

بسم الله الرحمن الرحيم

جامعة ميداوثن

كلية الإدارة

تخصص إدارة المخاطر



دراسة بحثية بعنوان :

أثر إدارة مخاطر الأطراف الخارجية الرقمية في تعزيز استمرارية الأعمال
لدى المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية
(الدور الوسيط للمرونة التشغيلية الرقمية)

إعداد الطالب /

سالم علي سعد الغامدي

الرقم الجامعي /

٢٦١٠٠٢١٥٣

إشراف :

د/ فايز جراد

د/ الفيصل حسن

العام الجامعي :

٢٠٢٦ م

(١) المقدمة:

أصبحت المنشآت الحديثة تعتمد بدرجة متزايدة على أطراف خارجية رقمية في تشغيل أعمالها اليومية، فلم تعد المنشأة تعمل بمعزل عن مزودي الخدمات التقنية والسحابية وأنظمة الدفع الإلكتروني وبرامج المحاسبة ومنصات التجارة الإلكترونية وشركات التوصيل وحلول الأمن السيبراني. وقد أدى هذا الاعتماد إلى تحسين الكفاءة وتسريع العمليات وخفض التكاليف، لكنه في المقابل أوجد نوعاً جديداً من المخاطر يتمثل في مخاطر الأطراف الخارجية الرقمية.

وتزداد أهمية هذا الموضوع لدى المنشآت الصغيرة والمتوسطة، لأن هذه المنشآت غالباً ما تعتمد على حلول رقمية جاهزة ومزودين خارجيين أكثر من اعتمادها على بنية تقنية داخلية مكتملة. وفي حال تعطل مزود خدمة رئيسي، أو تعرض منصة خارجية لاختراق، أو توقف بوابة دفع، أو فشل مزود سحابي، فإن أثر ذلك قد يظهر مباشرة في المبيعات، وخدمة العملاء، والتدفقات النقدية، والسمعة، والامتثال النظامي.

وتتفق هذه الفكرة مع منطق إدارة المخاطر الحديثة، التي تؤكد أن إدارة الخطر ليست إجراءً منفصلاً، بل عملية مستمرة تشمل تحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراقبتها والتواصل بشأنها، بما يساعد المنظمة على تحقيق أهدافها وتقليل آثار عدم اليقين (ISO، ٢٠١٨).

وفي السياق السعودي، تزداد أهمية إدارة المخاطر الرقمية مع تطور البيئة التنظيمية للأمن السيبراني، حيث أصدرت الهيئة الوطنية للأمن السيبراني الضوابط الأساسية للأمن السيبراني ECC 2-2024 لتعزيز الأمن السيبراني وحماية الأصول المعلوماتية والتقنية للجهات الوطنية، كما أصدرت ضوابط خاصة بجهات القطاع الخاص، بما يعكس انتقال الموضوع من كونه مسألة تقنية إلى كونه جزءاً من الحوكمة وإدارة المخاطر واستمرارية الأعمال (الهيئة الوطنية للأمن السيبراني، ٢٠٢٤؛ الهيئة الوطنية للأمن السيبراني، ٢٠٢٥).

٢) خلفية الدراسة وسياقها:

تقوم كثير من المنشآت الصغيرة والمتوسطة اليوم على منظومة رقمية مترابطة، فقد تستخدم المنشأة نظامًا سحابيًا لإدارة المبيعات، وبوابة دفع إلكتروني لتحصيل الإيرادات، ومنصة خارجية للتسويق الرقمي، وشركة توصيل لإكمال الخدمة، وبرنامجًا محاسبيًا سحابيًا لإدارة الفواتير، ومزودًا خارجيًا للدعم التقني. وهذا يعني أن تعطل أحد هذه الأطراف قد يتحول إلى خطر تشغيلي مباشر على المنشأة.

وتوضح أدبيات مخاطر سلاسل الإمداد السيبرانية أن الاعتماد على التكنولوجيا يقوم على منظومة مترابطة ومعقدة من الموردين ومزودي الخدمات، وأن إدارة هذه المخاطر تتطلب تحديد المخاطر وتقييمها ومعالجتها عبر مستويات سلسلة الإمداد، بما يشمل المنتجات والخدمات التقنية ومزودي الأنظمة والبرمجيات والخدمات الرقمية (NIST، ٢٠٢٤).

ومن هنا، فإن الدراسة الحالية لا تنظر إلى الطرف الخارجي باعتباره "موردًا" فقط، بل بوصفه مصدرًا محتملاً للخطر التشغيلي والرقمي. فالمشكلة لا تتمثل فقط في شراء خدمة من طرف خارجي، بل في مدى قدرة المنشأة على تقييم ذلك الطرف، ووضع شروط تعاقدية واضحة، ومراقبة مستوى الخدمة، ووضع خطط بديلة عند التعطل، وضمان استمرارية الأعمال في حال وقوع خلل.

