات الأعمال الحرجة أو أثر الانقطاع على العميل. فقد يحقق المزود نسبة توافر مرتفعة بينما يقع الانقطاع في وقت حرج لمعالجة المطالبات. لذلك يجب أن تربط المؤشرات بالخدمة الحيوية وحدود تحمل الأثر، وأن تتضمن إنذارًا مبكرًا لا جزاءات بعد وقوع الضرر فقط. كما ينبغي أن يوضح العقد ترتيب الأولويات عندما يخدم المزود عدة عملاء أثناء أزمة واسعة.

٢,٣,٦ البعد الثالث: الرقابة والمتابعة المستمرة:

تتغير مخاطر المزود بعد التعاقد بسبب التحديثات والاستحوادات وتبدل فرق العمل والثغرات والتعاقدات الفرعية والضغوط المالية. لذلك تُعد المراقبة المستمرة جوهر الحوكمة. وتشمل جمع مؤشرات الأداء والمخاطر، ومراجعة الحوادث والمشكلات، وتتبع نتائج التدقيق، وتحديث التقييم، ومراقبة الأخبار المالية والتهديدات، وتوثيق إجراءات التصحيح والتصعيد.

تتميز الرقابة الناضجة بأنها متدرجة بحسب المخاطر، وتنتج رؤية مجمعة للإدارة العليا بدل تقارير منفصلة لكل عقد. ويجب أن تجيب اللوحة عن أسئلة مثل: ما الخدمات الحرجة المعرضة لخطر مرتفع؟ ما المزودون الذين تجاوزوا حدود المخاطر؟ أين توجد ملاحظات متأخرة؟ ما حجم التركيز؟ وما خطط المعالجة؟ ويتيح هذا المنظور الانتقال من متابعة الامتثال إلى اتخاذ القرار الاستباقي.

٢,٣,٧ البعد الرابع: مخاطر البيانات والأمن السيبراني لدى الطرف الثالث:

يبدأ هذا البعد بتحديد البيانات والأصول التي يصل إليها المزود، ثم تطبيق مبدأ أقل صلاحية، وفصل البيئات، والمصادقة متعددة العوامل، والتشفير، وإدارة المفاتيح، وسجلات الأحداث، وإدارة الثغرات والتحديثات. كما يتطلب تحديد زمن إخطار الحوادث ومحتوى الإخطار وآلية حفظ الأدلة والتنسيق في الاستجابة. وتؤكد الضوابط السعودية أن متطلبات الأمن السيبراني للأطراف الخارجية يجب تحديدها وتوثيقها وتنفيذها ومراقبتها، وأن الاعتماد السحابي يحتاج ضوابط مكملة تراعي نموذج المسؤولية المشتركة (البنك المركزي السعودي، ٢٠١٧؛ الهيئة الوطنية للأمن السيبراني، ٢٠٢٤).

تكتسب سلسلة التوريد البرمجية أهمية خاصة؛ فقد يدخل الخطر عبر مكون أو مكتبة أو تحديث موثوق ظاهريًا. ولذلك يوصي NIST بتأسيس استراتيجية لإدارة مخاطر سلسلة التوريد السيبرانية، وتصنيف الموردين، وإبلاغ المتطلبات، والتحقق من الأداء طوال دورة الحياة. (NIST, 2024) وفي شركة التأمين ينبغي ربط التقييم السيبراني بخرائط البيانات والخدمات وليس بالمزود ككيان مجرد.

٢,٣,٨ البعد الخامس: خطط الطوارئ والخروج والاستبدال:

تضمن خطة الخروج ألا تتحول العلاقة الناجحة اليوم إلى قيد يمنع الشركة من الاستجابة غداً. وتشمل سيناريوهات الإنهاء المخطط، والتعثر المفاجئ، والحادث السيبراني، والإخلال التنظيمي، وارتفاع المخاطر إلى مستوى غير مقبول. ويجب أن تحدد الخطة بدائل المزود، وإمكانية نقل البيانات، وتوافق الصيغ، والموارد الداخلية، والوقت والتكلفة، وترتيب تشغيل مزدوج عند الحاجة، ومسؤولية المزود عن المساعدة الانتقالية.

لا تعد الخطة قابلة للتنفيذ لمجرد وجود وثيقة. ينبغي اختبار عناصرها، والتحقق من قدرة البديل، وتقدير المدة مقابل حدود تحمل الأثر. وقد يكون الخروج الكامل غير عملي في الحوسبة السحابية أو الأنظمة الأساسية؛ عندئذ تصبح هندسة القابلية للنقل والنسخ الاحتياطي المستقل واستمرار الوصول إلى البيانات أكثر أهمية من مجرد تسمية مزود بديل.

خلاصة حوكمة الطرف الثالث:

الحوكمة الفعالة تتبع منطق: اعرف الخدمة والتبعية، صنف الحرجية، افحص المزود، حوّل المتطلبات إلى عقد، راقب التغير، اختبر الاستجابة، واستعد للخروج. أي حلقة ضعيفة قد تجعل بقية الحلقات شكلية.

٢,٤ جاهزية الأمن السيبراني:

٢,٤,١ المفهوم ومكونات الجاهزية:

جاهزية الأمن السيبراني هي قدرة المؤسسة على منع الحوادث المحتملة وخفض احتمالها، واكتشافها مبكرًا، والاستجابة لها، واستعادة الخدمات والبيانات، والتعلم منها. وهي أوسع من امتلاك أدوات حماية؛ لأنها تشمل الحوكمة والسياسات والأدوار والموارد والوعي والمراقبة والاختبار والعلاقات الخارجية. ويضيف إطار NIST CSF 2.0 وظيفة «الحوكمة» إلى الوظائف المعروفة، ويربط الأمن باستراتيجية إدارة المخاطر ويخصص فئة لإدارة مخاطر سلسلة التوريد السيبرانية. (NIST, 2024)

وفي السياق السعودي، توفر ضوابط ECC 2-2024 حدًا أدنى من المتطلبات ضمن أربعة مكونات: حوكمة الأمن السيبراني، وتعزيزه، وصموده، والأمن المتعلق بالأطراف الخارجية والحوسبة السحابية. وتدعم هذه البنية النظر إلى الجاهزية كمتغير مركب يجمع الوقاية والكشف والتعافي والإدارة الخارجية (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤).

٢,٤,٢ الحوكمة والسياسات السيبرانية:

تحدد الحوكمة الجهة المسؤولة عن المخاطر، ودور مجلس الإدارة، وشهية المخاطر، وسياسات الاستثناء، ومتطلبات التقارير. ويجب أن تُدمج مخاطر الأطراف الثالثة في استراتيجية الأمن، وأن تكون المسؤولية النهائية لدى الشركة حتى عند إسناد التنفيذ. كما ينبغي أن ترتبط قرارات القبول والتجديد بنتائج التقييم السيبراني وأن تخضع الاستثناءات لتفويض زمني وخطة معالجة.

٢,٤,٣ الحماية وإدارة الهوية والبيانات:

تشمل الحماية إدارة الأصول والتكوينات والهوية والصلاحيات والتشفير والنسخ الاحتياطي وأمن الشبكات والتطبيقات. وعند التعامل مع طرف ثالث يجب تحديد الحسابات البشرية والخدمات، وإلغاء غير المستخدم، ومراقبة الامتيازات، وفصل بيانات الإنتاج والاختبار، وتقييد تصدير البيانات. كما يجب أن تتبع البيانات دورة حياة واضحة من الجمع إلى الإتلاف، مع إثبات الإرجاع أو الحذف عند إنهاء العقد.

٢,٤,٤ الكشف والاستجابة والتعافي:

تعتمد سرعة الاستجابة على رؤية موحدة للأحداث وقدرة المزود على مشاركة سجلات ومعلومات كافية. وينبغي تحديد من يعلن الحادث، وكيف يصنف، ومتى تُخطر الإدارة والجهة المنظمة والمعلماء، وكيف تحفظ الأدلة. وتُقاس الجاهزية بمؤشرات مثل متوسط

زمن الاكتشاف والاحتواء والاستعادة، ونسبة السيناريوهات المختبرة، ونسبة نقاط الضعف المتأخرة، لا بعدد الأدوات فقط.

أما التعافي فيتطلب نسخًا قابلة للاستعادة، وأهداف RTO و RPO واقعية، وقدرة على تشغيل بدائل أو إجراءات يدوية، واختبارات تشمل المزود. ويكشف الاختبار المشترك فجوات الاتصال والتبعيات الخفية التي لا تظهر في مراجعة الوثائق. وقد أكدت أطر المرونة أن الخطط الداخلية غير كافية إذا لم تشمل مقدمي الخدمات الحرجة (IAIS, 2023; BCBS, 2021).

٢,٤,٥ الوعي والتدريب والاختبار:

يبقى الإنسان عنصرًا حاسمًا لأن مالكي العلاقات والمشتريات والعمليات قد يتخذون قرارات تؤثر في الأمن قبل وصول العقد إلى فريق الأمن. لذلك يجب تدريبهم على تصنيف البيانات، وطلبات الوصول، ومؤشرات الإنذار، والإبلاغ عن الحوادث، وتجنب تجاوز التقييم بسبب ضغط الوقت. كما ينبغي تنفيذ تمارين مكتبية وتقنية ومحاكاة فقد مزود، وتوثيق الدروس وتحويلها إلى تحسينات قابلة للمتابعة.

٢,٥ المرونة التشغيلية:

٢,٥,١ مفهوم المرونة التشغيلية:

المرونة التشغيلية هي قدرة المؤسسة على تحديد خدماتها الأكثر أهمية، ورسم الموارد والتبعيات التي تدعمها، ووضع حدود للأثر الذي يمكن تحمله، ثم الاستعداد لمنع الاضطراب والاستجابة له والتعافي والتكيف. يختلف هذا المفهوم عن مجرد استعادة نظام؛ فقد يعمل النظام بينما تتعطل الخدمة بسبب نقص بيانات أو مورد أو طرف ثالث. كما يركز على النتيجة التي تهم العميل والسوق، وليس على سلامة المكونات منفردة (IAIS, 2023; BCBS, 2021).

تتضمن المرونة ثلاثة أزمنة مترابطة: قبل الاضطراب من خلال الاستشعار والوقاية والاستعداد؛ أثناءه من خلال الاحتواء واستمرار الحد الأدنى للخدمة والاتصال؛ وبعده من خلال التعافي والتحليل والتعلم وإعادة التصميم. ويعكس ذلك نموذج (Duchek 2020) في التوقع والمواجهة والتكيف، ويؤكد أن العودة إلى الوضع السابق ليست الهدف الوحيد؛ فقد يتطلب التعلم إزالة اعتماد أو تغيير عقد أو إعادة بناء عملية.

٢,٥,٢ الفرق بين المرونة واستمرارية الأعمال:

جدول (٢-٣): مقارنة بين استمرارية الأعمال والمرونة التشغيلية

وجه المقارنة	استمرارية الأعمال	المرونة التشغيلية
وحدة التركيز	العملية أو الموقع أو النظام	الخدمة الحيوية والنتيجة المقدمة للعميل
نقطة البداية	تحليل أثر الأعمال وخطط الاستمرارية	الخدمات المهمة وحدود تحمل الأثر وخرائط التبعية
النطاق	خطط الاستجابة والتعافي	الوقاية والاستجابة والتعافي والتكيف والحوكمة
الأطراف الثالثة	قد تُذكر ضمن الخطة	جزء أصيل من خريطة الخدمة والاختبار والحدود
القياس	وقدرة الاستعادة RPO و RTO	الأثر على العميل، مدة/حجم التعطل، جودة الخدمة، التعلم
المنظور	التعافي من سيناريوهات محددة	القدرة على تحمل طيف واسع من الاضطرابات الشديدة والمعقولة

المصدر: إعداد الباحث استنادًا إلى (ISO, 2019; BCBS, 2021; IAIS, 2023).

٢,٥,٣ الخدمات الحيوية وحدود تحمل الأثر:

تبدأ المرونة بتحديد الخدمة التي يترتب على تعطلها ضرر غير مقبول للمستفيدين أو التزامات الشركة أو سلامة السوق. وفي التأمين قد تشمل تلقي المطالبات الصحية، وتسوية المطالبات الكبيرة، وإصدار وثائق إلزامية، وخدمة قنوات التواصل الأساسية. وبعد تحديد الخدمة يوضع حد تحمل أثر يعبر عن أقصى مدة أو حجم أو ضرر يمكن قبوله، مع مراعاة الفئات المتأثرة والالتزامات النظامية.

تسمح الحدود بتقييم كفاية ترتيبات الطرف الثالث بطريقة عملية. فإذا كان حد تحمل تعطل المطالبات أربع ساعات بينما يحتاج نقل الخدمة إلى المزود البديل يومين، فإن خطة

الخروج غير ملائمة حتى لو كانت موثقة. وبذلك تربط الحدود بين المخاطر والاستثمار والاختبار وتمنع الاكتفاء بمؤشرات عامة لا تعكس تجربة العميل.

٢,٥,٤ رسم خرائط التبعيات:

ترسم الشركة الأشخاص والعمليات والتقنيات والبيانات والمواقع والأطراف التي تدعم كل خدمة حيوية. ويكشف الرسم نقاط الفشل المشتركة والاعتماد على أطراف لاحقة وازدواج المورد ظاهرياً مع اعتماد المزودين على منصة واحدة. وينبغي تحديث الخريطة عند تغيير النطاق أو التعاقد أو البنية، وربطها بالسجل المركزي للأطراف الثالثة وبسجل الأصول والبيانات.

٢,٥,٥ أبعاد المرونة التشغيلية في الدراسة:

- (١) استمرارية الخدمات الحيوية: المحافظة على الحد الأدنى المقبول من الخدمة أثناء تعطل مزود أو نظام.
- (٢) سرعة التعافي: إعادة الأداء إلى المستوى المستهدف خلال زمن يتوافق مع حدود تحمل الأثر.
- (٣) تقليل زمن توقف الأنظمة: منع امتداد العطل وتوفير البدائل والنسخ والمراقبة.
- (٤) مرونة معالجة المطالبات: الحفاظ على استقبال المطالبات وفرزها واتخاذ القرار والتواصل والتسوية.
- (٥) المحافظة على جودة الخدمة ورضا العملاء: إدارة الاتصال والشفافية والأولويات خلال الأزمة.
- (٦) تقليل الأثر المالي والسمعي: احتواء الخسائر والغرامات والشكاوى والمحافظة على الثقة.

