

خطة بحث ماجستير

أثر ممارسات إدارة المخاطر السيبرانية على استمرارية الأعمال في منشآت القطاع الخاص المنتسبة لغرفة الأحساء بالمنطقة الشرقية - المملكة العربية السعودية

إعداد الطالب:

عبدالرحمن عبدالعزيز القرينيس

الرقم الجامعي:

262000022

إشراف :

البروفيسور /فايز علي جراد

الدكتور/الفیصل عبد الحمید محمد

أولاً : المقدمة

يشهد العالم المعاصر تحولاً رقمياً غير مسبوق ، أسهم في إعادة تشكيل بيئة الأعمال وطبيعة العمليات التشغيلية في المنشآت على اختلاف أحجامها وقطاعاتها. وقد ترتب على هذا التحول المتسارع زيادة هائلة في الاعتماد على البنى التحتية لتكنولوجيا المعلومات والشبكات الرقمية، مما جعل المنشآت أكثر عرضة للتهديدات السيبرانية المتنامية من حيث الحجم والتعقيد. ففي ظل انتشار الهجمات الإلكترونية التي تستهدف سرقة البيانات، وابتزاز المنشآت، وتعطيل العمليات الحيوية، بات الأمن السيبراني أحد أبرز التحديات الاستراتيجية التي تواجهها المنشآت في العصر الرقمي.

وتكتسب منشآت القطاع الخاص في المملكة العربية السعودية أهمية خاصة في هذا السياق؛ إذ تمثل ركيزة أساسية للاقتصاد الوطني، وتسهم بشكل فعال في تحقيق مستهدفات رؤية المملكة 2030 من خلال تنويع مصادر الدخل، وخلق فرص العمل، وتعزيز التنافسية الاقتصادية. غير أن هذه المنشآت، وخاصة الصغيرة والمتوسطة منها، غالباً ما تفتقر إلى القدرات المالية والبشرية اللازمة لمواجهة التهديدات السيبرانية المتطورة، مما يجعلها هدفاً سهلاً للهجمات الإلكترونية التي قد تؤدي إلى توقف الأعمال، وفقدان البيانات الحساسة، والإضرار بالسمعة، بل وقد تهدد استمرارية المنشأة ذاتها (العراي وأبو عنزه، 2024).

وفي هذا الإطار، استشعرت الجهات التنظيمية في المملكة حجم التحديات التي تواجه منشآت القطاع الخاص، فأصدرت الهيئة الوطنية للأمن السيبراني (NCA) الضوابط السيبرانية لمنشآت القطاع الخاص غير البنية التحتية الوطنية الحرجة (NCNICC-1:2025) ، التي تهدف إلى وضع إطار تنظيمي واضح يلزم منشآت القطاع الخاص بتطبيق الحد الأدنى من المتطلبات السيبرانية، بما يتناسب مع حجم كل منشأة وطبيعة نشاطها. وتشمل هذه الضوابط متطلبات متكاملة تتعلق بالحوكمة، والدفاع السيبراني، والمرونة التشغيلية، ومن أبرز غاياتها تعزيز قدرة المنشآت على ضمان استمرارية أعمالها في مواجهة المخاطر السيبرانية.

وتبرز منطقة الأحساء بوصفها إحدى المناطق الاقتصادية الواعدة في المملكة، بما تضمه من تنوع في الأنشطة التجارية والصناعية والخدمية، وما تقدمه غرفة الأحساء من دور محوري في دعم وتطوير قطاع الأعمال المحلي. إلا أنه، وبالرغم من الأهمية المتزايدة للأمن السيبراني، لا تزال هناك فجوة معرفية واضحة حول واقع ممارسات إدارة المخاطر السيبرانية في منشآت القطاع الخاص في هذه المنطقة، ومدى التزامها بالضوابط التنظيمية الصادرة، وتأثير هذه الممارسات على استمرارية أعمالها. ومن ثم، تأتي هذه الدراسة لسد هذه الفجوة من خلال تقديم تحليل كمي للعلاقة بين ممارسات إدارة المخاطر السيبرانية واستمرارية الأعمال، مع التركيز على السياق المحلي لمنطقة الأحساء.

ثانياً : مشكلة البحث

تُعد استمرارية الأعمال من القضايا المصيرية التي تواجه منشآت القطاع الخاص، خاصة في ظل تزايد وتيرة الهجمات السيبرانية وتطور أساليبها باستمرار. فالهجمات الإلكترونية لم تعد تقتصر على المنشآت الكبرى، بل باتت تستهدف المنشآت الصغيرة والمتوسطة بشكل متزايد، نظراً لما تمثله من حلقة ضعف في سلسلة التوريد الرقمية، وما توفره من فرص للمهاجمين لاختراق أنظمة ذات حماية أقل. وقد أشارت الدراسات إلى أن أكثر من 60% من المنشآت الصغيرة والمتوسطة التي تتعرض لهجمة سيبرانية حادة تفشل في استعادة نشاطها خلال ستة أشهر من وقوع الحادث (Kaspersky, 2021).

ورغم صدور الضوابط السيبرانية الملزمة من الهيئة الوطنية للأمن السيبراني، وتزايد الوعي العام بمخاطر الأمن السيبراني، إلا أن هناك شحاً في الدراسات التطبيقية التي تقيس مستوى تطبيق ممارسات إدارة المخاطر السيبرانية في منشآت القطاع الخاص في منطقة الأحساء، وتقييم أثر هذه الممارسات على استمرارية الأعمال. وتتجلى مشكلة البحث في التساؤلات الرئيسة التالية:

السؤال الرئيس: ما أثر ممارسات إدارة المخاطر السيبرانية (تحديد المخاطر، تقييمها، معالجتها، مراقبتها) على استمرارية الأعمال (الجاهزية، الاستجابة، التعافي، التكيف) في منشآت القطاع الخاص المنتسبة لغرفة الأحساء بالمنطقة الشرقية؟

الأسئلة الفرعية:

- 1- ما مستوى تطبيق ممارسات إدارة المخاطر السيبرانية في منشآت القطاع الخاص المنتسبة لغرفة الأحساء؟
- 2- ما مستوى استمرارية الأعمال في تلك المنشآت؟
- 3- هل توجد علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر السيبرانية بأبعادها المختلفة واستمرارية الأعمال؟
- 4- ما أثر كل بعد من أبعاد ممارسات إدارة المخاطر السيبرانية على استمرارية الأعمال؟
- 5- هل توجد فروق ذات دلالة إحصائية في مستوى ممارسات إدارة المخاطر السيبرانية واستمرارية الأعمال تُعزى إلى خصائص المنشأة (الحجم، القطاع الاقتصادي)؟

ثالثاً : أهداف البحث

المهدف الرئيس :

التعرف على أثر ممارسات إدارة المخاطر السيبرانية بأبعادها (تحديد المخاطر، تقييمها، معالجتها، مراقبتها) على استمرارية الأعمال بأبعادها (الجاهزية، الاستجابة، التعافي، التكيف) في منشآت القطاع الخاص المنتسبة لغرفة الأحساء بالمنطقة الشرقية.

الأهداف الفرعية :

- 1-تحديد مستوى تطبيق ممارسات إدارة المخاطر السيبرانية في منشآت القطاع الخاص المنتسبة لغرفة الأحساء.
- 2-تحديد مستوى استمرارية الأعمال في منشآت القطاع الخاص المنتسبة لغرفة الأحساء.
- 3-اختبار وجود علاقة ارتباطية ذات دلالة إحصائية بين ممارسات إدارة المخاطر السيبرانية (كلاً منها على حدة ومجموعة) واستمرارية الأعمال.
- 4-قياس أثر أبعاد إدارة المخاطر السيبرانية (تحديد المخاطر، تقييمها، معالجتها، مراقبتها) على استمرارية الأعمال (الجاهزية، الاستجابة، التعافي، التكيف).
- 5-اختبار وجود فروق ذات دلالة إحصائية في استجابات أفراد العينة تُعزى إلى خصائص المنشأة (الحجم، القطاع الاقتصادي).
- 6-تقديم توصيات عملية قابلة للتطبيق لتعزيز ممارسات إدارة المخاطر السيبرانية في منشآت القطاع الخاص، بما يسهم في تحسين استمرارية أعمالها وزيادة مرونتها التنظيمية.