٣) مشكلة الدراسة:

تتمثل مشكلة الدراسة في أن المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية أصبحت تعتمد بدرجة متزايدة على أطراف خارجية رقمية في تشغيل أعمالها، مثل مزودي الخدمات السحابية، بوابات الدفع، منصات التجارة الإلكترونية، شركات التوصيل، وأنظمة المحاسبة السحابية. وعلى الرغم من أهمية هذه الخدمات في تحسين الكفاءة، إلا أن تعطلها أو ضعف حوكمتها قد يؤدي إلى اضطراب العمليات، وتراجع خدمة العملاء، وتعطل التحصيل، وفقدان البيانات، وضعف استمرارية الأعمال.

ومن ثم تسعى الدراسة إلى اختبار أثر إدارة مخاطر الأطراف الخارجية الرقمية في تعزيز استمرارية الأعمال، مع بحث الدور الوسيط للمرونة التشغيلية الرقمية.

(٤) أسئلة الدراسة:

ينبثق عن السؤال الرئيس الأسئلة الفرعية الآتية:

١. ما مستوى تطبيق إدارة مخاطر الأطراف الخارجية الرقمية لدى المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية؟
٢. ما مستوى المرونة التشغيلية الرقمية لدى هذه المنشآت؟
٣. ما مستوى استمرارية الأعمال لدى المنشآت الصغيرة والمتوسطة عند حدوث اضطرابات رقمية أو تشغيلية؟
٤. ما أثر إدارة مخاطر الأطراف الخارجية الرقمية في المرونة التشغيلية الرقمية؟
٥. ما أثر المرونة التشغيلية الرقمية في استمرارية الأعمال؟
٦. ما أثر إدارة مخاطر الأطراف الخارجية الرقمية في استمرارية الأعمال؟
٧. هل تتوسط المرونة التشغيلية الرقمية العلاقة بين إدارة مخاطر الأطراف الخارجية الرقمية واستمرارية الأعمال؟
٨. هل توجد فروق ذات دلالة إحصائية في استمرارية الأعمال تعزى إلى حجم المنشأة أو قطاعها أو درجة اعتمادها على الأطراف الرقمية الخارجية؟

(٥) أهداف الدراسة:

تهدف الدراسة إلى تحقيق الأهداف الآتية:

١. قياس مستوى تطبيق ممارسات إدارة مخاطر الأطراف الخارجية الرقمية في المنشآت الصغيرة والمتوسطة.
٢. تحديد مستوى المرونة التشغيلية الرقمية لدى المنشآت محل الدراسة.
٣. قياس مستوى استمرارية الأعمال في مواجهة الاضطرابات الرقمية والتشغيلية.
٤. اختبار أثر إدارة مخاطر الأطراف الخارجية الرقمية في المرونة التشغيلية الرقمية.
٥. اختبار أثر المرونة التشغيلية الرقمية في استمرارية الأعمال.

٦. اختبار الأثر المباشر لإدارة مخاطر الأطراف الخارجية الرقمية في استمرارية الأعمال.
٧. اختبار الدور الوسيط للمرونة التشغيلية الرقمية.
٨. تقديم توصيات عملية للمنشآت الصغيرة والمتوسطة تساعد على بناء إطار مبسط لإدارة مخاطر الأطراف الخارجية الرقمية.

٦ أهمية الدراسة:

أولاً: الأهمية العلمية

تنبع الأهمية العلمية للدراسة من حداثة موضوعها، إذ تجمع بين إدارة المخاطر، التحول الرقمي، الأطراف الخارجية، المرونة التشغيلية، واستمرارية الأعمال. وتختلف الدراسة عن الدراسات التقليدية في إدارة المخاطر التي تركز على المخاطر المالية أو مخاطر المشاريع أو المخاطر التأمينية، لأنها تتناول خطراً حديثاً ناتجاً عن الاعتماد المتزايد على الأطراف الرقمية الخارجية.

كما تستفيد الدراسة من معايير واتجاهات عالمية مثل ISO 31000 في إدارة المخاطر، ومن إرشادات NIST في إدارة مخاطر سلسلة الإمداد السيبرانية، ومن توجهات إدارة استمرارية الأعمال التي تؤكد أهمية الاستعداد التنظيمي والدعم الإداري والمرونة في حماية المنشآت الصغيرة والمتوسطة من الاضطرابات (ISO، ٢٠١٨؛ NIST، ٢٠٢٤؛ Ali et al.، ٢٠٢٣).