٢,٦ تفسير العلاقات بين متغيرات الدراسة

٢,٦,١ الحوكمة والمرونة التشغيلية:

تؤثر الحوكمة في المرونة من خلال خفض احتمال اختيار مزود غير ملائم، ورفع وضوح المسؤوليات، وإتاحة إنذار مبكر، وتحسين القدرة على التصعيد والانتقال. فالعناية الواجبة تمنع إدخال هشاشة غير مقبولة، والعقود تجعل التوقعات قابلة للإنفاذ، والمراقبة تكشف

التدهور، وخطط الخروج تمنح خيارات عند الفشل. ولذلك يُتوقع أن تسهم الأبعاد الخمسة في استمرار الخدمة وتقليل زمن التعافي والأثر.

تدعم الأدبيات هذا المنطق؛ فقد أظهرت أبحاث سلاسل التوريد السيبرانية أن الرؤية والتعاون والتقييم والمراقبة ترتبط بأداء أمني أفضل، وأن الهجمات قد تنتقل عبر روابط الموردين إلى الشركات. (Boyson, 2014; Gani et al., 2023; Crosignani et al., 2023) كما تضع الأطر الرقابية إدارة الطرف الثالث ضمن متطلبات المرونة التشغيلية (FSB, 2023; BCBS, 2025).

٢,٦,٢ الحوكمة وجاهزية الأمن السيبراني:

تفرض الحوكمة تحديد متطلبات الأمن قبل التعاقد، وتقويم المزود، وضبط الوصول، ومراقبة الثغرات والحوادث، واختبار الاستجابة. لذلك يُتوقع أن تزيد جودة الحوكمة من اكتمال السياسات والرؤية على الأحداث وسرعة التنسيق. وقد بينت الدراسات النوعية أن تقييم مخاطر الموردين ينضج عندما تتكامل الوظائف وتتوفر معلومات موثوقة وآليات متابعة مستمرة. (Slapnicar et al., 2025)

٢,٦,٣ الجاهزية السيبرانية والمرونة التشغيلية:

يسمح الكشف المبكر والاحتواء والنسخ والتعافي والتدريب بتقليل مدة الانقطاع واتساعه. كما أن الجاهزية تحد من تحول حدث لدى مزود إلى أزمة مؤسسية، لأنها توفر قنوات إخطار وأدوارًا وبيانات قرار وتمارين سابقة. ومن هنا يتوقع أثر موجب للجاهزية في المرونة، خصوصًا في الخدمات التأمينية الرقمية التي تتطلب توافر البيانات والأنظمة والاتصال.

٢,٦,٤ منطق الوساطة:

لا تنتج المرونة من وثيقة تقييم أو عقد وحده؛ بل من تحويل هذه المدخلات إلى قدرة تشغيلية على الحماية والكشف والاستجابة والتعافي. لذلك تقترح الدراسة وساطة جزئية: يحتفظ للحوكمة بأثر مباشر من خلال بدائل الخدمة والرقابة والعقود، وفي الوقت نفسه ينتقل جزء من الأثر عبر رفع الجاهزية السيبرانية. وتعني الوساطة الجزئية أن تحسين الأمن مهم، لكنه لا يغني عن الجوانب المالية والتشغيلية والقانونية وخطط الخروج.

شكل (٢-١): منطق انتقال أثر الحوكمة إلى المرونة التشغيلية

مدخلات الحوكمة	القدرة الوسيطة	النتيجة التشغيلية
+ عناية واجبة + عقد رقابة + بيانات + خروج	حوكمة وحماية وكشف واستجابة وتعافٍ واختبار	استمرار الخدمة + تعافٍ أسرع + أثر أقل + تكيف

المصدر: إعداد الباحث في ضوء النموذج النظري للدراسة.

٢,٧ السياق التنظيمي والمعياري

تعتمد الدراسة على مصادر عربية تنظيمية أولاً ثم على معايير وأطر أجنبية مكملية. ولا يُفهم الاستناد إلى أطر مصرفية أو دولية على أنه إحلال محل تنظيم قطاع التأمين السعودي؛ بل بوصفها ممارسات مرجعية تساعد في تفسير أبعاد الحوكمة والمرونة، على أن تكون لوائح وتعليمات هيئة التأمين والأنظمة السعودية هي المرجع النظامي الواجب التطبيق.

جدول (٢-٤): المرجعيات التنظيمية والمعيارية للدراسة

المرجعية	السنة	التركيز	صلة الدراسة
هيئة التأمين - تقرير سوق التأمين السعودي 2025	2026	حجم القطاع ونموه ومؤشرات الأداء	تحديد السياق التطبيقي واتساع أثر استمرارية الخدمة
الهيئة الوطنية للأمن ECC 2- - السيبراني 2024	2024	الحوكمة والحماية والصمود والأطراف الخارجية والسحابة	بناء أبعاد جاهزية الأمن ومخاطر الطرف الثالث
الهيئة الوطنية للأمن CCC 2- - السيبراني 2024	2024	متطلبات الأمن للحوسبة السحابية	تقييم مزودي السحابة والمسؤولية المشتركة

المرجعية	السنة	التركيز	صلة الدراسة
البنك المركزي السعودي - الدليل التنظيمي للأمن السيبراني	2017	متطلبات المؤسسات المالية والأطراف الثالثة	ربط الأمن بالحوكمة والرقابة والتعاقد
البنك المركزي السعودي - تعليمات الإسناد لطرف ثالث	2019	العناية الواجبة والعقود والرقابة والطوارئ والسجل	تشغيل أبعاد المتغير المستقل
نظام حماية البيانات الشخصية ولائحته التنفيذية	2021/2 023	معالجة البيانات وحقوق أصحابها والتزامات الجهات	ضبط معالجة ونقل وحذف بيانات المستفيدين
FSB Toolkit	2023	دورة الحياة والخدمات الدرجة والتبعيات النظامية	الإطار الشامل لإدارة الطرف الثالث
IAIS Issues Paper	2023	المرونة التشغيلية في قطاع التأمين	تخصيص مفهوم المرونة لقطاع الدراسة
NIST CSF 2.0	2024	الحوكمة وإدارة مخاطر سلسلة التوريد السيبرانية	بناء الجاهزية السيبرانية
BCBS Third-Party Risk Principles	2025	التناسب والجرية والتركيز والأطراف اللاحقة ودورة الحياة	تعزيز نموذج الحوكمة والمرونة

المرجعية	السنة	التركيز	صلة الدراسة
ISO 31000 / ISO 22301 / ISO 27001	2018/2019/2022	المخاطر والاستمرارية وأمن المعلومات	مرجعيات الإدارة والقياس والتكامل
DORA - Regulation (EU) 2022/2554	2022	المرونة الرقمية وإدارة مخاطر مزودي تقنية المعلومات	مقارنة دولية لرقابة مقدمي الخدمات الحرجة

المصدر: إعداد الباحث من الوثائق الرسمية المشار إليها.

٢,٨ الدراسات السابقة

٢,٨,١ الدراسات العربية:

دراسة بوداود (٢٠٢١):

هدفت دراسة بوداود إلى معرفة دور إدارة المخاطر في تحسين أداء شركات التأمين، واعتمدت منهج دراسة الحالة وتحليل عملية تحديد المخاطر وتقييمها ومعالجتها ومراقبتها. وخلصت إلى أن إدارة المخاطر المنظمة تساعد شركات التأمين على التنبؤ بالمخاطر والحد من آثار البيئة المتقلبة. تفيد الدراسة الحالية في تأكيد الصلة العامة بين إدارة المخاطر والأداء، لكنها لم تفصل مخاطر الأطراف الثالثة أو تختبر الجاهزية السيبرانية أو المرونة التشغيلية كمتغيرات مستقلة (بوداود، ٢٠٢١).

دراسة طرطاق (٢٠١٩):

تناولت طرطاق التوجهات الاستراتيجية لإدارة المخاطر التشغيلية في شركات التأمين في ضوء متطلبات الملاءة الثانية، واعتمدت تحليلاً نظرياً للمتطلبات والممارسات، وأبرزت ضرورة إدماج المخاطر التشغيلية في الحوكمة والرقابة بدل التعامل معها كخسائر عرضية. تستفيد الدراسة الحالية من التركيز القطاعي على التأمين والمخاطر التشغيلية، وتختلف عنها بإدخال الطرف الثالث والأمن السيبراني والاختبار الميداني للوساطة (طرطاق، ٢٠١٩).

دراسة يعقوب ووهّاب والفرطوسي (٢٠٢٢):

بنت الدراسة مؤشراً للإفصاح عن المخاطر السيبرانية وفق متطلبات دولية، وطبقته على شركات مدرجة في سوق العراق للأوراق المالية. اشتمل المؤشر على حوكمة الأمن والحماية

والاستراتيجية وإدارة المخاطر، وأظهرت النتائج تباين مستوى الإفصاح بين الشركات. تفيد الدراسة في تحديد مكونات الحوكمة السيبرانية، لكنها تقيس الإفصاح الخارجي لا الجاهزية الفعلية ولا مخاطر الموردين (يعقوب وآخرون، ٢٠٢٢).

دراسة حشمان وحدي (٢٠٢٤)

بحثت الدراسة المخاطر السيبرانية في الصناعة المالية الإسلامية من خلال تحليل طبيعة التهديدات والممارسات المستخدمة في المواجهة. وأكدت أهمية الحوكمة والتوعية والتقنيات والالتزام بالمعايير في حماية الثقة واستمرارية الأنشطة. تتقاطع مع الدراسة الحالية في البيئة المالية والجاهزية، لكنها أوسع قطاعياً ولم تختبر مساراً وسيطاً نحو المرونة التشغيلية (حشمان وحدي، ٢٠٢٤).

دراسة أحمد (٢٠٢٢)

تناولت دراسة أثر إدارة المخاطر على الجوانب الفنية في التأمينات العامة، واعتمدت دراسة ميدانية في شركات تأمين سودانية، وخلصت إلى أهمية وجود إدارة مخاطر مستقلة ودعمها بالكوادر والصلاحيات. وتدعم الدراسة فكرة أن النضج المؤسسي للمخاطر ينعكس على العمليات الفنية، لكنها لم تعالج الاعتماد التقني الخارجي أو المرونة السيبرانية (أحمد، ٢٠٢٢).

جدول (٥-٢): ملخص الدراسات العربية السابقة

الدراسة	المنهج/المجال	أبرز النتيجة	الفائدة والاختلاف
بوداود (2021)	- دراسة حالة شركات التأمين	الإدارة المنظمة للمخاطر تحسن القدرة على الأداء والتنبؤ.	تدعم العلاقة العامة؛ لا تختبر الطرف الثالث أو الوساطة.
طرطاق (2019)	- تحليل نظري المخاطر التشغيلية والتأمين	الحاجة إلى توجه استراتيجي وحوكمة للمخاطر التشغيلية.	تدعم المتغير التابع؛ لا تتناول الجاهزية السيبرانية.

الدراسة	المنهج/المجال	أبرز النتيجة	الفائدة والاختلاف
يعقوب وآخرون (2022)	مؤشر واختبار إفصاح - سوق مالي	تباين الإفصاح عن الحوكمة والحماية والمخاطر السيبرانية	تفيد في الأبعاد؛ تقيس الإفصاح لا الجاهزية التشغيلية
حشمان وحدي (2024)	- تحليل وصفي الصناعة المالية الإسلامية	تكامل الحوكمة والتوعية والتقنية. ضروري للمواجهة	تدعم الوسيط؛ لا تختبر المرونة أو الطرف الثالث.
أحمد (2022)	- دراسة ميدانية التأمينات العامة	استقلال إدارة المخاطر ودعمها يرفع الأداء الفني	تدعم القيمة القطاعية؛ لا تتناول التبعيات الخارجية.

المصدر: إعداد الباحث من الدراسات المشار إليها.

٢,٨,٢ الدراسات الأجنبية:

Boyson (2014)

طور منظورًا لإدارة المخاطر السيبرانية في سلاسل التوريد التقنية، وأكد أن الرؤية على الموردين والمعايير المشتركة والتعاون ضرورية للسيطرة على الأنظمة الحرجة. أسهم في تأصيل مخاطر الموردين السيبرانية، لكنه لم يختبر قطاع التأمين أو الوساطة.

Colicchia et al. (2019)

استخدمت دراسة استكشافية لفهم إدارة مخاطر المعلومات والأمن في سلاسل التوريد، ووجدت أن التكامل والتعاون والحوكمة عبر الحدود التنظيمية ضرورية، مع صعوبة قياس الأطراف الممتدة. تدعم بعد الرقابة وسلسلة التوريد.

Duchek (2020)

قدمت بناءً مفاهيميًا للمرونة التنظيمية كقدرة عليا تتكون من التوقع والمواجهة والتكيف. توفر أساسًا لتفسير كيف تحول الشركة ممارسات الحوكمة إلى استعداد واستجابة وتعلم، لكنها دراسة مفاهيمية عامة.

Hillmann & Guenther (2021)

قدمت مراجعة منهجية لبناء المرونة التنظيمية وناقشت إشكالات التعريف والقياس. أكدت ضرورة التمييز بين المرونة والصلابة والرشاقة، واستفادت الدراسة الحالية منها في تحديد المتغير التابع بصورة متعددة الأبعاد.

Benaroch (2021)

حللت الحوادث السيبرانية الناجمة عن أطراف ثالثة وناقشت انتقال الأثر إلى المؤسسة العميلة. دعمت أهمية النظر إلى الحادث بوصفه تبعية شبكية، إلا أن تركيزها لم يكن على برنامج الحوكمة الكامل.

Creazza et al. (2022)

استكشفت تصورات مديري سلاسل التوريد بشأن مكونات إدارة المخاطر السيبرانية في عصر التحول الرقمي، وأظهرت أهمية التكامل بين الوظائف والوعي والرؤية. تدعم الأبعاد البشرية والتنظيمية للجاهزية.

Gani et al. (2023)

اختبرت التفاعل بين ممارسات إدارة مخاطر سلسلة التوريد السيبرانية والأداء السيبراني، ووجدت روابط موجبة بين الممارسات المنظمة والنتائج الأمنية. تدعم مسار الحوكمة إلى الجاهزية.