رابعاً: أهمية البحث

أولاً: الأهمية النظرية

- 1-إثراء المكتبة العلمية العربية: تسهم هذه الدراسة في سد الفجوة البحثية القائمة في مجال إدارة المخاطر السيبرانية واستمرارية الأعمال في سياق منشآت القطاع الخاص، خاصة في منطقة الأحساء والمملكة العربية السعودية. وتعد هذه الدراسة من الدراسات الرائدة التي تجمع بين المتغيرين في بيئة الأعمال السعودية.

2-تطوير الإطار النظري: تقدم الدراسة نموذجاً مفاهيمياً متكاملًا يربط بين ممارسات إدارة المخاطر السيبرانية (المتثلة في أربعة أبعاد رئيسية: تحديد المخاطر، تقييمها، معالجتها، مراقبتها) واستمرارية الأعمال (المتثلة في أربعة أبعاد رئيسية: الجاهزية، الاستجابة، التعافي، التكيف)، وذلك استناداً إلى أدبيات معترف بها دولياً مثل ISO 31000 وإطار عمل NIST ، بالإضافة إلى الضوابط السيبرانية الصادرة عن الهيئة الوطنية للأمن السيبراني.

3-اختبار النماذج النظرية: تختبر الدراسة صحة النماذج النظرية المقترحة في بيئة الأعمال السعودية، مما يوفر أرضية صلبة لدراسات مستقبلية، ويسهم في تعزيز الفهم الأكاديمي للعلاقة بين إدارة المخاطر السيبرانية واستمرارية الأعمال في سياق المنشآت الصغيرة والمتوسطة.

4-استكشاف متغيرات ديموغرافية: تسهم الدراسة في التعرف على أثر خصائص المنشآت (الحجم، القطاع الاقتصادي) في مستوى ممارسات إدارة المخاطر السيبرانية واستمرارية الأعمال، مما يثري المعرفة حول دور هذه الخصائص في تشكيل الاستراتيجيات السيبرانية.

ثانياً: الأهمية التطبيقية

1-دعم صنع القرار: تقديم رؤى عملية قائمة على الأدلة حول واقع ممارسات إدارة المخاطر السيبرانية في منشآت القطاع الخاص، مما يساعد صنع القرار في غرفة الأحساء والهيئة الوطنية للأمن السيبراني والجهات المعنية على تطوير برامج دعم فعالة ومناسبة لاحتياجات المنشآت في المنطقة.

2-تعزيز الامتثال التنظيمي: تساعد نتائج الدراسة منشآت القطاع الخاص في فهم متطلبات الضوابط السيبرانية الصادرة عن الهيئة الوطنية للأمن السيبراني (NCNICC-1:2025) ، وتحديد الفجوات بين ممارساتها الحالية والمتطلبات التنظيمية، مما يعزز قدرتها على الامتثال وتجنب المخاطر القانونية والمالية المترتبة على عدم الامتثال.

3-تحسين استمرارية الأعمال: تقديم توصيات عملية يمكن للمنشآت تطبيقها لتعزيز قدرتها على مواجهة التهديدات السيبرانية، وضمان استمرارية أعمالها في حال وقوع حوادث سيبرانية، مما يقلل من احتمالية التوقف التشغيلي والخسائر المالية الناتجة عنه.

4-دعم الاقتصاد المحلي: من خلال تعزيز مرونة منشآت القطاع الخاص في مواجهة المخاطر السيبرانية، تسهم الدراسة في دعم الاستقرار الاقتصادي لمنطقة الأحساء وتعزيز تنافسية منشآتها في السوق المحلي والإقليمي.

5-توجيه السياسات: تقدم الدراسة رؤى يمكن أن تستفيد منها غرفة الأحساء في تصميم برامج توعوية وتدريبية وخدمات استشارية تهدف إلى رفع مستوى النضج السيبراني لمنشآتها المنتسبة.

خامساً : حدود البحث

1-الحدود المكانية: تقتصر الدراسة على منشآت القطاع الخاص المنتسبة لغرفة الأحساء بالمنطقة الشرقية من المملكة العربية السعودية، ولا تمتد إلى منشآت القطاع العام، أو المنشآت غير المنتسبة للغرفة.

2-الحدود الزمانية: تُجرى الدراسة خلال الفصلين الدراسيين الأول والثاني من العام الجامعي [تحديد العام الدراسي]، وتعكس البيانات المجمعة واقع الممارسات خلال هذه الفترة الزمنية المحددة.

3-الحدود الموضوعية: تركز الدراسة على أربعة أبعاد لممارسات إدارة المخاطر السيبرانية (تحديد المخاطر، تقييمها، معالجتها، مراقبتها) وأربعة أبعاد لاستمرارية الأعمال (الجاهزية، الاستجابة، التعافي، التكيف)، ولا تتناول جوانب أخرى قد تكون ذات صلة مثل الجوانب القانونية أو التأمينية للأمن السيبراني.

4-الحدود البشرية: تستهدف الدراسة المدراء التنفيذيين، ومدراء تكنولوجيا المعلومات، ومسؤولي الأمن السيبراني في المنشآت المستهدفة، وقد لا تشمل وجهات نظر جميع الموظفين أو الأطراف الخارجية المتعاملة مع المنشآت.

5-الحدود المنهجية:

تعتمد الدراسة على المنهج الوصفي التحليلي والكمي، باستخدام الاستبيان كأداة رئيسية لجمع البيانات، مما قد يحد من عمق المعلومات مقارنة بالمنهج النوعية مثل المقابلات المتعمقة. ومع ذلك، سيتم تضمين بعض الأسئلة المفتوحة في الاستبيان للتعويض جزئياً عن هذا القيد.

يعتمد قياس "استمرارية الأعمال" و"الجاهزية" على **التقييم الذاتي** للمدراء ومسؤولي المنشآت، وهو ما قد يعيل أحياناً إلى إعطاء صورة أكثر إيجابية عن واقع المنشأة مقارنة بالتدقيق الفعلي أو التقييم الموضوعي. ويقر الباحث بهذا القيد المنهجي، ويوصي الدراسات المستقبلية بالجمع بين التقييم الذاتي والتدقيق الخارجي للحصول على نتائج أكثر دقة.

سادساً : الدراسات السابقة

أولاً : الدراسات العربية

1- دراسة العراي وأبو عنزه (2024)

-العنوان : " دراسة تطبيقية عن دور إدارة المخاطر في تعزيز الأمن السيبراني للمؤسسات الصغيرة والمتوسطة في المملكة العربية السعودية " .

-الهدف : تقييم وتحسين إدارة المخاطر السيبرانية في المؤسسات الصغيرة والمتوسطة بالمملكة العربية السعودية.

-المنهج : المنهج الوصفي التحليلي والاستقرائي، باستخدام الاستبيانات والمقابلات ودراسات الحالة.

-النتائج : ضعف مستوى استخدام تكنولوجيا المعلومات لدى 50% من الموظفين؛ برامج مكافحة الفيروسات هي التقنية الأمنية الأكثر استخداماً بنسبة 40%؛ الهجمات الصوتية والفيديوية المزيفة تمثل أكبر عائق أمام إدارة المخاطر السيبرانية بنسبة 30%؛ 50% من الموظفين لديهم وعي بالمخاطر السيبرانية؛ وجود علاقة ارتباط قوية (89%) بين وعي الموظفين وإدارة المخاطر السيبرانية.

-التوصيات : رفع مستوى الوعي، تطوير سياسات شاملة، إجراء تقييمات دورية للمخاطر، الاستثمار في التقنيات الحديثة، بناء ثقافة أمنية قوية، وتوفير الموارد البشرية المؤهلة.