ثانياً: الأهمية التطبيقية

تفيد الدراسة ملاك ومديري المنشآت الصغيرة والمتوسطة في فهم أن التعاقد مع طرف رقمي خارجي لا ينبغي أن يكون قراراً تشغيلياً بسيطاً فقط، بل قراراً مرتبطاً بالمخاطر واستمرارية الأعمال. كما تساعد الدراسة المنشآت على تطوير آليات عملية مثل: تقييم الموردين قبل التعاقد، تصنيف الموردين حسب درجة الأهمية، متابعة مستوى الخدمة، تضمين شروط حماية البيانات، ووضع بدائل تشغيلية عند تعطل الخدمة.

(٧) حدود الدراسة:

- **الحدود الموضوعية:** تركز الدراسة على إدارة مخاطر الأطراف الخارجية الرقمية وأثرها في استمرارية الأعمال، مع اختبار الدور الوسيط للمرونة التشغيلية الرقمية.
- **الحدود البشرية:** ملاك المنشآت الصغيرة والمتوسطة، المديرون التنفيذيون، مديرو التشغيل، مديرو المالية، مسؤولو المخاطر، مسؤولو تقنية المعلومات، أو الموظفون المعنيون بالتعاقد مع مزودي الخدمات الرقمية.
- **الحدود المكانية:** المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية، مع إمكانية التركيز على مدن رئيسية مثل الرياض، جدة، الدمام، الخبر، مكة المكرمة، والمدينة المنورة.
- **الحدود الزمنية:** الفترة التي يتم فيها جمع البيانات خلال العام الدراسي الحالي.
- **الحدود التطبيقية:** تقتصر الدراسة على الأطراف الخارجية الرقمية، مثل مزودي الحوسبة السحابية، أنظمة نقاط البيع، بوابات الدفع الإلكتروني، أنظمة المحاسبة السحابية، منصات التجارة الإلكترونية، شركات التوصيل، مزودي الدعم التقني، ومزودي الأمن السيبراني.

٨) مصطلحات الدراسة وتعريفاتها الإجرائية:

المصطلح	التعريف النظري	التعريف الإجرائي في الدراسة
إدارة مخاطر الأطراف الخارجية الرقمية	عملية تحديد وتقييم ومعالجة ومراقبة المخاطر الناتجة عن الاعتماد على مزودي خدمات رقمية خارجيين.	الدرجة التي تحصل عليها المنشأة في أبعاد: حصر الأطراف الخارجية، تقييم المخاطر قبل التعاقد، الشروط التعاقدية، مراقبة الأداء، إدارة الحوادث، وخطط الخروج.
المرونة التشغيلية الرقمية	قدرة المنشأة على الاستمرار أو التعافي السريع عند حدوث اضطراب في الأنظمة أو الخدمات الرقمية.	قدرة المنشأة على توفير بدائل رقمية، سرعة التعافي، استمرار العمليات الحرجة، التواصل أثناء الأزمة، وتقليل أثر الانقطاع.
استمرارية الأعمال	قدرة المنشأة على المحافظة على أنشطتها الأساسية أثناء الاضطرابات وبعدها.	قدرة المنشأة على استمرار المبيعات، خدمة العملاء، معالجة المدفوعات، حماية البيانات، واستعادة العمليات بعد التعطل.
المنشآت الصغيرة والمتوسطة	منشآت تقع ضمن التصنيف المعتمد للمنشآت الصغيرة والمتوسطة في المملكة.	المنشآت التي تنطبق عليها معايير عدد العاملين أو الإيرادات وفق تصنيف "منشآت"

٩) الإطار النظري للدراسة :

يقوم الإطار النظري للدراسة على أربعة مداخل رئيسية:

1. مدخل إدارة المخاطر المؤسسية:

ينطلق هذا المدخل من أن الخطر ينبغي أن يدار ضمن منظومة متكاملة تشمل تحديد الخطر، تحليله، تقييمه، معالجته، مراقبته، والتواصل بشأنه. ويعد معيار ISO 31000 من

أهم المعايير الدولية التي تقدم مبادئ وإرشادات عامة لإدارة المخاطر في مختلف المنظمات بغض النظر عن حجمها أو قطاعها (ISO، ٢٠١٨).

2. مدخل مخاطر الأطراف الخارجية:

يركز هذا المدخل على أن المنشأة لا تتعرض فقط لمخاطر داخلية، بل تتأثر أيضاً بالمخاطر المرتبطة بالموردين ومزودي الخدمات والشركاء الخارجيين. وفي البيئة الرقمية، قد يكون الطرف الخارجي هو مزود خدمة سحابية أو منصة دفع أو شركة تقنية، ولذلك يصبح تقييم هذا الطرف ومراقبته جزءاً من منظومة إدارة المخاطر.