Crosignani et al. (2023)

استخدمت بيانات واسعة لتحليل انتشار الهجمات عبر سلاسل الشركات، وأظهرت أن الروابط التجارية تنقل أثر الهجمات إلى شركاء آخرين. توفر دليلاً على أن الاعتماد الخارجي مسار حقيقي لانتشار الخطر.

Slapnicar et al. (2025)

اعتمدت منهجاً مختلطاً شمل ٣٣ مقابلة و٥٣ استبانة لخبراء أمن، وطورت نظرية عملية لتقييم المخاطر السيبرانية للموردين. أظهرت أن النضج يتأثر بالسياق والمعلومات والمراقبة، وأن العملية قادرة على تمييز الموردين مرتفعي المخاطر.

جدول (٦-٢): ملخص الدراسات الأجنبية السابقة

الدراسة	نوعها/عينتها	الإسهام الرئيس	صلة الدراسة الحالية
Boyson (2014)	إطار تطبيقي لسلسلة التوريد السيبرانية	الحاجة إلى رؤية ومعايير مشتركة وتحكم استراتيجي.	تأصيل مخاطر الموردين التقنية.
Colicchia et al. (2019)	تحليل استكشافي لسلاسل التوريد	الحوكمة والتعاون مطلوبان لإدارة مخاطر المعلومات.	دعم الرقابة وسلسلة الأطراف.
Duchek (2020)	دراسة مفاهيمية	+ المرونة = توقع + مواجهة + تكيف.	تأسيس المتغير التابع.
Hillmann & Guenther (2021)	مراجعة منهجية	الحاجة إلى وضوح البناء والقياس متعدد الأبعاد.	تحسين التشغيل القياسي للمرونة.
Benaroch (2021)	تحليل حوادث طرف ثالث	الطرف الثالث قناة لانتقال الأثر السيبراني.	دعم مشكلة الدراسة.
Creazza et al. (2022)	دراسة نوعية لمديري السلاسل	التكامل والوعي والرؤية عناصر حاكمة.	دعم الجاهزية والحوكمة.
Gani et al. (2023)	دراسة كمية	ممارسات السلسلة السيبرانية تحسن الأداء الأمني.	دعم مسار H2.
Crosignani et al. (2023)	بيانات شركات وهجمات	انتشار الهجمات عبر الروابط التجارية.	دعم أثر التبعيات.

الدراسة	نوعها/عينتها	الإسهام الرئيس	صلة الدراسة الحالية
Slapnicar et al. (2025)	مختلط: 33 مقابلة و 53 استبانة	نظرية عملية لتقييم مخاطر الموردين ونضج المراقبة	أقرب الدراسات للمتغير المستقل

المصدر: إعداد الباحث من الدراسات المشار إليها.

٢,٨,٣ التعقيب على الدراسات السابقة:

تتفق الدراسات على أن إدارة المخاطر المنظمة، وتكامل الحوكمة والأمن، والرؤية على التبعيات، والقدرة على الاستجابة عوامل تؤثر في الأداء والمرونة. كما يظهر اتجاه حديث من التركيز على المورد المباشر إلى سلسلة الأطراف والتركيز والاعتماد النظامي. وتدعم الأدلة التجريبية انتقال الحوادث عبر العلاقات التجارية، وتبين الدراسات المختلطة أن جودة تقييم الموردين تعتمد على العملية والسياق، لا على الاستبيان الأمني وحده.

ومع ذلك تتوزع الأدبيات على مسارات منفصلة: دراسات التأمين العربية تركز على المخاطر العامة أو الملاءة والأداء؛ ودراسات الأمن تركز على الإفصاح أو التهديدات؛ ودراسات الطرف الثالث الأجنبية غالباً ما تركز على سلاسل التوريد أو البنوك والتقنية. وتظل هناك حاجة إلى نموذج ميداني يجمع الحوكمة والجاهزية والمرونة داخل قطاع التأمين السعودي، ويختبر الآلية الوسيطة بدل الاكتفاء بوصف الممارسات.

٢,٩ الفجوة البحثية وإسهام الدراسة

جدول (٧-٢): الفجوة البحثية واستجابة الدراسة الحالية

نوع الفجوة	ما يظهر في الأدبيات	استجابة الدراسة الحالية
موضوعية	ندرة الجمع بين حوكمة الطرف الثالث والمرونة التشغيلية والجاهزية السيبرانية	نموذج واحد بثلاثة متغيرات ومسارين مباشر وغير مباشر.
قطاعية	غلبة البنوك وسلاسل التوريد العامة والدراسات النظرية	تطبيق مخصص لشركات التأمين السعودية وخدماتها الحيوية.

نوع الفجوة	ما يظهر في الأدبيات	استجابة الدراسة الحالية
جغرافية	قلة الأدلة الميدانية العربية والسعودية.	قياس آراء وظائف المخاطر والتقنية والعمليات داخل المملكة.
منهجية	وصف متطلبات أو دراسات حالة دون اختبار وساطة.	Bootstrap تحليل انحدار ومسارات و للوساطة.
قياسية	تباين تعريفات المرونة والاعتماد على مؤشرات عامة.	أبعاد تشغيلية ترتبط باستمرار الخدمة والتعافي والمطالبات والأثر.
تطبيقية	فصل الأمن عن العقود والخروج والرقابة.	نموذج حوكمة وخارطة تنفيذ متكاملة KPI/KRI ومؤشرات

المصدر: إعداد الباحث بناء على المراجعة النقدية للدراسات السابقة.

٢,١٠ خلاصة الفصل:

أوضح الفصل أن الاعتماد على الأطراف الثالثة يوفر موارد وقدرات، لكنه يخلق تبعيات تحتاج حوكمة قائمة على المخاطر طوال دورة الحياة. وبين أن الجاهزية السيبرانية قدرة اجتماعية-تقنية تشمل الحوكمة والحماية والكشف والاستجابة والتعافي والاختبار، وأن المرونة التشغيلية تركز على استمرار الخدمات الحيوية ضمن حدود أثر مقبولة. وتدعم النظريات والأطر والدراسات توقع علاقات موجبة بين المتغيرات ووساطة جزئية للجاهزية. وفي ضوء الفجوة المستخلصة، يعرض الفصل الثالث التصميم المنهجي اللازم لاختبار النموذج.

الفصل الثالث : منهجية الدراسة وإجراءاتها

التصميم، المجتمع والعينة، الأداة، الصدق والثبات، الأخلاقيات والتحليل



٣,١ مقدمة الفصل:

يصف هذا الفصل الإجراءات التي تحول النموذج النظري إلى اختبار منظم قابل للتكرار. ويعرض فلسفة الدراسة وتصميمها، ومجتمع الدراسة وعينتها، وبناء أداة القياس، وإجراءات الصدق والثبات، وخطة جمع البيانات، والاعتبارات الأخلاقية، وأساليب التحليل الإحصائي. وقد روعي الاتساق بين سؤال الدراسة الرئيس والفرضيات والمتغيرات والأساليب المستخدمة، مع تجنب تفسير العلاقات المقطعية بوصفها سببية قطعية.

٣,٢ منهج الدراسة وتصميمها:

اعتمدت الدراسة المنهج الوصفي التحليلي بتصميم كمي مقطعي. فالجانب الوصفي يقيس مستويات حوكمة مخاطر الطرف الثالث وجاهزية الأمن السيبراني والمرونة التشغيلية، والجانب التحليلي يختبر العلاقات والتأثيرات والوساطة والفروق. ويعد التصميم ملائمًا لأن المتغيرات تمثل ممارسات وقدرات تنظيمية يمكن قياسها من خلال تقديرات العاملين ذوي الصلة، ولأن الهدف هو تفسير التباين بين الشركات والإدارات لا التدخل التجريبي.

وتبنى الدراسة توجهاً استدلالياً يبدأ من النظريات والأطر السابقة ويشترك فرضيات قابلة للاختبار. ويستخدم مستوى دلالة ($\alpha = 0.05$)، مع عرض حجم الأثر وفترات الثقة إلى جانب الدلالة؛ لأن القيمة العملية للعلاقة لا تختزل في قيمة p . كما تُفسر النتائج ضمن حدود العينة والتصميم وكون البيانات ذاتية التقرير.

٣,٣ مجتمع الدراسة:

يتكون المجتمع المستهدف من العاملين في شركات التأمين وإعادة التأمين وشركات الخدمات التأمينية ذات الصلة العاملة في المملكة العربية السعودية، ممن ترتبط أعمالهم بإدارة المخاطر أو العلاقات الخارجية أو استمرارية الخدمات. ويشمل ذلك إدارات المخاطر والالتزام وتقنية المعلومات والأمن السيبراني والعمليات والمطالبات والمراجعة الداخلية والشؤون القانونية والتعاقدات والجودة واستمرارية الأعمال.

اختير هذا المجتمع لأن المستجيب المطلع ينبغي أن يفهم أحد جوانب دورة حياة الطرف الثالث أو آثارها. واستُبعدت الوظائف التي لا تمتلك معرفة عملية بالعلاقات الخارجية أو المخاطر التشغيلية، حتى لا تتحول الاستجابات إلى انطباعات عامة. ومن الأفضل ميدانياً مخاطبة من أمضى مدة كافية في الشركة أو شارك في تقييم أو تعاقد أو مراقبة أو حادث أو تمرين استمرارية.

٣,٤ عينة الدراسة وطريقة اختيارها:

تستخدم الدراسة عينة قصدية طبقية وظيفيًا، بحيث تستهدف الوظائف الأكثر معرفة بالموضوع مع مراعاة تمثيل أنواع الجهات وأحجامها. ويمثل التوزيع عبر وظائف المخاطر والتقنية والعمليات آلية لتحسين تنوع الرؤية وتقليل هيمنة وظيفة واحدة. ويعد حجم (٢١٤) استجابة صالحة كافيًا لاختبارات الانحدار والوساطة في النموذج الحالي؛ إذ يتجاوز القواعد الإرشادية المتعلقة بعدد المشاهدات لكل متنبئ، ويمنح قدرة مناسبة لاكتشاف آثار متوسطة عند مستوى دلالة ٠,٠٥.

في التطبيق الفعلي، ينبغي توثيق عدد الروابط المرسل، والاستجابات المستلمة، والاستجابات المستبعدة وأسباب الاستبعاد، ونسبة الاستجابة. أما هذه النسخة التحليلية فتستخدم (٢١٤) حالة محاكاة بعد فحص منطقي للاكتمال واتساق الإجابة، ولا تدعي نسبة استجابة ميدانية فعلية.

٣,٥ مصادر البيانات:

٣,٥,١ البيانات الثانوية:

شملت البيانات الثانوية الأنظمة واللوائح والأدلة الصادرة عن هيئة التأمين والبنك المركزي السعودي والهيئة الوطنية للأمن السيبراني والجهات المختصة بحماية البيانات، إضافة إلى المعايير الدولية والأوراق الرقابية والمقالات المحكمة. واستُخدمت المصادر التنظيمية العربية أولاً لبناء السياق المحلي، ثم المصادر الأجنبية لتوسيع المقارنة وتأسيس المفاهيم.

٣,٥,٢ البيانات الأولية:

الأداة الرئيسة هي استبانة إلكترونية موجهة إلى أفراد المجتمع المستهدف. وتستخدم مقياس ليكرت الخماسي: (١) لا أوافق بشدة، (٢) لا أوافق، (٣) محايد، (٤) أوافق، (٥) أوافق بشدة. ويتيح المقياس تكوين درجات مركبة للأبعاد والمتغيرات مع المحافظة على سهولة الإجابة والمقارنة.

٣,٦ بناء أداة الدراسة:

طُورت فقرات الأداة من النموذج الوارد في العرض المبدئي، ثم روجعت في ضوء الضوابط السعودية وأطر FSB وBCBS وNIST وIAIS. تتكون الأداة من قسم للبيانات العامة وثلاثة

محاور قياس تحتوي ٣٠ فقرة. وحرصت الصياغة على أن تقيس كل عبارة ممارسة واحدة قابلة للملاحظة، وأن تتجنب المصطلحات التقنية غير الضرورية والأسئلة المزدوجة.

جدول (١-٣): توزيع فقرات الاستبانة

المحور	الأبعاد/الموضوعات	عدد الفقرات	الترميز
البيانات العامة	جهة العمل، الإدارة، الخبرة، حجم الشركة، مستوى التعامل مع الأطراف	5	D1-D5
حوكمة مخاطر الطرف الثالث	العناية الواجبة، العقود، الرقابة، البيانات والأمن، الطوارئ والخروج	10	TP1-TP10
جاهزية الأمن السيبراني	الحوكمة، التقييم، المتطلبات، الكشف، الاستجابة، التدريب، الاختبار، الوصول والبيانات	10	CR1-CR10
المرونة التشغيلية	الاستمرارية، التعافي، التوقف، النقل، الخدمات الحيوية، الاختبار، الجودة والأثر	10	OR1-OR10

المصدر: إعداد الباحث.

٣,٧ التعريفات القياسية وترميز الدرجات:

تُحسب الدرجة الكلية لكل متغير بمتوسط فقراته بعد التأكد من عدم وجود فقرات عكسية غير معالجة. وتُحسب أبعاد حوكمة الطرف الثالث بمتوسط كل زوج من الفقرات المرتبط بالبعد. أما محاور الجاهزية والمرونة فيعرض على مستوى المتغير والموضوعات الفرعية؛ لأن بعض الموضوعات ممثلة بفقرة واحدة في الصيغة المختصرة للأداة، وهو قيد ينبغي تحسينه مستقبلاً بإضافة ثلاث فقرات على الأقل لكل بعد عند بناء نموذج قياس كامن مستقل.

جدول (٣-٢): معايير تفسير المتوسطات الحسابية

مدى المتوسط	مستوى التقدير
1.00 - 1.80	منخفض جدًا
1.81 - 2.60	منخفض
2.61 - 3.40	متوسط
3.41 - 4.20	مرتفع
4.21 - 5.00	مرتفع جدًا

المصدر: إعداد الباحث بناء على تقسيم مدى مقياس ليكرت إلى خمس فئات متساوية.