-الرابط بالدراسة الحالية : تقدم هذه الدراسة إطاراً مهماً لفهم واقع إدارة المخاطر السيبرانية في المؤسسات الصغيرة والمتوسطة السعودية، وتؤكد على أهمية الوعي التنظيمي والثقافة الأمنية كعوامل أساسية في نجاح ممارسات إدارة المخاطر .

2-دراسة زغلول (2026)

-العنوان : " الرقابة على نظم المعلومات والأمن السيبراني " .

-الهدف : التعرف على دور تدقيق أمن المعلومات في الحد من مخاطر نظم المعلومات الإلكترونية في المنظمات الحكومية.

-المنهج : المنهج الوصفي والتحليلي، باستخدام الاستبيان لجمع البيانات من عينة من منتسبي الجهاز الأعلى للرقابة في مصر ومكاتب التدقيق والبنوك المصرية.

-النتائج : وجود علاقة ذات دلالة إحصائية بين سياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك، التدقيق الخارجي) والحد من مخاطر نظم المعلومات الإلكترونية؛ أهمية وجود إطار تنظيمي قوي ومستقل للرقابة على أنظمة المعلومات.

-التوصيات: تعزيز توعية الموظفين وتدريبهم، تنفيذ إجراءات تدقيق دورية، تعزيز التعاون مع الجهات العليا للرقابة، وتبني أفضل الممارسات والتقنيات الحديثة.

-الرابط بالدراسة الحالية: تسلط هذه الدراسة الضوء على أهمية الرقابة والتدقيق كأدوات أساسية في تعزيز الأمن السيبراني، وتؤكد على دور السياسات والإجراءات الرقابية في الحد من المخاطر.

3-دراسة العازمي (2022)

-العنوان: " دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات الحاسوبية من المخاطر الإلكترونية في ظل عصر الرقمنة" .

-الهدف: التعرف على طبيعة المخاطر التي تهدد أمن نظم المعلومات الحاسوبية الإلكترونية في البنوك الكويتية ومعدلات تكرارها ومصادر حدوثها.

-المنهج: المنهج الوصفي التحليلي.

-النتائج: وجود تأثير معنوي لتأثير تفعيل أبعاد حوكمة تكنولوجيا المعلومات على تأمين المعلومات الحاسوبية من المخاطر الإلكترونية؛ وأن اتباع نظام معلومات حاسوبية سليم يقلل من مخاطر نظم المعلومات الحاسوبية الإلكترونية؛ وأن الاستفادة من الخبرات العالمية في مجال أمن المعلومات ترفع من درجة الثقة في المعلومات الحاسوبية الإلكترونية.

-التوصيات: تعزيز تطبيق حوكمة تكنولوجيا المعلومات، والاستفادة من المعايير الدولية.

-الرابط بالدراسة الحالية: تؤكد هذه الدراسة على أهمية الحوكمة كإطار تنظيمي لإدارة المخاطر السيبرانية، وتبرز دورها في حماية المعلومات وتعزيز الثقة.

ثانياً : الدراسات الأجنبية

4- دراسة (2025) Alarifi

-العنوان: "SMEs' Resilience Toward Cyberattacks in Saudi Arabia A Review Paper".

-الهدف : تقديم مراجعة شاملة لأدبيات مرونة المؤسسات الصغيرة والمتوسطة تجاه الهجمات السيبرانية في المملكة العربية السعودية.

-المنهج : مراجعة منهجية للأدبيات.

-النتائج : تسليط الضوء على التحديات الفريدة التي تواجه المؤسسات الصغيرة والمتوسطة في المملكة في مجال الأمن السيبراني، مثل محدودية الموارد ونقص الخبرات المتخصصة؛ وتأكيد أهمية تبني استراتيجيات مرنة قائمة على المخاطر.

-التوصيات : ضرورة تطوير أطر عمل سيبرانية مخصصة للمؤسسات الصغيرة والمتوسطة، وتعزيز التعاون بين القطاعين العام والخاص.

-الربط بالدراسة الحالية : تقدم هذه الدراسة مرجعية نظرية مهمة حول مرونة المؤسسات الصغيرة والمتوسطة، وتسلط الضوء على التحديات الخاصة التي تواجهها في السياق السعودي.

5- دراسة معايير استمرارية الأعمال(2024)

-العنوان : "A study of international standards in Information technology Business continuity management"

-الهدف : مراجعة مجموعة من المعايير والأطر والممارسات المتعلقة بإدارة المخاطر، وإدارة استمرارية الأعمال، والأمن السيبراني.

-المنهج : مراجعة وتحليل للمعايير الدولية مثل ISO 22301 و ISO 31000.

-النتائج : تأكيد أهمية دمج أطر الأمن السيبراني مع معايير إدارة استمرارية الأعمال المعترف بها دولياً؛ تحديد مجالات التكامل بين إدارة المخاطر واستمرارية الأعمال.

-التوصيات : اعتماد نهج متكامل يدمج الأمن السيبراني في خطط استمرارية الأعمال، والاستفادة من المعايير الدولية في تصميم السياسات والإجراءات.

-الربط بالدراسة الحالية : تشكل هذه الدراسة مرجعية أساسية لفهم العلاقة التكاملية بين إدارة المخاطر واستمرارية الأعمال.

6- دراسة الهيئة الوطنية للأمن السيبراني (NCA, 2025)

-العنوان : "Cybersecurity Controls for Private Sector Entities Not Considered Critical Infrastructure (NCNICC-1:2025)".

-الهدف : وضع إطار تنظيمي ملزم لمنشآت القطاع الخاص غير الحرجة في المملكة العربية السعودية.

-المنهج : إطار تنظيمي معياري.

-النتائج : تحديد 13 مكوناً فرعياً و26 ضابطاً أساسياً لمنشآت الفئة (ب)، تشمل جوانب الحوكمة والدفاع والمرونة؛ تقسيم المنشآت إلى فئتين (أ) الكبيرة و(ب) الصغيرة والمتوسطة مع متطلبات مختلفة لكل فئة.

-التوصيات : تطبيق الضوابط وفقاً لحجم المنشأة، وتوفير آليات للامتثال والمراقبة.

-الرابط بالدراسة الحالية : يمثل هذا الإطار التنظيمي المرجعية الأساسية لقياس مدى تطبيق ممارسات إدارة المخاطر السيبرانية في الدراسة الحالية.

ثالثاً : التعليق على الدراسات السابقة والفجوة البحثية

الجانب	الدراسات السابقة	الفجوة التي تسدها الدراسة الحالية
المتغيرات	تناولت إدارة المخاطر السيبرانية أو استمرارية الأعمال بشكل منفصل	تجمع بين المتغيرين في نموذج متكامل وتختبر العلاقة بينهما
القطاع	ركزت على القطاع المصرفي أو الحكومي	تركز على منشآت القطاع الخاص غير المصرفية
المجال الجغرافي	دراسات عامة أو في مناطق أخرى	تركز على منطقة الأحساء تحديداً
الإطار التنظيمي	نادراً ما ربطت الدراسات السابقة بالضوابط التنظيمية المحلية	تربط الدراسة بين الممارسات والضوابط السيبرانية الصادرة عن الهيئة الوطنية للأمن السيبراني

المنهجية	اعتمدت بعض الدراسات على المراجعة النظرية أو المناهج النوعية	تعتمد على منهج كمي تحليلي بدرجة عالية من الدقة الإحصائية
الشمولية	تناولت جوانب محدودة من ممارسات إدارة المخاطر	تشمل أربعة أبعاد شاملة لإدارة المخاطر وأربعة أبعاد لاستمرارية الأعمال

سابعاً: الإطار النظري

1- مفهوم إدارة المخاطر السيبرانية

تعرف إدارة المخاطر السيبرانية بأنها " العملية المنهجية والمدرسة التي تتضمن تحديد وتقييم وترتيب المخاطر السيبرانية التي قد تواجه المنشأة، ثم وضع خطط واستراتيجيات للتعامل مع هذه المخاطر، سواء بتجنبها أو تخفيف آثارها أو نقلها أو قبولها، وذلك بهدف حماية المنشأة وتحقيق أهدافها الاستراتيجية (ISO 31000:2018) " وتشمل عملية إدارة المخاطر السيبرانية أربع مراحل رئيسية :

أولاً : تحديد المخاطر : تحديد جميع المخاطر السيبرانية المحتملة التي قد تؤثر على المنشأة، سواء كانت داخلية أو خارجية، من خلال تحليل الأصول والتهديدات والثغرات والضوابط الحالية.