3. مدخل المرونة التشغيلية:

تعني المرونة التشغيلية قدرة المنشأة على امتصاص الصدمات والتكيف معها والتعافي منها. وفي حالة المنشآت الصغيرة والمتوسطة، ترتبط المرونة التشغيلية بوجود خطط بديلة، وتحديد العمليات الحرجة، وتوافر قنوات اتصال وقت الأزمة، والقدرة على استعادة الخدمة بسرعة. وتشير مراجعات أدبيات استمرارية الأعمال إلى أن دعم الإدارة، والاستعداد التنظيمي، وتضمين ممارسات الاستمرارية من العوامل المهمة لحماية المنشآت الصغيرة والمتوسطة من الأزمات والاضطرابات (Ali et al، ٢٠٢٣).

4. مدخل الحوكمة السيبرانية والتنظيمية:

في المملكة، لم تعد إدارة المخاطر الرقمية مسألة اختيارية تماماً، بل أصبحت مرتبطة بالحوكمة والامتثال وحماية الأصول التقنية. وتوضح أدوات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني أنها تشمل سياسات ومعايير وإجراءات ووثائق حوكمة تستهدف تمكين الجهات من رفع كفاءة الأمن السيبراني وتعزيز الجاهزية والحد من المخاطر المتجددة (الهيئة الوطنية للأمن السيبراني، ٢٠٢٢).

(١٠) متغيرات الدراسة وأبعادها:

المتغير المستقل: إدارة مخاطر الأطراف الخارجية الرقمية

البعد	المقصود به	مثال تطبيقي
حصر وتصنيف الأطراف الخارجية	معرفة كل مزود خارجي تعتمد عليه المنشأة وتصنيفه حسب الأهمية	تصنيف بوابة الدفع كمزود حرج لأنها مرتبطة بالإيرادات
تقييم المخاطر قبل التعاقد	دراسة مخاطر الطرف الخارجي قبل توقيع العقد	مراجعة مستوى الحماية وخطط التعافي لدى مزود الخدمة
الحوكمة والشروط التعاقدية	تضمين العقود شروط مستوى الخدمة وحماية البيانات والمسؤوليات	وجود شرط يحدد مدة الاستجابة عند التعطل
المراقبة المستمرة	متابعة أداء الطرف الخارجي بعد التعاقد	قياس تكرار الأعطال أو التأخر في الدعم
إدارة الحوادث	وجود إجراءات للتعامل مع خلل الطرف الخارجي	آلية تصعيد عند توقف المنصة
خطط الخروج والبدائل	وجود بديل أو خطة انتقال عند فشل المزود	مزود دفع بديل أو نسخة احتياطية للبيانات

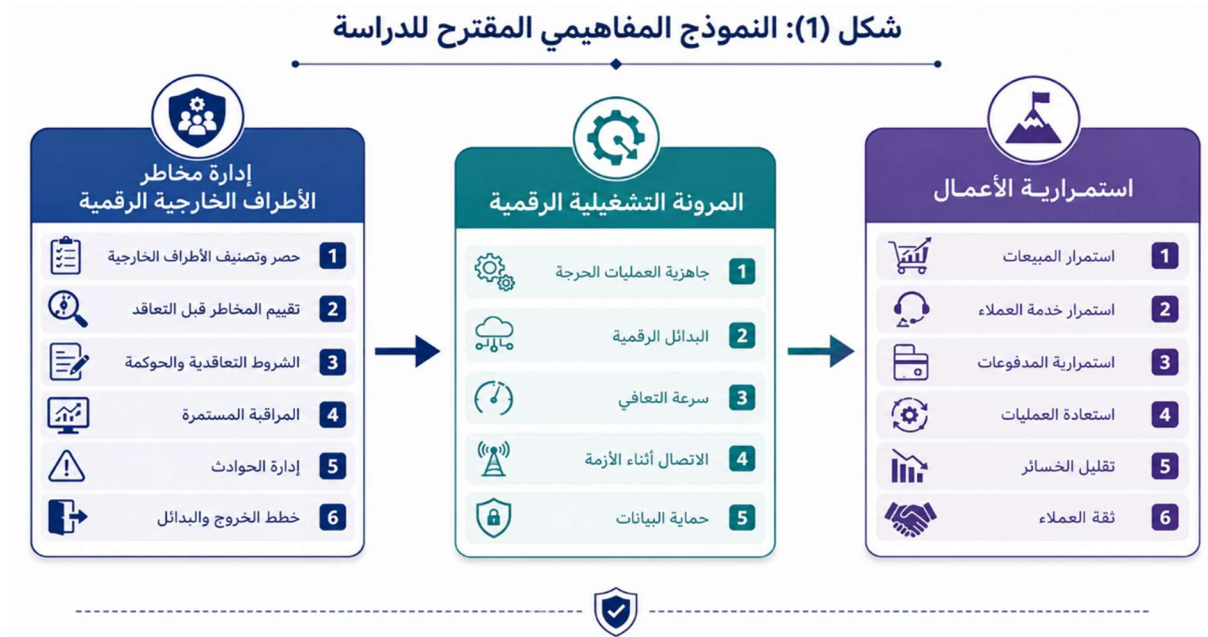
المتغير الوسيط: المرونة التشغيلية الرقمية