٣,٨ صدق الأداة:

٣,٨,١ الصدق الظاهري وصدق المحتوى:

يقترح عرض الأداة على ما لا يقل عن خمسة محكمين من تخصصات إدارة المخاطر والتأمين والأمن السيبراني والإحصاء. ويقيم المحكمون ملاءمة الفقرة للبعد، ووضوحها، وعدم تكرارها، وحساسيتها للبيئة السعودية. ويمكن حساب نسبة اتفاق المحكمين ومؤشر صدق المحتوى، وتعديل أو حذف الفقرات التي لا تحقق حدًا مقبولًا. ويجب الاحتفاظ بنموذج يبين الملاحظات والإجراء المتخذ لضمان شفافية التطوير.

٣,٨,٢ صدق البناء:

يُفحص صدق البناء من خلال الارتباطات بين الفقرات ودرجات محاورها، وملاءمة مصفوفة البيانات للتحليل العاملي. وفي النموذج التطبيقي بلغت قيمة (KMO 0.932)، وهي قيمة مرتفعة، وكان اختبار Bartlett دالًا إحصائيًا ($\chi^2 = 2715.77$ ، $df = 435$ ، $p < 0.001$)، ما يشير إلى أن الارتباطات ليست مصفوفة هوية وأن البيانات ملائمة للتحليل العاملي. كما تُراجع التحميلات والتقاطعات قبل اعتماد البنية.

٣,٩ ثبات الأداة:

يُقاس الاتساق الداخلي بمعامل كرونباخ ألفا، وتعد القيم التي تبلغ ٠,٧٠ فأكثر مقبولة للدراسات التطبيقية، مع مراعاة عدد الفقرات وتنوع البناء. وفي النموذج التحليلي بلغت ألفا

لمحور حوكمة الطرف الثالث (٠,٨٠٦)، ولجاهزية الأمن السيبراني (٠,٩٠٣)، وللمرونة التشغيلية (٠,٨٨١)، وهي قيم مقبولة إلى مرتفعة. ولا يعني ارتفاع ألفا وحده صدق البناء؛ لذلك عُرضت معه مؤشرات الصدق والارتباطات.

٣,١٠ الدراسة الاستطلاعية:

تطبيق الأداة على ٢٠-٣٠ مشاركاً من خصائص مشابهة للمجتمع دون إدراجهم في العينة النهائية. ويُطلب منهم بيان العبارات الغامضة والوقت اللازم للإجابة، ثم تفحص التوزيعات والاتساق الداخلي والبيانات المفقودة. وتهدف الدراسة الاستطلاعية إلى تحسين الأداة والإجراء، لا إلى اختبار الفرضيات مبكراً.

٣,١١ إجراءات جمع البيانات:

١. الحصول على الموافقة الأكاديمية والأخلاقية وخطابات تسهيل المهمة عند الحاجة.
٢. تحديد نقاط اتصال في الشركات والإدارات المستهدفة دون طلب قوائم بيانات شخصية غير ضرورية.
٣. إرسال رابط الاستبانة مرفقاً بمعلومات الدراسة والموافقة الطوعية والمدة المتوقعة.
٤. منع جمع الاسم أو رقم الهوية أو اسم الشركة إذا لم تكن هناك ضرورة بحثية، وتفعيل إجابة واحدة عند الإمكان دون تتبع غير لازم.
٥. إرسال تذكير محدود وغير ضاغط، ثم إغلاق الأداة في التاريخ المحدد.
٦. تنزيل البيانات في ملف مشفر، وفصل أي بيانات اتصال -إن وجدت- عن الإجابات.
٧. فحص الاكتمال والأنماط غير المنطقية وزمن الإجابة والتكرار وفق قواعد استبعاد مسبقة.
٨. توثيق سجل التنظيف والتحويل والترميز قبل بدء التحليل الاستدلالي.

٣,١٢ معالجة البيانات المفقودة والقيم المتطرفة:

يُفحص نمط القيم المفقودة قبل المعالجة. فإذا كانت النسبة محدودة وعشوائية يمكن استخدام متوسط البعد بشرط إجابة المشارك عن غالبية فقراته؛ أما الاستجابة التي تفتقد نسبة كبيرة فستُستبعد. وتراجع القيم المتطرفة أحادية ومتعددة المتغيرات، لكن لا تُحذف

تلقائيًا إذا كانت تمثل حالة حقيقية. كما تفحص الاستجابات المستقيمة التي تختار الخيار نفسه لجميع الفقرات، وزمن الإجابة غير المعقول، والتناقضات الواضحة.

٣,١٣ التحيز المنهجي المشترك:

لأن المتغيرات تقاس من المصدر نفسه وفي الوقت نفسه، اتخذت معالجات إجرائية مثل التأكيد على السرية، وفصل أقسام الاستبانة، وتبسيط العبارات، وعدم الإيحاء بوجود إجابة مرغوبة. وإحصائيًا، أظهر اختبار العامل الواحد أن العامل الأول يفسر (٣٥,٦٪) من التباين، وهي نسبة دون ٥٠٪، ما يقلل -ولا يلغي- القلق من أن مصدرًا واحدًا يفسر معظم التباين. ويمكن في الدراسة الفعلية إضافة متغير علامة أو جمع مؤشرات موضوعية من الشركة لرفع قوة الاستدلال.

٣,١٤ أساليب التحليل الإحصائي:

جدول (٣-٣): إجراءات التحليل الإحصائي

الإجراء	الغرض	معايير القرار/المخرجات
التكرارات والنسب	وصف الخصائص الديموغرافية والتنظيمية	العدد والنسبة المئوية
المتوسط والانحراف المعياري	تحديد مستوى المتغيرات والفقرات	فئات التفسير الخمس
كرونباخ ألفا	قياس الاتساق الداخلي	$\alpha \geq 0.70$ مقبول
KMO و Bartlett	اختبار ملائمة البيانات للتحليل العاملي	$KMO \geq 0.60$ و $p < 0.05$
ارتباط بيرسون	قوة واتجاه العلاقة بين المتغيرات	r والدلالة وفترة الثقة
الانحدار البسيط	H1 و H2 و H3 اختبار	β, t, p, R^2
الانحدار المتعدد	اختبار الآثار النسبية لأبعاد الحوكمة	β المعياري، R^2 ، VIF المعدل

الإجراء	الفرض	معياري القرار/المخرجات
الوساطة وBootstrap	والأثر غير المباشر H4 اختبار	عينه؛ فترة ثقة لا تشمل 5,000 الصفر
t/ANOVA	اختبار الفروق بين الفئات	وحجم الأثر $p < 0.05$
فحص الافتراضات	سلامة الاستدلال	الخطية، البواقي، تجانس التباين، عدم التعدد الخطي

المصدر: إعداد الباحث بالاستفادة من (Field (2018) و(Hayes (2022).

٣,١٥ نموذج اختبار الوساطة:

يختبر نموذج الوساطة ثلاثة مسارات: المسار (a) من حوكمة الطرف الثالث إلى جاهزية الأمن السيبراني؛ والمسار (b) من الجاهزية إلى المرونة مع ضبط الحوكمة؛ والمسار المباشر (c') من الحوكمة إلى المرونة مع وجود الوسيط. ويحسب الأثر غير المباشر بضرب $(a \times b)$ ، ويُعتمد إذا لم تشمل فترة الثقة المولدة من ٥,٠٠٠ عينة Bootstrap قيمة الصفر. كما يُعرض الأثر الكلي (c) ونسبة الوساطة دون اعتبارها بديلاً عن التفسير النظري (Hayes, 2022).

٣,١٦ الاعتبارات الأخلاقية:

- ❖ المشاركة طوعية، ويحق للمشارك التوقف قبل الإرسال دون أي أثر وظيفي.
- ❖ توضح صفحة المقدمة هدف الدراسة والمدة والاستخدام المتوقع للبيانات ووسيلة التواصل الأكاديمية.
- ❖ لا تُجمع أسرار تجارية أو تفاصيل حوادث قابلة للتعرف على شركة أو عميل أو مزود بعينه.
- ❖ تعرض النتائج مجمعة، ولا تستخدم الاقتباسات أو الفئات الصغيرة بطريقة تكشف الهوية.
- ❖ تُحفظ البيانات في مكان آمن ومقيد الوصول، وتُتلف وفق المدة المعتمدة من الجامعة.

❖ يُفصح عن استخدام البيانات المحاكاة في هذه المسودة، ويُمنع تمثيلها كاستجابات بشرية فعلية.

❖ يُلتزم بالأمانة العلمية وحقوق النشر وقواعد الاقتباس والتوثيق وعدم اختلاق المراجع أو النتائج.

٣,١٧ قيود المنهج:

تتعلق القيود بطبيعة التصميم المقطعي الذي لا يثبت السببية الزمنية، وبالاعتماد على تقديرات ذاتية قد تتأثر بالمعرفة أو الرغبة الاجتماعية، وبالعينة القصصية التي تحد من التعميم الاحتمالي. كما أن بعض الأبعاد في الأداة المختصرة ممثلة بعدد قليل من الفقرات. ويمكن التخفيف من ذلك مستقبلاً باستخدام بيانات طولية، وعينات طبقية احتمالية، ومؤشرات تشغيلية موضوعية، ومقياس كامن متعدد الفقرات لكل بعد.

٣,١٨ خلاصة الفصل:

عرض الفصل تصميمًا وصفيًا تحليليًا متسقًا مع أسئلة الدراسة، وحدد مجتمعًا متخصصًا وأداة من ٣٠ فقرة، وإجراءات للتحقق من الصدق والثبات والتحيز المشترك، وخطة تحليل تشمل الانحدار والوساطة والفروق. كما وضع ضوابط أخلاقية صريحة لاستخدام البيانات. ويطبق الفصل الرابع هذه الإجراءات على النموذج المحاكى لتوضيح طريقة عرض النتائج وتفسيرها، على أن يعاد التحليل عند توافر البيانات الميدانية الفعلية.

الفصل الرابع : عرض النتائج وتحليلها ومناقشتها

النتائج الوصفية، اختبار الفرضيات، الوساطة، والفروق



٤,١ مقدمة الفصل:

يعرض الفصل نتائج تطبيق خطة التحليل بالترتيب المنطقي: وصف العينة، وفحص جودة القياس، وتحديد مستويات المتغيرات، وتحليل الارتباطات، ثم اختبار الآثار المباشرة والوساطة والفروق. وتعرض الجداول الأرقام التي تدعم القرار، ثم تتبعها قراءة موضوعية تربط النتيجة بسؤال الدراسة والأدبيات من دون تكرار جميع القيم داخل النص.

٤,٢ فحص البيانات الأولى:

تضمنت قاعدة التحليل ٢١٤ حالة مكتملة. وتراوحت جميع الإجابات بين ١ و ٥، ولم توجد قيم خارج المدى أو بيانات مفقودة في النسخة المحاكاة. وفُحصت التوزيعات والالتواء والتفليطح ومخططات البواقي، ولم تظهر انحرافات شديدة تعيق استخدام الاختبارات المعلمية. كما لم تتجاوز معاملات الارتباط بين المتنبئات الحد الذي يثير قلق التعدد الخطي، وتراوحت قيم VIF لأبعاد الحوكمة ضمن حدود مقبولة.

٤,٣ خصائص عينة الدراسة:

جدول (٤-١): خصائص عينة الدراسة

المتغير	الفئة	التكرار	النسبة
جهة العمل	شركة تأمين	154	72.0%
	شركة إعادة تأمين	18	8.4%
	خدمات تأمينية	34	15.9%
	أخرى	8	3.7%
الإدارة	المخاطر	42	19.6%
	الالتزام	30	14.0%
	تقنية المعلومات	36	16.8%
	الأمن السيبراني	30	14.0%
	العمليات	28	13.1%

المتغير	الفئة	التكرار	النسبة
	المطالبات	19	8.9%
	المراجعة الداخلية	17	7.9%
	القانونية/التعاقدات	12	5.6%
سنوات الخبرة	أقل من 3 سنوات	31	14.5%
	سنوات 3-5	54	25.2%
	سنوات 6-10	75	35.0%
	أكثر من 10 سنوات	54	25.2%
حجم الشركة	صغيرة	33	15.4%
	متوسطة	73	34.1%
	كبيرة	108	50.5%
التعامل مع أطراف خارجية	منخفض	18	8.4%
	متوسط	72	33.6%
	مرتفع	124	57.9%

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

يبين التوزيع أن معظم المشاركين يعملون في شركات تأمين مباشرة، مع تمثيل لإعادة التأمين والخدمات التأمينية. كما تتوزع الاستجابات على وظائف المخاطر والتقنية والأمن والالتزام والعمليات والمطالبات والرقابة، وهو ما يدعم تنوع مصادر المعرفة. ويمثل ذوو الخبرة من ست سنوات فأكثر نسبة معتبرة، كما تهيمن الشركات الكبيرة ومستوى التعامل المرتفع مع الأطراف الخارجية؛ وهو توزيع منطقي بالنظر إلى كثافة الاعتماد الخارجي في المنشآت الأكبر والأكثر رقمنة.

٤,٤ صدق وثبات أداة القياس:

جدول (٤-٢): مؤشرات الصدق والثبات

المؤشر	القيمة	المعيار	الحكم
KMO	0.932	≥ 0.60	ملاءمة مرتفعة
Bartlett χ^2	2715.77	$df = 435, p < 0.001$	دال إحصائيًا
ألفا - حوكمة الطرف الثالث	0.806	≥ 0.70	ثبات جيد
ألفا - جاهزية الأمن السيبراني	0.903	≥ 0.70	ثبات مرتفع
ألفا - المرونة التشغيلية	0.881	≥ 0.70	ثبات مرتفع
اختبار العامل الواحد	35.6%	$< 50\%$	لا يفسر عامل واحد معظم التباين

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

تشير النتائج إلى أن مصفوفة الارتباطات مناسبة للتحليل، وأن المقاييس تتمتع باتساق داخلي مقبول. ويلاحظ أن ثبات محور الحوكمة أقل نسبيًا من المحورين الآخرين بسبب تمثيل خمسة أبعاد مختلفة بعشر فقرات فقط؛ إلا أنه يتجاوز الحد المقبول. ويساند ذلك استخدام المتوسطات المركبة في اختبار الفرضيات، مع توصية بتوسيع عدد فقرات كل بعد في البحوث اللاحقة.