ثانياً : تقييم المخاطر : تقييم كل خطر على حدة لتحديد احتمالية حدوثه وأثر ذلك على المنشأة، من خلال تحليل التأثير والاحتمالية، وتصنيف المخاطر حسب أولوياتها.

ثالثاً : معالجة المخاطر : وضع خطط للتعامل مع كل خطر، وقد تتضمن هذه الخطط تجنب المخاطر، أو تقليل احتمالية حدوثها، أو تقليل آثارها، أو نقل المخاطر إلى جهة أخرى.

رابعاً : مراقبة المخاطر : متابعة المخاطر بشكل مستمر وتقييم فعالية الخطط الموضوعة للتعامل معها، مع إجراء التعديلات اللازمة حسب الحاجة، وتحديث سجل المخاطر بشكل دوري.

وقد أكدت الهيئة الوطنية للأمن السيبراني في ضوابطها NCNICC-1:2025 على ضرورة تطبيق هذه المراحل في منشآت القطاع الخاص، مع مراعاة الفروق بين المنشآت الكبيرة والصغيرة والمتوسطة.

2- مفهوم استمرارية الأعمال

تعرف استمرارية الأعمال بأنها "قدرة المنشأة على مواصلة تقديم خدماتها ومنتجاتها بمستويات مقبولة ومحددة مسبقاً بعد وقوع حادث معطل (ISO 22301:2019) "وتشير الأمانة العامة لمجلس التعاون الخليجي في تعريفها إلى أنها " العملية الاستراتيجية والإجرائية التي تقوم بها المنشأة لضمان استمرار الوظائف الأساسية خلال وبعد حدث تخريبي " (GISF, 2024) .

وتتضمن استمرارية الأعمال أربعة أبعاد رئيسية، وفقاً لنموذج المرونة التنظيمية المعتمد في الأدبيات الحديثة :

أولاً : الجاهزية : قدرة المنشأة على التخطيط والاستعداد المسبق لمواجهة الأحداث المعطلة المحتملة، من خلال وضع السياسات والإجراءات، وتحديد الموارد اللازمة، وتدريب الموظفين، وإجراء التمارين والمحاكاة. ويتضمن هذا البعد وضع خطط استمرارية الأعمال (BCP) وخطط التعافي من الكوارث (DRP) ، وتحديد أوقات التعافي المستهدفة (RTO) ونقاط الاسترجاع المستهدفة (RPO) .

ثانياً : الاستجابة : قدرة المنشأة على التعامل الفوري مع الحادث المعطل عند وقوعه ، من خلال تفعيل فرق الاستجابة ، وتنفيذ إجراءات الطوارئ ، والاتصال الفعال مع أصحاب المصلحة ، واحتواء الأضرار. ويتطلب هذا البعد وجود هيكل واضح لإدارة الأزمات وقنوات اتصال محددة مسبقاً.

ثالثاً : التعافي : قدرة المنشأة على استعادة العمليات الحيوية والوظائف الأساسية بعد وقوع الحادث، ضمن الأطر الزمنية المحددة مسبقاً. ويشمل ذلك استعادة الأنظمة والبيانات، وإعادة تشغيل العمليات، وضمان استمرار تقديم الخدمات الأساسية للعملاء.

رابعاً : التكيف : قدرة المنشأة على التعلم من الحوادث السابقة، وتحسين الاستراتيجيات والإجراءات بشكل مستمر، وتعزيز المرونة التنظيمية لمواجهة التهديدات المستقبلية. ويتضمن هذا البعد تحليل الدروس المستفادة، وتحديث السياسات، وتطوير القدرات.

3-العلاقة بين إدارة المخاطر السيبرانية واستمرارية الأعمال

تشير الأدبيات إلى وجود تكامل وثيق بين إدارة المخاطر السيبرانية واستمرارية الأعمال؛ إذ يُعد الأمن السيبراني عنصراً أساسياً ضمن إطار إدارة المخاطر الشامل، ويسهم في تحديد وتقييم وتخفيف المخاطر التي تهدد الأصول الرقمية للمنشأة. وقد أكدت الدراسات الحديثة أن المنشآت التي تتبنى نهجاً متكاملًا لإدارة المخاطر السيبرانية واستمرارية الأعمال تحقق نتائج أفضل بكثير من تلك التي لا تفعل ذلك (Alarifi, 2025) .

ويمكن تمثيل هذه العلاقة من خلال دورة حياة متكاملة تشمل:

1-تحديد وتقييم المخاطر السيبرانية: تحديد المخاطر السيبرانية المحتملة وتقييم احتمالية حدوثها وأثرها على المنشأة.

2-تطوير استراتيجيات الاستجابة: وضع خطط طوارئ للتعامل مع الحوادث السيبرانية، بما في ذلك إجراءات الاستجابة والاستعادة والتعافي.

3-الحوكمة والامتثال: ضمان الامتثال للوائح والقوانين المتعلقة بالأمن السيبراني، وتطوير ثقافة أمنية قوية داخل المنشأة.

4-التحسين المستمر: إجراء مراجعات دورية لاستراتيجيات الأمن السيبراني، وتحديثها لمواكبة التطورات التكنولوجية والتهديدات الجديدة.

وتؤكد هذه العلاقة أن ممارسات إدارة المخاطر السيبرانية الفعالة تسهم في تعزيز قدرة المنشأة على الاستعداد والاستجابة والتعافي من الحوادث السيبرانية، مما ينعكس إيجاباً على استمرارية أعمالها ومرونتها التنظيمية.

4-الإطار التنظيمي في المملكة العربية السعودية

أصدرت الهيئة الوطنية للأمن السيبراني (NCA) الضوابط السيبرانية لمنشآت القطاع الخاص غير البنية التحتية الوطنية الحرجة (NCNICC-1:2025)، والتي تمثل إطاراً تنظيمياً ملزماً يهدف إلى وضع الحد الأدنى من المتطلبات السيبرانية التي يتعين على منشآت القطاع الخاص تطبيقها، مع مراعاة حجم كل منشأة وطبيعة نشاطها.

وتصنف الضوابط المنشآت إلى فئتين رئيسيتين:

الفئة (أ) - المنشآت الكبيرة :

-عدد الموظفين: 250 موظفاً فأكثر.

-الإيرادات السنوية: أكثر من 200 مليون ريال سعودي.

-المتطلبات: مجموعة كاملة من الضوابط تشمل الحوكمة والدفاع والمرونة.

الفئة (ب) - المنشآت الصغيرة والمتوسطة:

-عدد الموظفين: من 6 إلى 249 موظفاً.

-الإيرادات السنوية: من 3 ملايين إلى 200 مليون ريال سعودي.

-المتطلبات: مجموعة مبسطة من الضوابط تشمل 13 مكوناً فرعياً و26 ضابطاً أساسياً.

وتهدف هذه الضوابط إلى تحقيق ثلاثة أهداف رئيسية:

1-تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية.

2-حماية سرية المعلومات وسلامتها وتوافرها.

3-تعزيز استمرارية الأعمال لمنشآت القطاع الخاص.