البعد	المقصود به
جاهزية العمليات الحرجة	تحديد العمليات التي لا يمكن توقفها
البدائل الرقمية	وجود بدائل للأنظمة أو المزودين الحرجين
سرعة التعافي	القدرة على استعادة الخدمة خلال وقت مقبول
الاتصال أثناء الأزمة	وجود آلية تواصل داخلي وخارجي عند التعطل
حماية البيانات	ضمان استعادة البيانات وعدم فقدانها
التعلم من الحوادث	تحسين الإجراءات بعد كل حادث أو تعطل

المتغير التابع: استمرارية الأعمال

المؤشر	البعد
انخفاض توقف البيع عند تعطل مزود خارجي	استمرار المبيعات
قدرة المنشأة على التواصل وخدمة العملاء وقت الأزمة	استمرار خدمة العملاء
توفر بدائل للتحصيل والدفع	استمرارية المدفوعات
سرعة العودة إلى الوضع الطبيعي	استعادة العمليات
الحد من الخسائر المالية والتشغيلية	تقليل الخسائر
المحافظة على ثقة العملاء أثناء الاضطراب	ثقة العملاء

١١) النموذج المفاهيمي للدراسة:



تفسير النموذج:

يفترض النموذج أن المنشآت التي تطبق ممارسات أكثر نضجاً في إدارة مخاطر الأطراف الخارجية الرقمية تكون أكثر قدرة على بناء مرونة تشغيلية رقمية. وهذه المرونة تساعد على الاستمرار عند حدوث اضطراب، وتقليل أثر الانقطاع، وتسريع العودة إلى الوضع الطبيعي.

كما يفترض النموذج وجود أثر مباشر لإدارة مخاطر الأطراف الخارجية الرقمية في استمرارية الأعمال، وأثر غير مباشر من خلال المرونة التشغيلية الرقمية.

(١٢) فرضيات الدراسة:

رقم الفرضية	نص الفرضية
H1	توجد علاقة أثر ذات دلالة إحصائية بين إدارة مخاطر الأطراف الخارجية الرقمية والمرونة التشغيلية الرقمية لدى المنشآت الصغيرة والمتوسطة.
H2	توجد علاقة أثر ذات دلالة إحصائية بين المرونة التشغيلية الرقمية واستمرارية الأعمال.
H3	توجد علاقة أثر ذات دلالة إحصائية بين إدارة مخاطر الأطراف الخارجية الرقمية واستمرارية الأعمال.
H4	تختلف أبعاد إدارة مخاطر الأطراف الخارجية الرقمية في درجة تأثيرها على استمرارية الأعمال.
H5	تتوسط المرونة التشغيلية الرقمية العلاقة بين إدارة مخاطر الأطراف الخارجية الرقمية واستمرارية الأعمال.
H6	توجد فروق ذات دلالة إحصائية في استمرارية الأعمال تعزى إلى حجم المنشأة أو قطاعها أو درجة اعتمادها على الخدمات الرقمية الخارجية.

(١٣) الدراسات والمصادر العربية ذات الصلة:

المصدر/الدراسة	المجال	أبرز ما يرتبط بالدراسة الحالية
الهيئة الوطنية للأمن السيبراني، ٢٠٢٥	ضوابط الأمن السيبراني للقطاع الخاص	تؤكد أهمية الحد من المخاطر السيبرانية وحماية المعلومات والأصول التقنية للقطاع الخاص، وتتضمن محورًا متعلقًا بالأطراف الخارجية.
الهيئة الوطنية للأمن السيبراني، ٢٠٢٤	الضوابط الأساسية للأمن السيبراني ECC 2-2024	تؤكد حماية الأصول المعلوماتية والتقنية وتعزيز الأمن السيبراني على المستوى الوطني.
الهيئة الوطنية للأمن السيبراني، ٢٠٢٢	أدوات الأمن السيبراني	تقدم نماذج سياسات ومعايير وإجراءات ووثائق حوكمة تساعد الجهات على رفع الجاهزية والحد من المخاطر.
منشآت، ٢٠٢٣	دعم وتطوير المنشآت الصغيرة والمتوسطة	تؤكد أهمية قطاع المنشآت الصغيرة والمتوسطة ودوره في تحقيق مستهدفات رؤية ٢٠٣٠.
بارشيد، ٢٠٢٥	أثر الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات الحاسوبية	تبرز العلاقة بين الأمن السيبراني والحد من مخاطر نظم المعلومات في البيئة السعودية.