٤,٥ النتائج الوصفية لمتغيرات الدراسة:

جدول (٣-٤): المتوسطات والانحرافات المعيارية للمتغيرات

الترتيب	المستوى	الانحراف	المتوسط	المتغير
1	مرتفع	0.647	3.766	جاهزية الأمن السيبراني
2	مرتفع	0.611	3.761	المرونة التشغيلية
3	مرتفع	0.523	3.691	حوكمة مخاطر الطرف الثالث

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

جاءت المتغيرات الثلاثة ضمن المستوى المرتفع، وتقدمت جاهزية الأمن السيبراني بمتوسط (٣,٧٧)، تلتها المرونة التشغيلية (٣,٧٦)، ثم حوكمة مخاطر الطرف الثالث (٣,٦٩). وتشير الفروق المحدودة بين المتوسطات إلى أن الشركات تبني قدرات أمنية وتشغيلية متقاربة، لكن متوسط الحوكمة يكشف مساحة تحسين في بعض مراحل دورة الطرف الثالث، ولا سيما الطوارئ والخروج.

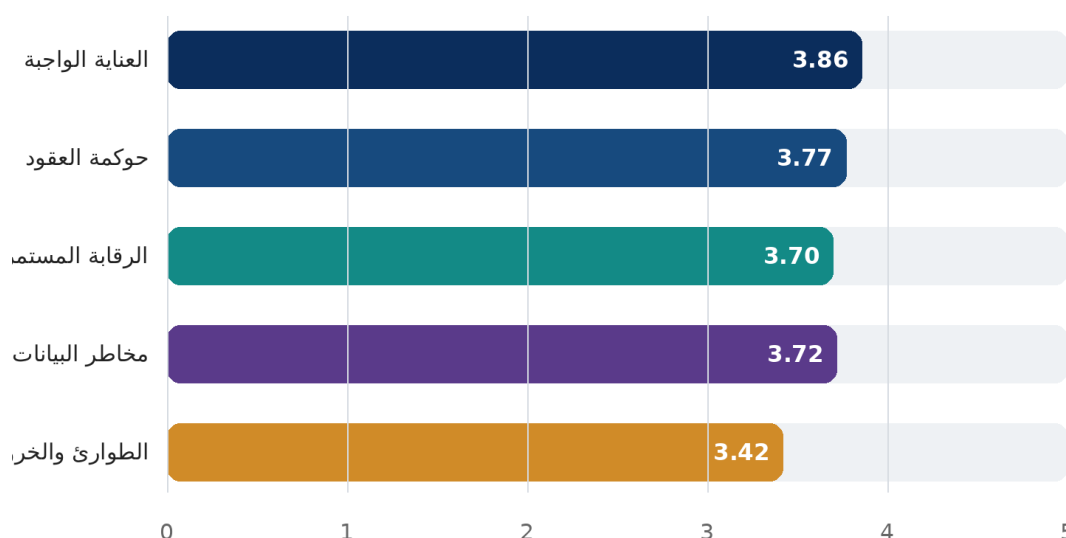
١,٥,٤ أبعاد حوكمة مخاطر الطرف الثالث:

جدول (٤-٤): نتائج أبعاد حوكمة مخاطر الطرف الثالث

الترتيب	البعد	المتوسط	الانحراف	المستوى
1	العناية الواجبة قبل التعاقد	3.855	0.724	مرتفع
2	حوكمة العقود ومستويات الخدمة	3.769	0.759	مرتفع
3	إدارة مخاطر البيانات والأمن السيبراني	3.717	0.737	مرتفع
4	الرقابة والمتابعة المستمرة	3.696	0.737	مرتفع
5	خطط الطوارئ والخروج والاستبدال	3.418	0.832	مرتفع

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

متوسطات أبعاد حوكمة مخاطر الطرف الثالث



شكل (٤-١): متوسطات أبعاد حوكمة مخاطر الطرف الثالث

المصدر: إعداد الباحث من نتائج التحليل الإحصائي للبيانات المحاكاة.

احتلت العناية الواجبة قبل التعاقد المرتبة الأولى بمتوسط (٣,٨٦)، ما يدل على اهتمام نسبي بفحص القدرات المالية والفنية والأمنية للمزود. وجاءت حوكمة العقود في مرتبة متقدمة، وهو ما يعكس شيوع مؤشرات الأداء وبنود حماية البيانات. في المقابل كان بعد خطط الطوارئ والخروج والاستبدال الأقل بمتوسط (٣,٤٢) رغم بقائه عند الحد المرتفع. وتعد هذه الفجوة مهمة؛ لأن الشركات قد تحسن اختيار المزود والتعاقد معه، لكنها تواجه صعوبة أكبر في تصميم بديل قابل للتنفيذ واختباره ضمن حدود الأثر.

٤,٥,٢ فقرات جاهزية الأمن السيبراني:

جدول (٤-٥): نتائج جاهزية الأمن السيبراني

الترتيب	الفقرة	المتوسط	الانحراف	المستوى
1	تقييم المستوى السيبراني للمزودين المعتمدين	3.991	0.845	مرتفع
2	تقييد وصول المزودين وفق الحاجة الفعلية	3.869	0.873	مرتفع
3	استخدام ضوابط لحماية البيانات المتبادلة	3.841	0.863	مرتفع
4	اختبار خطط الاستجابة والتعافي دوريًا	3.822	0.870	مرتفع

الترتيب	الفقرة	المتوسط	الانحراف	المستوى
5	وجود سياسات واضحة لمخاطر الأمن المرتبطة بالأطراف الخارجية	3.818	0.893	مرتفع
6	وجود آلية لاكتشاف الحوادث المرتبطة بالمزودين	3.762	0.896	مرتفع
7	إلزام المزودين بمتطلبات أمنية محددة	3.757	0.886	مرتفع
8	مراجعة صلاحيات المزودين دوريًا	3.715	0.903	مرتفع
9	وجود خطة استجابة تشمل حوادث الطرف الثالث	3.556	0.874	مرتفع
10	تدريب الموظفين على مخاطر الطرف الثالث والأمن السيبراني	3.528	0.958	مرتفع

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

كانت أعلى الفقرات «تقييم المستوى السيبراني للمزودين المعتمدين» بمتوسط (٣,٩٩)، ما يشير إلى نضج نسبي في الضوابط الوقائية. أما أقلها فكانت «تدريب الموظفين على مخاطر الطرف الثالث والأمن السيبراني» بمتوسط (٣,٥٣). ويؤكد ذلك أن الاختبار والتدريب يمثلان عادة مرحلة أكثر صعوبة من وضع السياسات أو تطبيق الضوابط التقنية، مع أنهما ضروريان لتحويل التصميم إلى قدرة فعلية عند الحادث.

٤,٥,٣ فقرات المرونة التشغيلية:

جدول (٦-٤): نتائج المرونة التشغيلية

الترتيب	الفقرة	المتوسط	الانحراف	المستوى
1	استمرار الخدمات الأساسية عند تعطل مزود خدمة	3.939	0.889	مرتفع
2	وضوح أولويات الخدمات الحيوية أثناء الأزمات	3.925	0.874	مرتفع
3	وجود خطط استمرارية تشمل الأطراف الخارجية	3.822	0.897	مرتفع
4	الحفاظ على جودة خدمة العملاء أثناء الاضطراب	3.780	0.874	مرتفع
5	مرونة نقل الخدمة إلى مزود بديل	3.743	0.869	مرتفع
6	التعافي السريع من الاضطرابات التشغيلية	3.729	0.873	مرتفع

الترتيب	الفقرة	المتوسط	الانحراف	المستوى
7	وجود آليات لحماية السمعة أثناء الاضطراب	3.729	0.945	مرتفع
8	وجود آليات لتقليل الأثر المالي للحوادث	3.692	0.849	مرتفع
9	عدم تسبب مشكلات المزودين في توقف طويل	3.687	0.861	مرتفع
10	اختبار سيناريوهات انقطاع الخدمة مع المزودين	3.561	0.869	مرتفع

المصدر: نتائج التحليل الإحصائي للبيانات المحاكاة.

تقدمت فقرة «استمرار الخدمات الأساسية عند تعطل مزود خدمة» بمتوسط (٣,٩٤)، بينما جاءت «اختبار سيناريوهات انقطاع الخدمة مع المزودين» في المرتبة الأخيرة بمتوسط (٣,٥٦). وتتسق النتيجة مع انخفاض بعد الخروج؛ إذ يبدو أن المحافظة على الخدمة والجودة داخل الترتيب القائم أقوى من اختبار الانقطاع أو نقل الخدمة عند فشل المزود.

٤,٦ الارتباطات بين متغيرات الدراسة:

جدول (٧-٤): مصفوفة الارتباطات بين المتغيرات

المتغير	1	2	3	المتوسط	الانحراف
حوكمة الطرف الثالث 1.	1.000			3.691	0.523
جاهزية الأمن السيبراني 2.	0.603***	1.000		3.766	0.647
المرونة التشغيلية 3.	0.703***	0.657***	1.000	3.761	0.611

المصدر: نتائج التحليل الإحصائي. *** دال عند $p < 0.001$.

جميع الارتباطات موجبة ودالة. وبلغ ارتباط الحوكمة بالمرونة (٠,٧٠٣)، ما يشير إلى أن ارتفاع نضج دورة الطرف الثالث يقترن بقدرة أكبر على استمرار الخدمة والتعافي. وبلغ ارتباط الحوكمة بالجاهزية (٠,٦٠٣)، وارتباط الجاهزية بالمرونة (٠,٦٥٧). وهذه القيم قوية بما يكفي لدعم الاختبار، لكنها لا تصل إلى مستويات تشير إلى تطابق المتغيرات أو مشكلة تعدد خطي حادة.

٤,٧ اختبار الفرضية الرئيسة الأولى وأبعادها:

جدول (٤-٨): الانحدار المتعدد لأبعاد الحوكمة على المرونة التشغيلية

البعد	β المعياري	t	p	VIF	القرار
العناية الواجبة قبل التعاقد	0.264	4.775	< 0.001	1.28	دال
حوكمة العقود ومستويات الخدمة	0.217	3.877	< 0.001	1.30	دال
الرقابة والمتابعة المستمرة	0.130	2.246	0.026	1.40	دال
إدارة مخاطر البيانات والأمن السبراني	0.198	3.575	< 0.001	1.28	دال
خطط الطوارئ والخروج والاستبدال	0.214	3.781	< 0.001	1.34	دال

المصدر: نتائج التحليل الإحصائي. $R^2 = 0.501$ ، المعدل = ٤٨٩، $p < 0.001$ ، $F = 41.73$.

كان أثر الدرجة الكلية للحوكمة في المرونة موجباً ودالاً ($p < 0.001$)، فتقبل $H1$. وفي النموذج المتعدد فسرت الأبعاد الخمسة معاً (١, ٥٠٪) من تباين المرونة. وظهرت جميع الأبعاد مؤثرة، مع بروز العناية الواجبة ثم حوكمة العقود وخطط الخروج وإدارة مخاطر البيانات، بينما كان أثر الرقابة المستمرة أصغر لكنه دال. ولا تعني المقارنة النسبية إهمال أي بعد؛ فالدورة تعمل كنظام مترابط، وقد يتغير ترتيب الآثار في البيانات الفعلية.

٤,٨ اختبار H2 و H3 ونموذج الوساطة H4

جدول (٤-٩): نتائج اختبار المسارات والوساطة

المسار	β /الأثر	SE	t	p	R ² /فترة الثقة
(a) الحوكمة ← الجاهزية: H2	0.603	0.055	11.013	< 0.001	0.364
(b) الجاهزية ← المرونة مع ضبط الحوكمة: H3	0.366	0.056	6.550	< 0.001	0.580
(c') الأثر المباشر للحوكمة في المرونة	0.482	0.056	8.614	< 0.001	0.580
(c) الأثر الكلي للحوكمة في المرونة	0.703	0.049	14.396	< 0.001	0.494
H4: الأثر غير المباشر (a×b)	0.221	-	-	دال	95% CI [0.143, 0.304]

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

نتائج نموذج الوساطة



شكل (٤-٢): نتائج نموذج الوساطة

المصدر: إعداد الباحث من نتائج التحليل الإحصائي للبيانات المحاكاة.

أظهرت النتائج أن الحوكمة تتنبأ بالجاهزية السيبرانية ($p < 0.001$) ($\beta = 0.603$)، فتُقبل H2. كما ظلت الجاهزية متنبئًا بالمرونة بعد ضبط الحوكمة ($\beta = 0.366$) ($p < 0.001$)، فتُقبل H3. وبلغ الأثر غير المباشر (0.221) بفترة ثقة [0.143, 0.304] لا تشمل الصفر؛ فتُقبل H4. ومع بقاء الأثر المباشر دالًا، تكون الوساطة جزئية، ويعبر المسار غير المباشر عن نحو (31.4٪) من الأثر الكلي النموذجي.

تعني الوساطة أن جزءًا مهمًا من قيمة الحوكمة يتحقق عندما ترفع قدرة الشركة على الحماية والكشف والاستجابة والتعافي. ومع ذلك يبقى للحوكمة أثر مباشر ناتج عن عناصر لا تختزل في الأمن، مثل الملاءة المالية للمزود، وخيارات الاستبدال، وقدرة التعاقد والتشغيل البديل.

٤,٩ اختبار الفروق وفق الخصائص التنظيمية:

جدول (٤-١٠): اختبار الفروق وفق المتغيرات التنظيمية

القرار	η^2	p	F	المتغير
غير دال	0.015	0.380	1.032	جهة العمل
غير دال	0.023	0.666	0.707	الإدارة
غير دال	0.012	0.468	0.850	سنوات الخبرة
غير دال	0.012	0.278	1.287	حجم الشركة
غير دال	0.005	0.564	0.574	مستوى التعامل مع الأطراف

المصدر: نتائج تحليل التباين الأحادي للبيانات المحاكاة.

لم تظهر فروق دالة في تقدير المرونة التشغيلية وفق جهة العمل أو الإدارة أو الخبرة أو حجم الشركة أو مستوى التعامل مع الأطراف، وكانت أحجام الأثر صغيرة. وبناءً عليه لا تُقبل H5 في النموذج المحاكى. وقد يشير ذلك إلى أن المتطلبات والممارسات المؤسسية المشتركة أقوى من الخصائص الفردية، أو إلى أن الفروق الفعلية تحتاج عينة أكبر ومؤشرات موضوعية على مستوى الشركة. ولا ينبغي تفسير غياب الدلالة على أنه تطابق كامل بين الشركات.