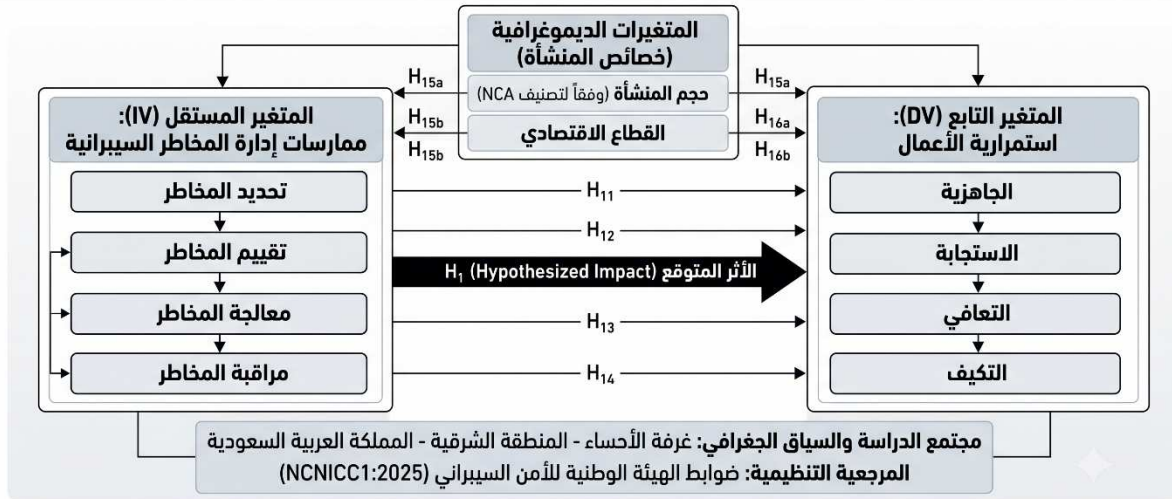
وتتضمن المتطلبات الأساسية للغة (ب) ما يلي :

المكون	المتطلبات الرئيسة
إدارة الأصول السيبرانية	تحديد الأصول وتصنيفها والحفاظ على قائمة جرد محدثة
أمن الشبكات	تجزئة الشبكات، استخدام جدران الحماية، إدارة النفاذ
إدارة الهوية والنفاذ	تطبيق مبدأ أقل الصلاحيات، استخدام المصادقة متعددة العوامل
حماية الأجهزة الطرفية	استخدام برامج مكافحة الفيروسات، تحديث الأنظمة
أمن التطبيقات	تطبيق ممارسات التطوير الآمن، اختبار أمن التطبيقات
أمن البيانات	تشفير البيانات، منع فقدان البيانات، إدارة النسخ الاحتياطي
إدارة الحوادث	وضع خطة للاستجابة للحوادث، وتشكيل فريق للاستجابة
استمرارية الأعمال	وضع خطط استمرارية الأعمال والتعافي من الكوارث، وإجراء اختبارات دورية

5- نموذج البحث المفاهيمي

بناءً على الإطار النظري المذكور يمكن تمثيل نموذج البحث المفاهيمي على النحو التالي :

نموذج البحث المفاهيمي المقترح : أثر ممارسات إدارة المخاطر السيبرانية على استمرارية الأعمال في منشآت القطاع الخاص المنتسبة لغرفة الأحساء



شكل رقم (1): نموذج البحث المفاهيمي المقترح (أثر ممارسات إدارة المخاطر السيبرانية على استمرارية الأعمال). المصدر: إعداد الباحث بناءً على الإطار النظري والدراسات السابقة.

6-متغيرات البحث

النوع	المتغير	الأبعاد
المتغير المستقل	ممارسات إدارة المخاطر السيبرانية	تحديد المخاطر تقييم المخاطر معالجة المخاطر مراقبة المخاطر
المتغير التابع	استمرارية الأعمال	الجاهزية الاستجابة التعافي التكيف
المتغيرات الديموغرافية	خصائص المنشأة	حجم المنشأة حسب تصنيف NCA القطاع الاقتصادي

ثامناً : فرضيات البحث

بناءً على مشكلة البحث وأهدافه والإطار النظري والنموذج المفاهيمي، يمكن صياغة الفرضيات التالية:

الفرضية الرئيسية:

- H₀** : لا توجد علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر السيبرانية بأبعادها (تحديد المخاطر، تقييمها، معالجتها، مراقبتها) واستمرارية الأعمال بأبعادها (الجاهزية، الاستجابة، التعافي، التكيف) في منشآت القطاع الخاص المنتسبة لغرفة الأحساء.
- H₁** : توجد علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر السيبرانية بأبعادها واستمرارية الأعمال في منشآت القطاع الخاص المنتسبة لغرفة الأحساء.

الفرضيات الفرعية :

الفرضية الفرعية الأولى :

H₀₁ : لا يوجد أثر ذو دلالة إحصائية لتحديد المخاطر السيبرانية على استمرارية الأعمال.

H₁₁ : يوجد أثر ذو دلالة إحصائية لتحديد المخاطر السيبرانية على استمرارية الأعمال.

الفرضية الفرعية الثانية :

H₀₂ : لا يوجد أثر ذو دلالة إحصائية لتقييم المخاطر السيبرانية على استمرارية الأعمال.

H₁₂ : يوجد أثر ذو دلالة إحصائية لتقييم المخاطر السيبرانية على استمرارية الأعمال.

الفرضية الفرعية الثالثة :

H₀₃ : لا يوجد أثر ذو دلالة إحصائية لمعالجة المخاطر السيبرانية على استمرارية الأعمال.

H₁₃ : يوجد أثر ذو دلالة إحصائية لمعالجة المخاطر السيبرانية على استمرارية الأعمال.

الفرضية الفرعية الرابعة :

H₀₄ : لا يوجد أثر ذو دلالة إحصائية لمراقبة المخاطر السيبرانية على استمرارية الأعمال.

H₁₄ : يوجد أثر ذو دلالة إحصائية لمراقبة المخاطر السيبرانية على استمرارية الأعمال.

الفرضيات المتعلقة بالفروق الديموغرافية :

الفرضية الفرعية الخامسة (أثر حجم المنشأة):

H_{05a} : لا توجد فروق ذات دلالة إحصائية في ممارسات إدارة المخاطر السيبرانية تُعزى إلى حجم المنشأة (وفقاً لتصنيف الهيئة الوطنية للأمن السيبراني).

H_{15a} : توجد فروق ذات دلالة إحصائية في ممارسات إدارة المخاطر السيبرانية تُعزى إلى حجم المنشأة.

الفرضية الفرعية السادسة (أثر القطاع الاقتصادي):

H_{05b} : لا توجد فروق ذات دلالة إحصائية في ممارسات إدارة المخاطر السيبرانية تُعزى إلى القطاع الاقتصادي للمنشأة.

H_{15b} : توجد فروق ذات دلالة إحصائية في ممارسات إدارة المخاطر السيبرانية تُعزى إلى القطاع الاقتصادي للمنشأة.

الفرضية الفرعية السابعة (أثر حجم المنشأة على استمرارية الأعمال):

H_{06a} : لا توجد فروق ذات دلالة إحصائية في استمرارية الأعمال تُعزى إلى حجم المنشأة.

H_{16a} : توجد فروق ذات دلالة إحصائية في استمرارية الأعمال تُعزى إلى حجم المنشأة.

الفرضية الفرعية الثامنة (أثر القطاع الاقتصادي على استمرارية الأعمال):

H_{06b} : لا توجد فروق ذات دلالة إحصائية في استمرارية الأعمال تُعزى إلى القطاع الاقتصادي للمنشأة.

H_{16b} : توجد فروق ذات دلالة إحصائية في استمرارية الأعمال تُعزى إلى القطاع الاقتصادي للمنشأة.

تاسعاً : منهجية البحث

1- نوع الدراسة ومنهجها

تعتمد هذه الدراسة على **المنهج الوصفي التحليلي** بوصفه المنهج الأكثر ملاءمة لطبيعة البحث، حيث يهدف إلى :

-**وصف** الواقع الحالي لممارسات إدارة المخاطر السيبرانية واستمرارية الأعمال في منشآت القطاع الخاص المنتسبة لغرفة الأحساء، من خلال جمع البيانات الكمية وتحليلها إحصائياً.

-**تحليل** العلاقات بين متغيرات الدراسة، واختبار الفرضيات، وتحديد أثر المتغير المستقل على المتغير التابع.

-**استقراء** النتائج العامة من عينة الدراسة وتعميمها على مجتمع الدراسة.