التعليق على المصادر العربية:

توضح المصادر العربية أن البيئة التنظيمية السعودية أصبحت أكثر اهتمامًا بإدارة المخاطر الرقمية، وحوكمة الأمن السيبراني، وحماية الأصول التقنية، ودعم المنشآت الصغيرة والمتوسطة. إلا أن معظم هذه المصادر لا تختبر بصورة مباشرة العلاقة بين إدارة مخاطر

الأطراف الخارجية الرقمية واستمرارية الأعمال لدى المنشآت الصغيرة والمتوسطة، وهذا ما تسعى الدراسة الحالية إلى معالجته.

(١٤) الدراسات والمصادر الأجنبية ذات الصلة:

المصدر/الدراسة	المجال	أبرز ما يرتبط بالدراسة الحالية
ISO، ٢٠١٨	إدارة المخاطر	يقدم إطارًا عامًا لإدارة المخاطر يشمل التحديد والتحليل والتقييم والمعالجة والمراقبة.
NIST، ٢٠٢٤	إدارة مخاطر سلسلة الإمداد السيبرانية	يوضح أن إدارة مخاطر سلسلة الإمداد السيبرانية عملية منهجية لإدارة التعرض للمخاطر عبر الموردين ومزودي المنتجات والخدمات التقنية.
Ali et al.، ٢٠٢٣	استمرارية الأعمال لدى SMEs	تؤكد أن دعم الإدارة والاستعداد التنظيمي وتضمين ممارسات الاستمرارية عوامل مهمة في حماية المنشآت الصغيرة والمتوسطة من الاضطرابات.
COSO، ٢٠١٧	إدارة المخاطر المؤسسية	يربط إدارة المخاطر بالاستراتيجية والأداء والحوكمة.
NIST CSF 2.0، ٢٠٢٤	إطار الأمن السيبراني	يدعم دمج إدارة المخاطر السيبرانية ضمن الحوكمة وإدارة سلسلة الإمداد.

التعليق على الدراسات الأجنبية:

تركز الدراسات والأطر الأجنبية على أن المخاطر الرقمية لم تعد محصورة داخل المنظمة، بل تمتد إلى الموردين ومزودي الخدمات وسلاسل الإمداد الرقمية. وتستفيد الدراسة الحالية من هذه الأدبيات في بناء نموذج يربط بين إدارة مخاطر الأطراف الخارجية، والمرونة التشغيلية، واستمرارية الأعمال.

(١٥) الفجوة البحثية:

تتمثل الفجوة البحثية في أن كثيراً من الدراسات تناولت إدارة المخاطر بوجه عام، أو الأمن السيبراني، أو استمرارية الأعمال، بينما لا تزال العلاقة بين إدارة مخاطر الأطراف الخارجية الرقمية واستمرارية الأعمال لدى المنشآت الصغيرة والمتوسطة في البيئة السعودية بحاجة إلى دراسة ميدانية واضحة.

المحور	ما تناولته الدراسات السابقة	ما تضيفه الدراسة الحالية
إدارة المخاطر	ركزت على المخاطر العامة أو المالية أو مخاطر المشاريع	تركز على مخاطر الأطراف الخارجية الرقمية
الأمن السيبراني	تناول الحماية والامتثال والضوابط	تربط الأمن والحوكمة باستمرارية الأعمال
المنشآت الصغيرة والمتوسطة	درست التحديات والتمويل والتحول الرقمي	تدرس قدرة SMEs على إدارة مخاطر مزودي الخدمات الرقمية
استمرارية الأعمال	ركزت على الاستعداد للأزمات	تختبر أثر إدارة مخاطر الأطراف الخارجية في الاستمرارية
النموذج التحليلي	غالبًا علاقات مباشرة	تضيف متغيراً وسيطاً: المرونة التشغيلية الرقمية

(١٦) منهجية الدراسة:

- منهج الدراسة: تعتمد الدراسة على المنهج الوصفي التحليلي، لأنه الأنسب لوصف واقع إدارة مخاطر الأطراف الخارجية الرقمية، وقياس مستوى المرونة التشغيلية الرقمية، وتحليل أثر هذه المتغيرات في استمرارية الأعمال.
- مجتمع الدراسة: يتكون مجتمع الدراسة من المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية التي تستخدم خدمات رقمية خارجية في أنشطتها التشغيلية أو المالية أو التسويقية أو التقنية.