٤,١٠ ملخص قرارات اختبار الفرضيات:

جدول (٤-١١): قرار اختبار فرضيات الدراسة

الفرضية	المضمون المختصر	القرار
H1	حوكمة الطرف الثالث تؤثر في المرونة التشغيلية	مقبولة
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	إدارة مخاطر البيانات والأمن تؤثر في المرونة	مقبولة
H1.5	الطوارئ والخروج والاستبدال تؤثر في المرونة	مقبولة
H2	الحوكمة تؤثر في جاهزية الأمن السيبراني	مقبولة
H3	جاهزية الأمن السيبراني تؤثر في المرونة	مقبولة
H4	الجاهزية تتوسط العلاقة بين الحوكمة والمرونة	مقبولة - وساطة جزئية
H5	فروق وفق الخصائص الوظيفية والتنظيمية	غير مقبولة في النموذج المحاكى

المصدر: إعداد الباحث من نتائج التحليل الإحصائي.

٤,١١ مناقشة النتائج:

٤,١١,١ مستوى حوكمة مخاطر الطرف الثالث:

يعكس المستوى المرتفع للحوكمة إدراكًا مؤسسيًا لأهمية تقييم المزودين وإدراج متطلبات الأداء والبيانات ومراجعة العلاقات. وتتفق النتيجة مع الاتجاه التنظيمي السعودي الذي يربط ترتيبات الإسناد بالعناية الواجبة والرقابة وخطط الطوارئ والسجل المحدث (البنك المركزي السعودي، ٢٠١٩). كما تنسجم مع الأدبيات التي ترى أن التقييم والمراقبة والتكامل بين الوظائف عناصر أساسية لنضج إدارة الموردين السيبرانيين (Slapnicar et al., 2025). في المقابل، كان الخروج والطوارئ الأقل. ويمكن تفسير ذلك بارتفاع تكاليف النقل، والاعتماد على منصات متخصصة، وصعوبة اختبار فشل مزود دون التأثير في الخدمة.

وتظهر الأطر الحديثة أن هذه الصعوبة لا تبرر إهمال الخروج، بل تستدعي حلولاً متدرجة مثل قابلية نقل البيانات، والقدرة الداخلية الدنيا، والتشغيل المزدوج، وخيارات الاستعادة المستقلة. (FSB, 2023; BCBS, 2025).

٤,١١,٢ مستوى جاهزية الأمن السيبراني:

يتسق ارتفاع الجاهزية مع البيئة التنظيمية التي تفرض حوكمة وحماية وصموداً وضوابط للأطراف الخارجية والسحابة (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤). ويظهر تقدم فقرات حماية البيانات والتقييم أن الضوابط الوقائية أكثر رسوخاً، بينما يكشف انخفاض الاختبار والتدريب انتقالاً غير مكتمل من الامتثال إلى القدرة. وقد أكد NIST أن إدارة سلسلة التوريد السيبرانية تتطلب استراتيجية واتصال متطلبات ومراقبة واختباراً عبر الوظائف، لا تقييماً ورقياً عند البداية فقط. (NIST, 2024).

٤,١١,٣ مستوى المرونة التشغيلية:

يدل المستوى المرتفع على وجود خطط وقدرة على استمرار الخدمة، لكنه لا يعني أن جميع التبعيات اختُبرت. فالفجوة بين جودة الخدمة اليومية واختبار سيناريوهات فقد المزود توضح الفرق بين الأداء المستقر والمرونة المثبتة. وتتفق النتيجة مع طرح IAIS الذي يدعو إلى منظور خدماتي يحدد التبعيات والحدود والاختبارات، ومع نموذج Duchek الذي لا يكتفي بالمواجهة بل يضيف التوقع والتكيف. (IAIS, 2023; Duchek, 2020).

٤,١١,٤ أثر الحوكمة في المرونة:

يدعم الأثر الموجب منطق نظرية الاعتماد على الموارد؛ فالاعتماد لا يصبح هشاشة حتمية عندما توجد آليات لاختيار المزود وفرض الشروط والمراقبة والحفاظ على البدائل. كما يدعم القدرات الديناميكية؛ لأن التقييم المستمر وخطط الخروج تمنح الشركة قدرة على استشعار التدهور وإعادة تشكيل الموارد. وتتفق النتيجة مع بوداود (٢٠٢١) وطرطاق (٢٠١٩) في الصلة بين إدارة المخاطر والأداء التشغيلي في التأمين، وتضيف إليهما تحديد الطرف الثالث واختبار أبعاده.

كما تتوافق مع Boyson (2014) و Gani et al. (2023) بشأن أثر الممارسات المنظمة في خفض مخاطر السلسلة وتحسين الأداء الأمني، ومع الأدلة على انتقال الهجمات عبر العلاقات التجارية. (Crosignani et al., 2023) ويعني ذلك أن الحوكمة ليست تكلفة امتثال فقط، بل استثمار في موثوقية الخدمة.

٤,١١,٥ الدور الوسيط لجاهزية الأمن السيبراني:

تقدم الوساطة أهم إضافة تفسيرية للدراسة. فالسياسة والعقد والتقييم لا يؤثران في المرونة بالكامل بصورة مباشرة؛ بل يرفعان أولاً وضوح أدوار الأمن وضبط الوصول والكشف والتنسيق والاختبار، ثم تُترجم هذه القدرات إلى تقليل زمن التوقف والأثر. وتنسجم النتيجة مع المنظور الاجتماعي-التقني ومع بناء NIST الذي يربط الحوكمة بوظائف الحماية والكشف والاستجابة والتعافي. (NIST, 2024)

وبقاء الأثر المباشر يؤكد أن المرونة أوسع من الأمن السيبراني. فقد يفشل المزود ماليًا أو تشغيليًا دون حادث سيبراني، وقد يضعف العقد أو البديل حتى مع وجود أدوات أمنية. لذلك ينبغي ألا تنحصر حوكمة الطرف الثالث في فريق الأمن، بل تكون برنامجًا متعدد الوظائف تقوده المخاطر ومالكو الخدمات وتشارك فيه المشتريات والقانونية والالتزام والتقنية واستمرارية الأعمال.

٤,١٢ خلاصة الفصل:

أظهرت النتائج النموذجية مستويات مرتفعة للمتغيرات، مع فجوة نسبية في خطط الخروج والاختبارات المشتركة. وأكدت الارتباطات والانحدارات أثر الحوكمة وأبعادها في المرونة، وأثبت نموذج الوساطة أن جاهزية الأمن السيبراني تنقل جزءًا معتبرًا من هذا الأثر مع بقاء مسار مباشر. ولم تظهر فروق دالة وفق الخصائص التنظيمية. وتبنى توصيات الفصل الخامس على هذه النتائج، مع التأكيد مجددًا على ضرورة إعادة التحليل بالبيانات الفعلية قبل الاعتماد الأكاديمي.

الفصل الخامس: الاستنتاجات والتوصيات

تحويل نتائج الدراسة إلى نموذج حوكمة وخارطة تنفيذ قابلة للقياس



٥,١ مقدمة الفصل:

يختتم هذا الفصل الدراسة بتجميع نتائجها في استنتاجات مترابطة، ثم تحويلها إلى توصيات عملية قابلة للتنفيذ والقياس لدى شركات التأمين في المملكة العربية السعودية. ولا يقتصر الفصل على إعادة عرض الأرقام، بل يفسر ما تعنيه للإدارة العليا ومالكي الخدمات ووظائف المخاطر والأمن السيبراني والمشتريات والقانونية واستمرارية الأعمال، ويقترح نموذجًا تشغيليًا وخارطة طريق ومؤشرات أداء ومخاطر.

ولأن المرفق لم يتضمن قاعدة استجابات فعلية، فإن الاستنتاجات الكمية الواردة هنا مرتبطة بالنموذج المحاكى الموضح في الفصل الرابع. أما التوصيات النظرية والتنظيمية فمبنية على مراجعة الأدبيات والأطر الرسمية، ويمكن تطبيقها مبدئيًا، مع ضرورة إعادة تقدير الأولويات والأحجام الإحصائية بعد جمع البيانات الميدانية.

٥,٢ ملخص النتائج الرئيسية:

جدول (٥-١): خلاصة النتائج ودلالاتها الإدارية

النتيجة	الدليل المختصر	الدلالة الإدارية
مستوى حوكمة الطرف الثالث	مرتفع بمتوسط كلي (3.69)، مع تفوق العناية الواجبة وانخفاض نسبي في الطوارئ والخروج.	وجود أساس حوكمي، لكن قابلية الاستبدال والاختبار تحتاجان تعزيزًا.
جاهزية الأمن السيبراني	مرتفعة بمتوسط (3.77)، مع فجوة نسبية في التدريب والتمارين المشتركة.	الامتثال الوقائي أقوى من القدرة المختبرة على الاستجابة المشتركة.
المرونة التشغيلية	مرتفعة بمتوسط (3.76)، مع انخفاض نسبي في نقل الخدمة واختبار فقد المزود.	جودة الخدمة اليومية لا تكفي لإثبات الصمود في الاضطراب.
الأثر الكلي للحوكمة	$R^2 = 0.703$ ؛ $\beta = 0.703$ ؛ $R^2 = 0.494$) أثر موجب دال	الحوكمة أصل تشغيلي يفسر جزءًا مهمًا من تفاوت المرونة.

النتيجة	الدليل المختصر	الدلالة الإدارية
أبعاد الحوكمة الخمسة	جميع الأبعاد ذات آثار موجبة. دالة في نموذج الانحدار المتعدد	القيمة تتحقق من حزمة متكاملة لا من إجراء منفرد.
الدور الوسيط	وساطة جزئية؛ الأثر غير المباشر = 0.221 وفترة الثقة لا تشمل الصفر	الجاهزية السيبرانية قناة تنفيذية مهمة بين الحوكمة والمرونة.
الفروق التنظيمية	لم تظهر فروق دالة في النموذج المحاكى	يجب التركيز على نضج النظام المؤسسي مع التحقق ميدانيًا من الفروق.

المصدر: إعداد الباحث استنادًا إلى نتائج الفصل الرابع؛ النتائج الكمية محاكاة.

٥,٣ الاستنتاجات والإجابة عن أسئلة الدراسة:

٥,٣,١ واقع حوكمة مخاطر الطرف الثالث:

تشير الدراسة إلى أن شركات التأمين تستطيع بناء مستوى جيد من الحوكمة عندما تتوفر سياسة موحدة وسجل للمزودين وتصنيف للأهمية وعناية واجبة وعقود قابلة للرقابة. غير أن النضج الحقيقي لا يقاس بعدد الاستبيانات أو البنود التعاقدية، بل بقدرة الشركة على معرفة أي خدمة تعتمد على أي مزود وأي طرف لاحق وأي بيانات، وبقدرتها على اكتشاف التدهور والتدخل والخروج قبل تجاوز حد تحمل الأثر.

ويستنتج أن أضعف حلقة محتملة تقع بعد التعاقد: المراقبة القائمة على المخاطر، واختبار سيناريوهات التعطل، وقابلية نقل البيانات والخدمة. وهذا يتوافق مع الاتجاه التنظيمي الذي ينقل إدارة المخاطر من تقييم الدخول إلى دورة حياة كاملة تشمل الرقابة والاستمرارية والخروج (البنك المركزي السعودي، ٢٠١٩). (FSB, 2023; BCBS, 2025).

٥,٣,٢ مستوى جاهزية الأمن السيبراني:

تظهر الجاهزية بوصفها منظومة قدرات تشمل الحوكمة والحماية والكشف والاستجابة والتعافي والتعلم. وتستنتج الدراسة أن الضوابط التقنية، مهما كانت متقدمة، لا تنتج

جاهزية كاملة إذا لم ترتبط بملكية واضحة للخدمة، وبإخطار سريع للحوادث، وبسجلات قابلة للمشاركة، وبتمارين مشتركة مع المزودين، وبقرارات تصعيد يفهمها أصحاب المصلحة. كما أن الجاهزية ليست صفة ثابتة؛ فهي تتغير مع التقنيات والمزودين والتهديدات. لذلك يلزم قياسها عبر أدلة تشغيلية مثل زمن اكتشاف الحادث وزمن الاحتواء ونسبة حسابات المزود التي خضعت للمراجعة ونسبة التمارين التي أُغلقت ملاحظاتها، وليس من خلال وجود السياسة وحده (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤). (NIST, 2024).

٥,٣,٣ مستوى المرونة التشغيلية:

تستنتج الدراسة أن المرونة التشغيلية هي قدرة على إبقاء النتيجة المهمة للعميل داخل حد تحمل مقبول، حتى عندما يتعطل مورد أو نظام أو موقع. ومن ثم يجب أن تبدأ من الخدمة الحيوية، ثم تُرسم تبعياتها البشرية والتقنية والبيانية والتعاقدية، وتحدد بدائلها، وتختبر على سيناريوهات شديدة ومعقولة. ولا تكفي خطط التعافي المنفصلة إذا تعذر ربطها برحلة المطالبة أو الإصدار أو شبكة مقدمي الخدمة. (IAIS, 2023; BCBS, 2021).

٥,٣,٤ أثر الحوكمة في المرونة:

تؤكد النتيجة أن حوكمة الطرف الثالث تؤثر إيجابياً في المرونة لأنها تخفف عدم اليقين، وتربط التزام المزود بالخدمة الحيوية، وتوفر إنذاراً مبكراً وخيارات للاستجابة والخروج. وتعمل الأبعاد الخمسة بصورة تكاملية: العناية الواجبة تمنع اختيار علاقة غير مناسبة، والعقد يحول التوقعات إلى التزام، والمراقبة تكشف الانحراف، وضوابط البيانات والأمن تحد من انتقال الأثر، وخطة الخروج تمنع تحول الاعتماد إلى احتجاز تشغيلي.