كما يستخدم **المنهج الكمي** من خلال الاستبيان كأداة رئيسية لجمع البيانات، مع تضمين بعض الأسئلة المفتوحة للحصول على رؤى نوعية إضافية تعزز فهم النتائج الكمية.

2-مجتمع وعينة الدراسة

مجتمع الدراسة:

يتكون مجتمع الدراسة من جميع منشآت القطاع الخاص المنتسبة لغرفة الأحساء بالمنطقة الشرقية. ووفقاً لإحصائيات غرفة الأحساء، يبلغ عدد المنشآت المنتسبة حوالي **751 منشأة**، موزعة على مختلف القطاعات الاقتصادية (تجاري، صناعي، خدمي، مقاولات، وغيرها).

عينة الدراسة:

يتم اختيار عينة عشوائية طبقية (Stratified Random Sample) من مجتمع الدراسة، حيث يتم تقسيم المجتمع إلى طبقات حسب القطاع الاقتصادي وحجم المنشأة، ثم اختيار عينة عشوائية من كل طبقة.

• **تحديد حجم العينة:** تم تحديد حجم العينة باستخدام **معادلة Cochran** للعينات المحدودة، وذلك

على النحو التالي:

$$n_0 = \frac{Z^2 \cdot p \cdot (1 - p)}{e^2}$$

حيث :

- $Z = 1.96$ % القيمة الجدولية المقابلة لمستوى الثقة 95
- $p = 0.50$ نسبة التباين المقدرة في المجتمع (نسبة 0.50 لتعظيم حجم العينة)
- $e = 0.05$ هامش الخطأ المقبول

$$n_0 = \frac{(1.96)^2 \times 0.50 \times 0.50}{(0.05)^2} = \frac{3.8416 \times 0.25}{0.0025} = 384.16$$

وبتطبيق معادلة تصحيح حجم العينة للمجتمعات المحدودة: (Finite Population Correction)

$$n = \frac{n_0}{1 + \frac{(n_0 - 1)}{N}}$$

حيث $N = 751$ (حجم المجتمع) فإن :

$$n = \frac{384.16}{1 + \frac{383.16}{751}} = \frac{384.16}{1 + 0.510} = \frac{384.16}{1.510} \approx 254$$

وبمراعاة نسبة عدم الاستجابة المتوقعة (حوالي 15-20%)، سيتم توزيع **300 استبيان** لضمان الحصول على عدد كافٍ من الاستجابات الصالحة للتحليل (لا يقل عن 254 استبياناً صالحاً).

وحدة المعاينة:

تتمثل وحدة المعاينة في المدراء التنفيذيين، أو مدراء تكنولوجيا المعلومات، أو مسؤولي الأمن السيبراني في المنشآت المستهدفة، باعتبارهم الأكثر دراية بممارسات إدارة المخاطر السيبرانية واستمرارية الأعمال في منشاتهم.

معايير اختيار العينة:

1- أن تكون المنشأة منتسبة لغرفة الأحساء.

2- أن تعمل المنشأة في القطاع الخاص (غير حكومي).

3- أن يكون للمنشأة نشاط اقتصادي فعلي.

4- أن يكون لدى المنشأة حد أدنى من البنية التحتية لتكنولوجيا المعلومات (وجود أجهزة حاسوب، اتصال بالإنترنت، وما شابه).

3- أداة جمع البيانات

الاستبيان :الأداة الرئيسية لجمع البيانات الكمية، وقد تم تصميمه وفقاً للأسس العلمية للبناء المقاييس، ويشتمل على أربعة أقسام رئيسة:

القسم الأول: البيانات الديموغرافية والمعلومات العامة عن المنشأة

يتضمن هذا القسم مجموعة من المتغيرات الديموغرافية التي تساعد في وصف عينة الدراسة وتشمل :

-حجم المنشأة (حسب تصنيف الهيئة الوطنية للأمن السيبراني): (من 6 إلى 49 موظفاً - صغيرة، من 50 إلى 249 موظفاً - متوسطة، 250 موظفاً فأكثر - كبيرة). ويُستثنى من هذا التصنيف المنشآت التي يقل عدد موظفيها عن 6 موظفين، حيث لا تنطبق عليها الضوابط السيبرانية وفقاً لتعريف الهيئة.

-القطاع الاقتصادي: (تجاري ، صناعي ، خدمي ، مقاولات ، أخرى)

-المسمى الوظيفي للمستجيب : (مدير تنفيذي ، مدير تكنولوجيا معلومات ، مسؤول أمن سيبراني، محاسب/مالي ، أخرى) .

-عدد سنوات الخبرة في المنشأة الحالية.

القسم الثاني : ممارسات إدارة المخاطر السيبرانية

يتضمن هذا القسم مجموعة من العبارات تقيس أبعاد المتغير المستقل الأربعة، وقد تم تصميمها استناداً إلى معايير ISO 31000 وضوابط الهيئة الوطنية للأمن السيبراني (NCNICC-1:2025) والأدبيات السابقة:

النوع	المتغير	الأبعاد
ممارسات إدارة المخاطر السيبرانية	تحديد المخاطر	"تقوم المنشأة بتحديد الأصول الرقمية الحيوية بشكل دوري 5-6". عبارات
ممارسات إدارة المخاطر السيبرانية	تقييم المخاطر	"تقوم المنشأة بتقييم احتمالية وتأثير المخاطر السيبرانية المحتملة 5-6". عبارات
ممارسات إدارة المخاطر السيبرانية	معالجة المخاطر	"تطبق المنشأة ضوابط أمنية مناسبة لمعالجة المخاطر المحددة". عبارات 5-6
ممارسات إدارة المخاطر السيبرانية	مراقبة المخاطر	"تقوم المنشأة بمراجعة وتحديث سجل المخاطر السيبرانية بشكل دوري 5-6". عبارات
—	—	الإجمالي: 20-24 عبارة

القسم الثالث: استمرارية الأعمال

يتضمن هذا القسم مجموعة من العبارات تقيس أبعاد المتغير التابع الأربعة، وقد تم تصميمها استناداً إلى معايير ISO 22301 والأدبيات السابقة:

العدد	العبارة	البعد
5-6 عبارات	"تمتلك المنشأة خطة مكتوبة لاستمرارية الأعمال". (BCP)	الجاهزية
4-5 عبارات	"تمتلك المنشأة فريقاً للاستجابة للحوادث السيبرانية".	الاستجابة
4-5 عبارات	"تمتلك المنشأة خطة محدثة للتعافي من الكوارث". (DRP)	التعافي
4-5 عبارات	"تقوم المنشأة بتحديث استراتيجياتها السيبرانية بناءً على الدروس المستفادة من الحوادث".	التكيف
الإجمالي: 17-21 عبارة	—	—

القسم الرابع : أسئلة مفتوحة (اختياري)

يتضمن هذا القسم أسئلة مفتوحة تتيح للمستجيبين تقديم رؤى إضافية حول التحديات والممارسات في مجال إدارة المخاطر السيبرانية واستمرارية الأعمال.

مقياس الاستجابة :

يستخدم مقياس ليكرت الخماسي (Likert Scale) للاستجابة على العبارات، على النحو التالي:

الوزن	المستوى	الدرجة
1	غير موافق بشدة	1
2	غير موافق	2
3	محايد	3
4	موافق	4
5	موافق بشدة	5

4- صدق الأداة وثباتها

أ- صدق الأداة (Validity)

الصدق الظاهري (Face Validity) :

يتم عرض الاستبيان في صورته الأولية على مجموعة من المحكمين من الأكاديميين المتخصصين في إدارة الأعمال وتكنولوجيا المعلومات والأمن السيبراني، بالإضافة إلى خبراء عمليين من غرفة الأحساء والهيئة الوطنية للأمن السيبراني ويطلب من المحكمين تقييم :

-وضوح صياغة العبارات وسلامتها اللغوية.

-مدى ملائمة العبارات للأبعاد المخصصة لها.

-مدى شمولية العبارات لأبعاد المتغيرات.

-اقتراح أي تعديلات أو إضافات.