○ عينة الدراسة : يقترح أن تتكون العينة من 250 إلى ٣٥٠ مفردة من ملاك ومديري ومسؤولي المنشآت الصغيرة والمتوسطة. ويمكن استخدام العينة القصدية المنظمة أو العينة الطبقية حسب القطاع.

القطاعات المقترحة للتطبيق

القطاع	أمثلة على الأطراف الخارجية الرقمية
التجارة الإلكترونية	منصات المتاجر، بوابات الدفع، شركات الشحن
المطاعم والمقاهي	تطبيقات الطلبات، منصات التوصيل، نقاط البيع
الخدمات المهنية	أنظمة المحاسبة السحابية، إدارة العملاء، التوقيع الإلكتروني
الخدمات اللوجستية	أنظمة التتبع، إدارة المخزون، مزودو الخرائط
التجزئة	نقاط البيع، برامج الولاء، الدفع الإلكتروني
المنشآت التقنية الصغيرة	مزودو الاستضافة، الحوسبة السحابية، أدوات التطوير

(١٧) أداة الدراسة المقترحة:

تعتمد الدراسة على استبانة مكونة من خمسة أقسام:

القسم الأول: البيانات العامة

حجم المنشأة، القطاع، المدينة، عدد سنوات النشاط، عدد العاملين، نوع الخدمات الرقمية المستخدمة، درجة الاعتماد على أطراف خارجية، وجود مسؤول مخاطر أو تقنية معلومات.

القسم الثاني: إدارة مخاطر الأطراف الخارجية الرقمية

أمثلة لعبارات الاستبانة:

البعد	العبارة المقترحة
الحصر والتصنيف	تمتلك المنشأة قائمة واضحة بالأطراف الخارجية الرقمية التي تعتمد عليها.
تقييم المخاطر	تقوم المنشأة بتقييم مخاطر مزود الخدمة قبل التعاقد معه.
الشروط التعاقدية	تتضمن العقود شروطاً واضحة لمستوى الخدمة وحماية البيانات.
المراقبة المستمرة	تتابع المنشأة أداء مزودي الخدمات الرقمية بانتظام.
إدارة الحوادث	توجد إجراءات واضحة للتعامل مع تعطل مزود خارجي رقمي.
البدائل والخروج	تمتلك المنشأة بدائل أو خطط انتقال عند فشل مزود رئيسي.

القسم الثالث: المرونة التشغيلية الرقمية

البعد	العبارة المقترحة
جاهزية العمليات	تحدد المنشأة العمليات الرقمية الأكثر أهمية لاستمرار أعمالها.
البدائل	تمتلك المنشأة بدائل تشغيلية عند تعطل أحد الأنظمة الرقمية.
سرعة التعافي	تستطيع المنشأة استعادة خدماتها الرقمية خلال وقت مناسب.
الاتصال وقت الأزمة	توجد آلية تواصل واضحة مع الموظفين والعملاء عند حدوث تعطل.
حماية البيانات	تحتفظ المنشأة بنسخ احتياطية أو حلول لاستعادة البيانات.

القسم الرابع: استمرارية الأعمال

البعد	العبارة المقترحة
استمرار المبيعات	تستطيع المنشأة مواصلة البيع عند حدوث تعطل رقمي محدود.
خدمة العملاء	تستطيع المنشأة خدمة العملاء أثناء اضطرابات الأنظمة الرقمية.
المدفوعات	تمتلك المنشأة بدائل لتحصيل المدفوعات عند تعطل بوابة الدفع.
تقليل الخسائر	تساعد إجراءات إدارة المخاطر في تقليل الخسائر الناتجة عن التعطل.
ثقة العملاء	تحافظ المنشأة على ثقة العملاء عند حدوث خلل في الخدمات الرقمية.

القسم الخامس: سؤال مفتوح

ما أبرز المخاطر التي تواجه منشأتك عند الاعتماد على أطراف خارجية رقمية؟

(١٨ أساليب التحليل الإحصائي:

سيتم تحليل البيانات باستخدام برنامج SPSS ، ويمكن استخدام SmartPLS أو AMOS في حال اختبار النموذج البنائي كاملاً.