٥,٣,٥ الدور الوسيط للجاهزية السيبرانية:

تفسر الوساطة الجزئية كيف تتحول الحوكمة إلى مرونة: ترفع الحوكمة وضوح المتطلبات والاتصال والرصد والتحكم في الوصول والاختبار، فتتحسن قدرة الأمن السيبراني على الحماية والكشف والاستجابة والتعافي، ثم يقل أثر التعطل في الخدمات. وبقاء أثر مباشر يعني أن الحوكمة تعالج كذلك فشل المزود المالي أو البشري أو القانوني أو التشغيلي. ولذلك فإن وضع البرنامج داخل الأمن السيبراني وحده يضيق نطاقه، بينما وضعه داخل المشتريات وحدها يضعف عمقه الرقابي.

الاستنتاج المركزي:

لا تتحقق المرونة بشراء خدمة موثوقة مرة واحدة؛ بل بامتلاك رؤية مستمرة للتبعية، وحقوق تعاقدية قابلة للتنفيذ، وقدرات مشتركة للاكتشاف والاستجابة، وخيارات واقعية للاستمرار أو الخروج.

٥,٤ التوصيات العملية:

جدول (٥-٢): مصفوفة التوصيات والمسؤوليات والأولويات

م	التوصية	المالك الرئيس	مؤشر المتابعة	الأفق	الأولوية
1	إنشاء إطار مؤسسي موحد لحوكمة مخاطر الطرف الثالث مع تفويض من مجلس الإدارة.	مجلس الإدارة/لجنة المخاطر	اعتماد السياسة وتحديد شهية المخاطر ونسبة الخدمات المغطاة	فورية	عالية جداً
2	بناء سجل مركزي يربط كل مزود بالخدمة الحيوية والبيانات والطرف اللاحق ومالك العلاقة.	إدارة المخاطر والمشتريات	من المزودين 100% المهمين مسجلون ومصنفون	0-3 أشهر	عالية جداً
3	اعتماد تصنيف قائم على الأهمية والأثر بدل تصنيف الإنفاق فقط.	المخاطر واستمرارية الأعمال	نسبة العلاقات المعاد تصنيفها واكتمال تحليل الأثر	0-3 أشهر	عالية
4	توحيد العناية الواجبة متعددة التخصصات وربط عمقها بدرجة الخطر.	المشتريات/الأم ن/القانونية	نسبة التقييمات المكتملة قبل التعاقد وعدد الاستثناءات	3-6 أشهر	عالية
5	تحديث العقود ببند الأمن والإخطار والتدقيق والاستمرارية والأطراف اللاحقة والخروج.	الشؤون القانونية	نسبة العقود المهمة المحتوية على الحد الأدنى من البنود	3-9 أشهر	عالية جداً

م	التوصية	المالك الرئيس	مؤشر المتابعة	الأفق	الأولوية
6	إطلاق مراقبة مستمرة تعتمد مؤشرات الأداء والمخاطر وإعادة التقييم بحسب الحدث.	مالك الخدمة/المخاطر	نسبة الإنذارات المغلقة في الموعد وعدد العلاقات المتدهورة	3-9 أشهر	عالية
7	تقليل الصلاحيات الدائمة للمزودين ومراجعة الوصول والسجلات بصورة دورية.	الأمن السيبراني وتقنية المعلومات	نسبة الحسابات المراجعة وزمن إلغاء الوصول	0-6 أشهر	عالية جدًا
8	تنفيذ تمارين مشتركة لفقد مزود أو اختراق سلسلة توريد وربطها بحدود تحمل الأثر.	استمرارية الأعمال والأمن	نسبة الخدمات المهمة المختبرة وإغلاق الملاحظات	6-12 شهرًا	عالية
9	إعداد خطة خروج قابلة للاختبار لكل علاقة مهمة تشمل نقل البيانات والبدائل والقدرة الداخلية.	مالك الخدمة/القانونية/التقنية	نسبة العلاقات المهمة ذات خطة خروج مجربة	6-12 شهرًا	عالية جدًا
10	رفع تقارير مخاطر مركزة إلى الإدارة العليا عن التركز والاستثناءات والاختبارات والحوادث.	مسؤول مخاطر الطرف الثالث	انتظام لوحة القياس وجودة قرارات التصعيد	ربع سنوي	عالية

المصدر: إعداد الباحث استنادًا إلى نتائج الدراسة والأطر التنظيمية.

٥.٥ النموذج المقترح لحوكمة مخاطر الطرف الثالث:

يقترح البحث نموذجًا دوريًا يبدأ بالخدمة الحيوية ولا ينتهي بإغلاق العقد. ويقوم على ثلاث طبقات: حوكمة تحدد الملكية والشهية؛ دورة حياة تضبط العلاقة؛ وتمكين سيبراني وتشغيلي يثبت القدرة عبر القياس والاختبار. وتغذي الحوادث والاختبارات والتغيرات مرحلة التعلم، فتعود نتائجها إلى التصنيف والعقد والضوابط.

جدول (٣-٥): النموذج التشغيلي المقترح

المخرج	العناصر	طبقة النموذج
قرار واعٍ ومتسق بشأن الاعتماد الخارجي	،شبهة المخاطر، الأدوار، السياسة اللجان، الاستثناءات	١. الحوكمة والتوجيه
توجيه الموارد إلى العلاقات الأعلى أثرًا	،الخدمات الحيوية، التبعيات البيانات، الأهمية، التركيز	٢. تحديد النطاق والتصنيف
قبول أو معالجة أو رفض مبني على دليل	،مالي، تشغيلي، قانوني، سيبراني خصوصية، استمرارية	٣. العناية الواجبة
تحويل المعالجة إلى التزام قابل للتنفيذ	،الإخطار، التدقيق، SLA، RTO/RPO، الأطراف اللاحقة، الخروج	٤. التعاقد والتهيئة
اكتشاف مبكر وتدخل متناسب	أحداث التغيير، تقارير، KPI/KRI الضمان، الثغرات، الحوادث	٥. المراقبة والإنذار
إبقاء الخدمة ضمن حد تحمل الأثر	خرائط التبعية، تمارين، بدائل، نسخ واستعادة، اتصال أزمات	٦. المرونة المشتركة
إنهاء آمن وتغذية دورة الحوكمة	،نقل البيانات، إنهاء الوصول، بديل، مراجعة لاحقة، تحسين	٧. الخروج والتعلم

المصدر: إعداد الباحث بالاستناد إلى البنك المركزي السعودي (٢٠١٩)؛ الهيئة الوطنية للأمن السيبراني (٢٠٢٤)؛ (FSB (2023)؛ (BCBS (2025).

٥,٦ مستويات النضج المقترحة:

جدول (٤-٥): سلم نضج حوكمة الطرف الثالث

المستوى	الخصائص	الخطوة التالية
ابتدائي	قوائم متفرقة، استجابة بعد الحدث، ملكية غير واضحة	جرد المزودين وتحديد المسؤولين.
منظم	سياسة وقوالب موحدة وتقييم قبل التعاقد.	تطبيق التصنيف وسجل مركزي.
متكامل	ربط المزود بالخدمة والبيانات؛ مراقبة وتعاقد متعدد الوظائف	توحيد البيانات ولوحات القياس.
مختبر	حدود تحمل واختبارات مشتركة وخطط خروج مجربة.	توسيع السيناريوهات ومعالجة التركيز.
متكيف	مراقبة شبه آنية وتعلم من الأحداث وإعادة تشكيل سريعة.	تحسين تنبؤي ومقارنة معيارية.

المصدر: نموذج مقترح من إعداد الباحث.

٥,٧ خارطة التنفيذ المرحلية:

جدول (٥-٥): خارطة طريق تنفيذ النموذج المقترح

المرحلة	الأعمال الرئيسة	النتيجة المستهدفة	بوابة الانتقال
٠ - ٣ أشهر: التأسيس	راعٍ تنفيذي، سياسة سجل أولي، تعريف الخدمة الحيوية، تصنيف سريع	تغطية أعلى المخاطر وتوحيد اللغة	اكتمال الجرد؛ تعيين المالكين؛ اعتماد السياسة

المرحلة	الأعمال الرئيسة	النتيجة المستهدفة	بوابة الانتقال
٣-٦ أشهر: الضبط	،عناية واجبة موحدة مكتبة بنود، مراجعة الوصول، لوحة مؤشرات أولية	خفض الفجوات الدرجة في العلاقات القائمة	نسبة العقود المراجعة؛ الاستثناءات؛ زمن إلغاء الوصول.
6 - 12 شهرًا: الاختبار	خرائط تبعية، تمارين ،مشتركة، خطط خروج مراقبة قائمة على الأحداث	تحويل الوثائق إلى قدرة مثبتة.	نسبة الاختبارات الناجحة؛ زمن الاستعادة؛ إغلاق الملاحظات
12 - 18 شهرًا: التكامل	تكامل الأنظمة، تحليل التركز، تقارير مجلس الإدارة، ضمان مستقل	إدارة محفظة الطرف الثالث على مستوى المؤسسة	حدود التركيز؛ جودة البيانات؛ مستوى النضج.
بعد 18 شهرًا: التحسين	،أتمتة الرصد ،سيناريوهات متقدمة مقارنة معيارية، تعلم مستمر	قدرة متكيفة مع تغير السوق والتهديد	انخفاض الخسائر والتعطيل؛ سرعة القرار؛ تحسن رضا العملاء

المصدر: إعداد الباحث.

٥,٨ مؤشرات الأداء والمخاطر المقترحة

جدول (٥-٦): لوحة قياس استرشادية للبرنامج

النوع	المؤشر	طريقة الحساب	الحد الاسترشادي	الدورية
KPI	تغطية التقييم	÷ عدد العلاقات المهمة المقيمة إجمالي العلاقات المهمة	≥ 95%	شهري
KPI	اكتمال البنود	العقود المهمة المستوفية للحد الأدنى ÷ الإجمالي	≥ 90%	ربع سنوي

النوع	المؤشر	طريقة الحساب	الحد الاسترشادي	الدورية
KRI	الاستثناءات المتأخرة	استثناءات المخاطر التي تجاوزت تاريخ المعالجة	$\leq 5\%$	شهري
KRI	التركيز	نسبة الخدمات الحيوية المعتمدة على مزود واحد دون بديل	اتجاه هابط	ربع سنوي
KPI	الاختبار	الخدمات المهمة التي اختُبرت خلال 12 شهرًا	100%	ربع سنوي
KPI	إغلاق الملاحظات	÷ الملاحظات المغلقة في الموعد الإجمالي	$\geq 90\%$	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	ساعة 24 $\leq$	لكل خروج
KRI	تجاوز حد الأثر	عدد الحوادث التي تجاوزت حد تحمل الخدمة	صفر/اتجاه هابط	ربع سنوي

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

٥,٩ توصيات للجهات التنظيمية والقطاع:

- (١) إصدار إرشاد قطاعي متكامل لمخاطر الطرف الثالث في التأمين يربط الإسناد والأمن السيبراني والخصوصية والمرونة التشغيلية.
- (٢) تعزيز الإفصاح الرقابي عن التركيز في المزودين المهمين والأطراف اللاحقة ومواقع معالجة البيانات.

- ٣) تشجيع تمارين قطاعية مشتركة لسيناريو تعطل مزود سحابي أو منصة مطالبات أو بوابة دفع، مع حماية سرية المعلومات.
- ٤) تطوير قوالب موحدة للحد الأدنى من البنود التعاقدية وحقوق التدقيق والإخطار والحصول على البيانات عند الخروج.
- ٥) إنشاء آلية آمنة لتبادل مؤشرات المخاطر والحوادث والدروس بين شركات التأمين والجهات ذات العلاقة.
- ٦) ربط تقييم المرونة الرقابي بالخدمات والنتائج المقدمة للمستفيد، وليس بخطة تقنية منفصلة فقط.

٥,١٠ حدود الدراسة:

- التصميم المقطعي، عند تطبيقه، يقيس التصورات في نقطة زمنية واحدة ولا يثبت السببية الزمنية وحده.
- الاعتماد على الاستبانة قد يتأثر بالتحيز الاجتماعي وباختلاف معرفة المشاركين بتفاصيل العقود والاختبارات.
- تعدد أحجام الشركات ونماذج أعمالها ومستويات تعهدها قد يخفي فروقاً لا تظهر في المتوسط الكلي.
- يتغير السياق التنظيمي والسيبراني بسرعة؛ ولذلك تحتاج المراجع والضوابط إلى مراجعة قبيل المناقشة والتسليم.

٥,١١ مقترحات للبحوث المستقبلية:

- إجراء دراسة طولية تربط تغير مستوى الحوكمة بأزمة التعطل والحوادث والشكاوى ومؤشرات استعادة الخدمة.
- اختبار النموذج باستخدام بيانات متعددة المصادر: موظفون، عقود، سجلات حوادث، تقارير تدقيق، ونتائج تمارين.
- دراسة أثر تركّز الاعتماد على مزودي السحابة والمنصات الصحية والدفع على مرونة قطاع التأمين.
- مقارنة شركات التأمين بحسب الحجم ونموذج العمل ومستوى النضج الرقمي، أو مقارنة المملكة بأسواق خليجية أخرى.

- اختبار متغيرات وسيطة أو معدلة مثل ثقافة المخاطر، جودة العلاقة، نضج استمرارية الأعمال، أو دعم الإدارة العليا.
- تطوير مؤشر موضوعي لنضج حوكمة الطرف الثالث والتحقق من صدقه التنبؤي للحوادث والخسائر التشغيلية.

٥,١٢ الخاتمة العامة :

تنتهي الدراسة إلى أن الطرف الثالث ليس خارج حدود شركة التأمين من منظور المخاطر؛ فقد يكون خارج هيكلها القانوني، لكنه داخل سلسلة تقديم الخدمة وداخل نطاق مسؤوليتها تجاه العميل والجهات المنظمة. وكلما ازدادت رقمنة التأمين، أصبح فهم التبعيات وفرض المتطلبات ومراقبة الأداء واختبار البدائل من شروط الثقة والاستمرارية. والرسالة الرئيسة هي أن المرونة التشغيلية لا تُشتري من مزود، بل تُبنى من خلال حوكمة مؤسسية وقدرات سيبرانية وتعاون متعدد الوظائف واختبارات واقعية. ويساعد النموذج المقترح شركات التأمين على الانتقال من ملفات امتثال متفرقة إلى منظومة قرار وقياس وتعلم تغطي دورة الحياة كاملة. ويبقى استكمال المسح الميداني وإعادة التحليل شرطاً لازماً لتحويل النتائج النموذجية في هذه النسخة إلى نتائج علمية نهائية قابلة للمناقشة الأكاديمية.