يتم تعديل الاستبيان بناءً على ملاحظات المحكمين، ثم يُطبق على عينة استطلاعية صغيرة (20-30 مستجيباً) للتأكد من وضوح التعليمات والعبارات.

صدق البناء :

يتم التحقق من صدق البناء باستخدام :

1- التحليل العاملي الاستكشافي : للتأكد من أن عبارات كل بعد تتجمع في عامل واحد، وللتأكد من أن أبعاد المتغير المستقل منفصلة عن أبعاد المتغير التابع.

2- معامل الارتباط بين العبارة والبعد : حساب معامل ارتباط بيرسون بين درجة كل عبارة والدرجة الكلية للبعد الذي تنتمي إليه، بحيث يكون معامل الارتباط موجباً ودال إحصائياً عند مستوى $(\alpha \leq 0.05)$

الصدق التمييزي : يتم التأكد من أن معاملات الارتباط بين أبعاد المتغير المستقل والمتغير التابع ليست عالية جداً (بحيث لا تتجاوز 0.85)، مما يشير إلى تميز المتغيرين عن بعضهما.

ب- ثبات الأداة

يتم حساب ثبات الاستبيان باستخدام معامل ألفا كرونباخ حيث :

- يعتبر المعامل مقبولاً إذا كانت قيمته ≤ 0.70 .

- يعتبر المعامل جيداً إذا كانت قيمته ≤ 0.80 .

- يعتبر المعامل ممتازاً إذا كانت قيمته ≤ 0.90 .

يتم حساب معامل ألفا كرونباخ لكل بعد من أبعاد المتغيرات على حدة وكذلك للمقياس ككل ويتوقع أن تتجاوز قيم المعامل 0.80 لجميع الأبعاد مما يشير إلى درجة عالية من الثبات الداخلي.

كما يستخدم معامل ارتباط سبيرمان-براون بطريقة التجزئة النصفية (Split-Half) للتأكد من ثبات الاستبيان.

5- الأساليب الإحصائية المستخدمة

يتم تحليل البيانات باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) الإصدار 26، بالإضافة إلى استخدام برنامج Smart PLS 4 للتحليل الهيكلي. وتشمل الأساليب الإحصائية المستخدمة:

أ- الإحصاء الوصفي

1-المتوسطات الحسابية : لتحديد مستوى كل عبارة وبعد ومتغير.

2-الانحرافات المعيارية : لقياس درجة تشتت الاستجابات حول المتوسط.

3-التكرارات والنسب المئوية : لوصف خصائص العينة الديموغرافية.

4-معامل الاختلاف : لمقارنة درجة التشبع بين الأبعاد المختلفة.

ب- الإحصاء الاستدلالي :

تحديد منطقة الرفض : نظراً لأن الفرضيات مصاغة لاختبار وجود علاقة أو أثر دون تحديد الاتجاه (إيجابي أو سلبي)، فإن الاختبارات الإحصائية ستكون ثنائية الذيل ولضمان أقصى درجات الدقة الإحصائية عند اتخاذ قرار رفض الفرضية الصفرية، سيتم اعتماد مستوى دلالة $\alpha = 0.05$ ، مع توزيع منطقة الرفض على طرفي المنحنى الطبيعي، بحيث تكون قيمة $\alpha/2 = 0.025$ في كل طرف. وبالتالي، سيتم رفض الفرضية الصفرية إذا كانت القيمة الاحتمالية (P-Value) أقل من 0.05، أو إذا كانت قيمة إحصائية الاختبار تقع في منطقة الرفض (أقل من القيمة الحرجة السفلية أو أعلى من القيمة الحرجة العليا).

1-معامل ارتباط بيرسون : لاختبار العلاقة بين المتغير المستقل (أبعاده) والمتغير التابع (أبعاده)، وللتأكد من عدم وجود علاقة عالية بين أبعاد المتغير المستقل (Multicollinearity) .

2-تحليل الانحدار الخطي المتعدد :

الانحدار البسيط : لقياس أثر كل بعد من أبعاد المتغير المستقل على المتغير التابع (الفرضيات الفرعية).

الانحدار المتعدد : لقياس الأثر المشترك لأبعاد المتغير المستقل على المتغير التابع (الفرضية الرئيسية).

3-اختبار تحليل التباين الأحادي : لاختبار الفروق في استجابات أفراد العينة تُعزى إلى خصائص المنشأة

(الحجم، القطاع الاقتصادي). وفي حالة وجود فروق، يتم استخدام اختبار (Post Hoc) مثل اختبار (Tukey HSD) لتحديد مصدر الفروق.

4-اختبار للعينات المستقلة : يستخدم في حالة المتغيرات الديموغرافية التي تتكون من فئتين فقط.

5-تحليل المسار (Path Analysis) باستخدام (Smart PLS) : لتأكيد العلاقات بين المتغيرات

في النموذج الهيكلي، واختبار جودة النموذج من خلال مؤشرات مثل:

R^2 معامل التحديد لقياس قوة النموذج.

Q^2 مؤشر الملاءمة التنبؤية.

SRMR جذر متوسط مربعات البواقي المعياري للتأكد من جودة المطابقة.

6- اختبار هارمان للعامل الواحد : نظراً لأن البحث يعتمد على أداة واحدة (الاستبيان) لجمع البيانات حول المتغير المستقل والتابع في نفس الوقت ومن نفس المستجيبين، فهناك خطر حدوث تباين الطريقة المشتركة وللتأكد من خلوه البيانات من هذا التحيز، سيتم تطبيق اختبار هارمان للعامل الواحد ضمن التحليل العاملي الاستكشافي. فإذا لم يظهر عامل واحد يفسر أكثر من 50% من التباين الكلي، فإن ذلك يشير إلى أن تباين الطريقة المشتركة لا يشكل تهديداً جوهرياً لصحة النتائج.

7- اختبارات الفروض : يتم قبول الفرضية إذا كانت قيمة (P-Value) أقل من مستوى الدلالة ($\alpha \leq 0.05$)، مع مراعاة طبيعة الاختبار ثنائي الذيل.

6- الاعتبارات الأخلاقية للبحث

1- الموافقة المسبقة : الحصول على موافقة خطية من غرفة الأحساء لتوزيع الاستبيانات على المنشآت المنتسبة.

2- الموافقة المستنيرة : إيضاح الغرض من الدراسة للمستجيبين، وتأكيد أن المشاركة طوعية، وأنه يمكن الانسحاب في أي وقت.

3- السرية والخصوصية : تأكيد أن البيانات ستستخدم للأغراض العلمية فقط، ولن يتم الكشف عن هوية المستجيبين أو منشآتهم في أي تقرير أو منشور.

4- الأمانة العلمية : الالتزام بالأمانة العلمية في جمع البيانات وتحليلها وتفسيرها، وتجنب أي تلاعب أو تحيز.

5- حقوق الملكية : احترام حقوق الملكية الفكرية في استخدام الأدوات والمقاييس والمراجع.

عاشراً : هيكل البحث

يتكون البحث من خمسة فصول رئيسة على النحو التالي:

الفصل التمهيدي : الإطار العام للبحث

- مقدمة البحث.
- مشكلة البحث وأسئلته.
- أهداف البحث وأهميته.
- حدود البحث.
- الدراسات السابقة.
- مصطلحات البحث ومفاهيمه.

الفصل الأول : الإطار النظري والدراسات السابقة

- المبحث الأول : إدارة المخاطر السيبرانية (المفهوم، الأبعاد، الأهمية، المعايير الدولية والإطار التنظيمي السعودي).
- المبحث الثاني : استمرارية الأعمال (المفهوم، الأبعاد، الأهمية، المعايير الدولية).
- المبحث الثالث : العلاقة بين إدارة المخاطر السيبرانية واستمرارية الأعمال.
- المبحث الرابع : الدراسات السابقة (العربية والأجنبية).
- المبحث الخامس : نموذج البحث والفرضيات.

الفصل الثاني : منهجية البحث

- نوع الدراسة ومنهجها.
- مجتمع وعينة الدراسة.
- أداة جمع البيانات (الاستبيان) وتصميمه.
- صدق الأداة وثباتها.