الهدف التحليلي	الاختبار الإحصائي المقترح
وصف خصائص العينة	التكرارات والنسب المئوية
قياس مستوى المتغيرات	المتوسطات الحسابية والانحرافات المعيارية
اختبار ثبات الأداة	معامل كرونباخ ألفا
اختبار العلاقة بين المتغيرات	معامل ارتباط بيرسون
اختبار الأثر المباشر	الانحدار الخطي البسيط والمتعدد
اختبار الدور الوسيط	تحليل الوساطة باستخدام Bootstrap
اختبار الفروق	اختبار T-test وتحليل التباين ANOVA
اختبار جودة النموذج	SmartPLS أو AMOS عند توافر حجم عينة مناسب

معايير الحكم على المتوسطات

المتوسط الحسابي	مستوى التطبيق
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

(١٩) هيكل الرسالة المتوقع:

الفصل الأول: الإطار العام للدراسة

المقدمة، مشكلة الدراسة، الأسئلة، الأهداف، الأهمية، الحدود، المصطلحات، النموذج، الفرضيات.

الفصل الثاني: الإطار النظري والدراسات السابقة

إدارة المخاطر، مخاطر الأطراف الخارجية، المخاطر الرقمية، المرونة التشغيلية، استمرارية الأعمال، الدراسات السابقة، الفجوة البحثية.

الفصل الثالث: منهجية الدراسة

المنهج، المجتمع، العينة، أداة الدراسة، الصدق والثبات، إجراءات جمع البيانات، أساليب التحليل.

الفصل الرابع: عرض النتائج وتحليلها

وصف العينة، تحليل المتغيرات، اختبار الفرضيات، اختبار الدور الوسيط.

الفصل الخامس: المناقشة والتوصيات

مناقشة النتائج، الاستنتاجات، التوصيات التطبيقية، المقترحات البحثية المستقبلية.

٢٠) القيمة العلمية المتوقعة للدراسة:

تقدم الدراسة نموذجًا بحثيًا حديثًا يمكن أن يضيف إلى أدبيات إدارة المخاطر في البيئة العربية والسعودية، لأنها تنقل موضوع إدارة المخاطر من التركيز التقليدي على المخاطر المالية أو التأمينية إلى التركيز على المخاطر الرقمية الممتدة خارج حدود المنشأة. كما أنها تربط بين إدارة مخاطر الأطراف الخارجية واستمرارية الأعمال من خلال متغير وسيط مهم هو المرونة التشغيلية الرقمية.

٢١) القيمة التطبيقية المتوقعة للدراسة:

يمكن أن تساعد نتائج الدراسة المنشآت الصغيرة والمتوسطة على بناء ممارسات عملية مثل:

١. إعداد سجل للأطراف الخارجية الرقمية.
٢. تصنيف الموردين حسب درجة الأهمية والخطورة.
٣. تقييم مزودي الخدمة قبل التعاقد.
٤. تضمين شروط واضحة لمستوى الخدمة وحماية البيانات.
٥. وضع خطط بديلة عند تعطل مزود حرج.
٦. اختبار جاهزية المنشأة لاستمرار الأعمال عند حدوث اضطراب.
٧. تحسين التواصل مع العملاء والموظفين أثناء الأزمات.

قائمة بالمراجع الأولية :

أولاً: المراجع العربية

١. الهيئة الوطنية للأمن السيبراني. (2025). ضوابط الأمن السيبراني لجهات القطاع الخاص من غير ذوات البنى التحتية الحساسة.
٢. الهيئة الوطنية للأمن السيبراني. (2024). الضوابط الأساسية للأمن السيبراني ECC 2-2024.
٣. الهيئة الوطنية للأمن السيبراني. (2022). أدوات الأمن السيبراني: سياسات، معايير، إجراءات، وثائق حوكمة.
٤. الهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت". (2023). "نبذة عن منشآت ودورها في دعم قطاع المنشآت الصغيرة والمتوسطة.
٥. بارشيد، ناهد عبدالله. (2025). أثر الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية: دراسة ميدانية على القطاعات الحكومية في المملكة العربية السعودية.
٦. هيئة الحكومة الرقمية. الأدلة والسياسات ذات الصلة بالتحول الرقمي والخدمات الرقمية.
٧. الهيئة السعودية للبيانات والذكاء الاصطناعي. نظام حماية البيانات الشخصية ولوائحه التنفيذية.

ثانيًا: المراجع الأجنبية

1. ISO. (2018). **ISO 31000:2018 Risk Management — Guidelines.**
2. NIST. (2024). **NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management.**
3. COSO. (2017). **Enterprise Risk Management—Integrating with Strategy and Performance.**
4. Ali, Q. S. A., et al. (2023). **Systematic Literature Review of Business Continuity Management Practices: Integrating Organisational Resilience and Performance in SMEs BCM Framework.**
5. NIST. (2024). **The NIST Cybersecurity Framework 2.0.**
6. IEC. (2019). **IEC 31010:2019 Risk Management — Risk Assessment Techniques.**