قائمة المراجع:

أولاً: المراجع العربية

- البنك المركزي السعودي. (٢٠١٧). الإطار التنظيمي للأمن السيبراني. [\[رابط\]](#)
- البنك المركزي السعودي. (٢٠١٩). تعليمات إسناد المهام إلى طرف ثالث. [\[رابط\]](#)
- البنك المركزي السعودي. (د.ت.). الأمن السيبراني للأطراف الخارجية، كتاب القواعد التنظيمية. [\[رابط\]](#)
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٤). الضوابط الأساسية للأمن السيبراني - ECC 2-٢٠٢٤. [\[رابط\]](#)
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٠). ضوابط الأمن السيبراني للحوسبة السحابية. [\[رابط\]](#)
- هيئة التأمين. (٢٠٢٦). تقرير سوق التأمين السعودي لعام ٢٠٢٥. [\[رابط\]](#)
- بوداود، خليل. (٢٠٢١). أثر إدارة المخاطر على تحسين أداء شركات التأمين: دراسة حالة. مجلة الاقتصاد والتنمية المستدامة، ٤(٢)، ٨-٢٠. [\[رابط\]](#)
- حشمان، سرين، وحدي، عبد القادر. (٢٠٢٤). المخاطر السيبرانية في الصناعة المالية الإسلامية. المجلة الجزائرية للعملة والسياسات الاقتصادية، ١٥ (عدد خاص)، ٥٩-٧٢. [\[رابط\]](#)
- طرطاق، رتيبة. (٢٠١٩). التوجهات الاستراتيجية لإدارة المخاطر التشغيلية في شركات التأمين على ضوء متطلبات معيار الملاءة ٢. مجلة العلوم الإدارية والمالية، ٩٢-١١٠. [\[رابط\]](#)
- يعقوب، ابتهاج إسماعيل، ووهّاب، أسعد محمد علي، والفرطوسي، علي محمد حسين. (٢٠٢٢). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية. [\[رابط\]](#)
- أحمد، زهير النعيم الزين. (٢٠٢٢). أثر إدارة المخاطر على الجوانب الفنية في التأمينات العامة: دراسة ميدانية على شركات التأمين السودانية. رسالة جامعية.

ثانياً: المراجع الأجنبية

- Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. [\[Link\]](#)

- Basel Committee on Banking Supervision. (2025). Principles for the sound management of third-party risk (BCBS d605). Bank for International Settlements. [\[Link\]](#)
- 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> [\[Link\]](#)
- 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> [\[Link\]](#)
- 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> [\[Link\]](#)
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management—Integrating with strategy and performance. [\[Link\]](#)
- 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> [\[Link\]](#)
- Croignani, 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> [\[Link\]](#)
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13, 215–246. <https://doi.org/10.1007/s40685-019-0085-7> [\[Link\]](#)

- European Insurance and Occupational Pensions Authority. (2020). Guidelines on outsourcing to cloud service providers. [\[Link\]](#)
- European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. [\[Link\]](#)
- Financial Stability Board. (2023). Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities. [\[Link\]](#)
- Field, A. (2018). *Discovering statistics using IBM SPSS Statistics* (5th ed.). SAGE Publications. [\[Link\]](#)
- Gani, Z., Arifin, Z., Amran, A., & Wahab, N. A. (2023). The effect of cybersecurity practices on supply chain performance. *Industrial Management & Data Systems*, 123(3), 843–861. <https://doi.org/10.1108/IMDS-05-2022-0313> [\[Link\]](#)
- Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management*, 25(2), 223–240. <https://doi.org/10.1108/SCM-10-2018-0357> [\[Link\]](#)
- Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). Guilford Press. [\[Link\]](#)
- 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> [\[Link\]](#)
- International Association of Insurance Supervisors. (2023). Issues paper on insurance sector operational resilience. [\[Link\]](#)
- International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. [\[Link\]](#)
- International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. [\[Link\]](#)

- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security management systems—Requirements. [\[Link\]](#)
- Keskin, O. F., Caramancion, K. M., Tatar, U., & Ustun, T. S. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, 10(10), 1168. <https://doi.org/10.3390/electronics10101168> [\[Link\]](#)
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). [\[Link\]](#)
- Slapničar, S., Vidmar, T., & Tsen, E. (2025). Process theory of supplier cyber risk assessment. *Australasian Journal of Information Systems*, 29. <https://doi.org/10.3127/ajis.v29.5323> [\[Link\]](#)

الملاحق :

الملحق (١): استبانة الدراسة

مقدمة الاستبانة

المشارك الكريم/المشاركة الكريمة، تهدف هذه الاستبانة إلى دراسة أثر حوكمة مخاطر الطرف الثالث في تعزيز المرونة التشغيلية لدى شركات التأمين في المملكة العربية السعودية، مع اختبار الدور الوسيط لجاهزية الأمن السيبراني. يقصد بالطرف الثالث أي جهة خارجية تقدم خدمة أو نظامًا أو معالجة بيانات أو دعمًا يؤثر في عمليات الشركة. لا توجد إجابة صحيحة أو خاطئة؛ المطلوب تقدير الممارسة الفعلية في جهة العمل. ستستخدم البيانات لأغراض علمية، وتعرض بصورة مجمعة دون تعريف فردي.

مقياس الإجابة

١ = لا أوافق بشدة | ٢ = لا أوافق | ٣ = محايد | ٤ = أوافق | ٥ = أوافق بشدة

القسم الأول: البيانات العامة

جدول (م-١): البيانات العامة

الرمز	البيان	الخيارات
D1	جهة العمل	شركة تأمين؛ شركة إعادة تأمين؛ خدمات تأمينية؛ أخرى
D2	الإدارة/الوظيفة	المخاطر؛ الالتزام؛ تقنية المعلومات؛ الأمن السيبراني؛ العمليات؛ المطالبات؛ المراجعة؛ القانونية/التعاقدات
D3	سنوات الخبرة	أقل من ٣؛ ٣-٥؛ ٦-١٠؛ أكثر من ١٠ سنوات
D4	حجم الشركة	صغيرة؛ متوسطة؛ كبيرة
D5	مستوى التعامل مع الأطراف الثالثة	منخفض؛ متوسط؛ مرتفع

المصدر: إعداد الباحث.

القسم الثاني: حوكمة مخاطر الطرف الثالث

جدول (م-٢): فقرات حوكمة مخاطر الطرف الثالث

الرمز	البعد	العبارة
TP1	العناية الواجبة	تجري الشركة تقييمًا ماليًا وتشغيليًا وتنظيميًا للمزود قبل التعاقد.
TP2	العناية الواجبة	يتناسب عمق العناية الواجبة مع أهمية الخدمة والبيانات والمخاطر.
TP3	العقود وSLA	تحدد العقود مستويات الخدمة والمسؤوليات وحقوق الرقابة والتدقيق بوضوح.
TP4	SLA والعقود و	تتضمن العقود متطلبات الإخطار بالحوادث والاستمرارية والأطراف اللاحقة والخروج.
TP5	المراقبة المستمرة	تراقب الشركة أداء ومخاطر المزود طوال مدة العلاقة باستخدام مؤشرات محددة.
TP6	المراقبة المستمرة	تعاد مراجعة المزود عند تغير الخدمة أو الملكية أو مستوى الخطر أو وقوع حادث.
TP7	البيانات والأمن	تفرض الشركة ضوابط مناسبة للوصول للمزود إلى البيانات والأنظمة ومراجعة صلاحياته.
TP8	البيانات والأمن	تتحقق الشركة من معالجة الثغرات والحوادث السيبرانية لدى المزود ضمن أزمدة محددة.
TP9	الطوارئ والخروج	توجد خطة موثقة لاستمرار الخدمة أو التحول إلى بديل عند تعطل المزود المهم.
TP10	الطوارئ والخروج	تختبر الشركة قابلية نقل البيانات وإنهاء الوصول واستبدال المزود المهم.

المصدر: إعداد الباحث بالاستناد إلى الأطر والدراسات السابقة.

القسم الثالث: جاهزية الأمن السيبراني

جدول (م-٣): فقرات جاهزية الأمن السيبراني

الرمز	العبارة
CR1	توجد حوكمة وسياسة معتمدة لإدارة مخاطر الأمن السيبراني المرتبطة بالأطراف الثالثة.
CR2	تحدد الشركة الأصول والبيانات والخدمات الحرجة التي يصل إليها المزودون.
CR3	تطبق الشركة مبدأ أقل صلاحية ومصادقة مناسبة على حسابات المزودين.
CR4	تراقب الشركة سجلات وأحداث الوصول الخارجي وتكشف الأنشطة غير المعتادة.
CR5	توجد آلية واضحة وسريعة لتبادل معلومات الحوادث مع المزود والتصعيد الداخلي.
CR6	تنفذ الشركة تمارين مشتركة للاستجابة لحوادث تشمل مزودين مهمين.
CR7	توجد نسخ واستعادة وخيارات تشغيل تحمي الخدمة عند فقد نظام أو بيانات لدى المزود.
CR8	تراجع الشركة نتائج الحوادث والتمارين وتغلق الملاحظات ضمن مواعيد محددة.
CR9	تخضع ضوابط المزودين لتقييم أو تدقيق دوري قائم على المخاطر.
CR10	يتلقى الموظفون ومالكو العلاقات تدريباً مناسباً على مخاطر الطرف الثالث والإبلاغ.

المصدر: إعداد الباحث.

القسم الرابع: المرونة التشغيلية

جدول (م-٤): فقرات المرونة التشغيلية

الرمز	العبارة
OR1	حددت الشركة خدماتها التأمينية الحيوية والنتائج المهمة المقدمة للعملاء.
OR2	حددت الشركة حدود تحمل واضحة لمدة وحجم الأثر المقبول عند التعطل.
OR3	توجد خرائط حديثة لتبعيات الخدمات على الأشخاص والأنظمة والبيانات والمزودين.
OR4	يمكن استمرار الحد الأدنى من الخدمة عند تعطل مزود خارجي مهم.
OR5	يمكن استعادة الخدمة والبيانات ضمن الأهداف الزمنية والنقطية المحددة.
OR6	توجد آلية فعالة للتواصل مع العملاء والجهات المنظمة أثناء الاضطرابات.
OR7	اختبرت الشركة سيناريو فقد مزود مهم أو خدمة سحابية أو منصة خارجية.
OR8	تحافظ الشركة على جودة الخدمة الأساسية أثناء الاضطرابات الشديدة والمعقولة.
OR9	يمكن نقل الخدمة أو البيانات إلى بديل خلال مدة مقبولة.
OR10	تستخدم الشركة نتائج الحوادث والاختبارات لتحسين الخطط والضوابط.

المصدر: إعداد الباحث.

الملحق (٢): نموذج الموافقة المستنيرة

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

الغرض: جمع تقديرات مهنية حول ممارسات الحوكمة والجاهزية والمرونة. المشاركة طوعية، ويجوز التوقف قبل إرسال الإجابة دون أي تبعات. لا تطلب الأداة اسم المشارك أو رقم هويته، ولا ينبغي إدخال أسرار تجارية أو معلومات عميل أو تفاصيل حادث غير معلن.

تحفظ البيانات في وسيط آمن وتستخدم بصورة مجمعة للأغراض الأكاديمية، وفق موافقة لجنة الأخلاقيات وسياسة الجامعة.

بوضع علامة في خانة «أوافق»، يقر المشارك بأنه قرأ المعلومات، وأن عمره ووضعه المهني يسمحان بالمشاركة وفق شروط الدراسة، وأنه يوافق طوعاً على استخدام إجاباته المجهلة للأغراض المبينة.

الموافقة	البيان
أوافق على المشاركة ☐	☐ لا أوافق
____/____/____: التاريخ	رمز الاستبانة: _____

الملحق (٣): استمارة تحكيم الأداة

يرجى من المحكم تقدير وضوح كل فقرة وملاءمتها للبعد وسلامة صياغتها، واقتراح التعديل أو الحذف أو الإضافة. يفضل أن يمثل المحكمون إدارة المخاطر والأمن السيبراني واستمرارية الأعمال والمنهجية الكمية وقطاع التأمين.

جدول (م-٥): نموذج مختصر لتحكيم الأداة

العنصر	حكم الملاءمة	الملاحظة/الصياغة المقترحة
البعد/الفقرة 1	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	
البعد/الفقرة 2	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	
البعد/الفقرة 3	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	
البعد/الفقرة 4	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	

العنصر	حكم الملاءمة	الملاحظة/الصياغة المقترحة
البعد/الفقرة 5	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	
البعد/الفقرة 6	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	
البعد/الفقرة 7	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	
البعد/الفقرة 8	ملائمة ☐ تحتاج تعديل ☐ غير ملائمة ☐	

المصدر: إعداد الباحث.

الملحق (٤): قاموس الترميز والتحليل

جدول (م-٦): قاموس المتغيرات

الرمز	المتغير	القياس	قاعدة الاشتقاق
D1-D5	خصائص تنظيمية	فئوي اسمي/رتبي	ترميز رقمي مع الاحتفاظ بجدول القيم
TP1-TP10	حوكمة الطرف الثالث	ليكرت 5-1	متوسط الفقرات؛ الأعلى = حوكمة أقوى
CR1-CR10	الجاهزية السيبرانية	ليكرت 5-1	= متوسط الفقرات؛ الأعلى جاهزية أقوى
OR1-OR10	المرونة التشغيلية	ليكرت 5-1	متوسط الفقرات؛ الأعلى = مرونة أقوى
TP_DD	العناية الواجبة	TP1-TP2 متوسط	بعد فرعي مستقل
TP_CT	SLA العقود و	TP3-TP4 متوسط	بعد فرعي مستقل

الرمز	المتغير	القياس	قاعدة الاشتقاق
TP_MN	المراقبة	TP5-TP6 متوسط	بعد فرعي مستقل
TP_CY	البيانات والأمن	TP7-TP8 متوسط	بعد فرعي مستقل
TP_EX	الطوارئ والخروج	TP9-TP10 متوسط	بعد فرعي مستقل

المصدر: إعداد الباحث.