- الأساليب الإحصائية المستخدمة (مع الإشارة إلى اختبار هارمان للعامل الواحد ومنطقة الرفض).
- الاعتبارات الأخلاقية.

الفصل الثالث : التحليل الإحصائي واختبار الفرضيات

- المبحث الأول : الخصائص الديموغرافية لعينة الدراسة (الإحصاء الوصفي).
- المبحث الثاني : الإحصاء الوصفي لمتغيرات الدراسة (المتوسطات والانحرافات المعيارية).
- المبحث الثالث : اختبار صدق وثبات الأداة.
- المبحث الرابع : اختبار الفرضيات (الارتباط، الانحدار، الفروق).
- المبحث الخامس : مناقشة النتائج.

الفصل الرابع : النتائج والتوصيات

- المبحث الأول : ملخص النتائج الرئيسية.
- المبحث الثاني : مناقشة النتائج في ضوء الإطار النظري والدراسات السابقة.
- المبحث الثالث : التوصيات العملية.
- المبحث الرابع : مقترحات لدراسات مستقبلية.

المراجع والملاحق

- قائمة المراجع (عربية وأجنبية).
- الملحق (1) : نموذج الاستبيان.
- الملحق (2) : قائمة المحكمين.
- الملحق (3) : خطاب تسهيل المهمة من غرفة الأحساء.

-الملحق (4) : قائمة المصطلحات والمفاهيم الأساسية.

حادي عشر : الجدول الزمني للبحث

المرحلة	النشاط	المدة	الجدول الزمني
المرحلة الأولى: التمهيد	إعداد خطة البحث، مراجعة الأدبيات	شهران	الشهر 1-2
المرحلة الثانية: تصميم الأداة	تصميم الاستبيان، التحكيم، التجربة الاستطلاعية	شهر ونصف	الشهر 3-4
المرحلة الثالثة: جمع البيانات	توزيع الاستبيانات، المتابعة، الاسترداد	شهران	الشهر 5-6
المرحلة الرابعة: التحليل	تفريغ البيانات، التحليل الإحصائي، اختبار الفرضيات	شهران	الشهر 7-8
المرحلة الخامسة: الكتابة	كتابة الفصول، مراجعة النتائج	شهران	الشهر 9-10
المرحلة السادسة: المراجعة	مراجعة البحث، التعديلات، التقديم النهائي	شهر واحد	الشهر 11
الإجمالي	—	11 شهراً	—

ثاني عشر : الميزانية التقديرية للبحث

البند	التفاصيل	التكلفة المقدرة (ريال سعودي)
الاستبيانات	طباعة الاستبيانات، التوزيع، المتابعة	2,000 – 3,000
التنقل والمواصلات	السفر إلى الأحساء، التنقل بين المنشآت	3,000 – 5,000
المقابلات	(إن أمكن) تكاليف التنقل واللقاءات	1,000 – 2,000
البرامج الإحصائية	تراخيص برامج SPSS / Smart PLS	1,500 – 2,500
التدقيق اللغوي	مراجعة لغوية للبحث باللغتين العربية والإنجليزية	1,000 – 2,000
الطباعة والتجليد	طباعة الرسالة، التجليد، الأقراص المدمجة	1,500 – 2,500
مصاريف متفرقة	اتصالات، إنترنت، قرطاسية	1,000 – 1,500
الإجمالي	—	11,000 – 18,500 ريال سعودي

ثالث عشر : قائمة المراجع

أولاً : المراجع العربية

- 1-العربي ، ماجد قليل محمد، وأبو عنزه، أسماء. (2024). دراسة تطبيقية عن دور إدارة المخاطر في تعزيز الأمن السيبراني للمؤسسات الصغيرة والمتوسطة في المملكة العربية السعودية *International Journal of Financial, Administrative and Economic Sciences*, 3(10).
- 2-زغلول، سامي علي محمد. (2026). الرقابة على نظم المعلومات والأمن السيبراني. بحث مقدم للمشاركة في المسابقة العلمية الرابعة عشر لمنظمة الأرابوساي.

- 3-العازمي، عبد الله فالخ. (2022). دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات الحاسوبية من المخاطر الإلكترونية في ظل عصر الرقمنة. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، 13(2).
- 4-الدوسري، س.، العمري، ه.، والشهري، م. (2023). تحديات إدارة المخاطر السيبرانية في عصر التقنيات الناشئة: دراسة استكشافية على المؤسسات السعودية. *مجلة جامعة الملك سعود للعلوم التقنية*، 35(3)، 280-295.
- 5-الدوسري، س.، العمري، ه.، والشهري، م. (2024). أثر التعاون وتبادل المعلومات على تعزيز القدرات الدفاعية السيبرانية في المؤسسات السعودية. *المجلة العربية للعلوم الأمنية*، 37(1).
- 6-الزهراني، أ.، والغامدي، م. (2023). نموذج متكامل لإدارة المخاطر السيبرانية واستمرارية الأعمال في المؤسسات السعودية. *مجلة جامعة الملك عبد العزيز: علوم الحاسبات وتقنية المعلومات*، 12(3)، 180-195.
- 7-الزهراني، أ. (2023). منهجية تحليل الوثائق في دراسات الأمن السيبراني: دراسة تطبيقية على المؤسسات الحكومية السعودية. *المجلة السعودية للعلوم الإدارية*، 18(4)، 315-330.
- 8-القحطاني، م. (2023). إطار لقياس وتحسين نضج إدارة المخاطر السيبرانية في المؤسسات السعودية.. جامعة الملك فهد للبترول والمعادن.
- 9-البنك المركزي السعودي (SAMA) الدليل التنظيمي لإدارة استمرارية الأعمال
- 10-الهيئة الوطنية للأمن السيبراني. (2025). الضوابط السيبرانية لمنشآت القطاع الخاص غير البنية التحتية الوطنية الحرجة. (NCNICC-1:2025) الرياض.
- 11-الغامدي، نورة. (2023). أثر تطبيق معايير الأمن السيبراني على إدارة المخاطر في الشركات الصغيرة والمتوسطة بالمنطقة الشرقية. *المجلة السعودية للعلوم التقنية*، 8(2)، 180-205.
- 12-العتيبي، م.، والقحطاني، س. (2024). نموذج متكامل لتقييم المخاطر السيبرانية في المؤسسات السعودية. *المجلة السعودية لأمن المعلومات*، 7(1)، 15-30.

- 13-Alarifi, S. H. (2025). SMEs' Resilience Toward Cyberattacks in Saudi Arabia: A Review Paper. *International Journal of Scientific Research and Management (IJSRM)*.
- 14-Alorabi, M. Q. M., & Abuanzeh, A. (2024). The Role of Risk Management in Enhancing Cybersecurity for Small and Medium Enterprises (SMEs) in Saudi Arabia "Applied Study". *International Journal of Financial, Administrative and Economic Sciences*, 3(10).
- 15-National Cybersecurity Authority (NCA). (2025). *Cybersecurity Controls for Private Sector Entities Not Considered Critical Infrastructure (NCNICC-1:2025)*. Kingdom of Saudi Arabia.
- 16-ISO. (2018). *ISO 31000:2018 Risk management — Guidelines*. International Organization for Standardization.
- 17-ISO. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. International Organization for Standardization.
- 18-NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology.
- 19-NIST. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.
- 20-Kaspersky. (2021). *State of cybersecurity in the Middle East: Key trends in 2021*.

- 21-AlGhamdi, R., Alfarraj, O., & Bahaddad, A. (2020). How retailers at different stages of e-commerce maturity evaluate their entry to e-commerce activities? *Journal of Computer Science*, 16(7), 983-994.
- 22-Almutairi, N., & Alruwaili, M. (2023). Cybersecurity risk management in Saudi SMEs: A systematic literature review. *Saudi Journal of Business and Management Studies*, 8(1), 1-12.
- 23-Aven, T. (2022). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1-13.
- 24-Hopkin, P. (2023). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (6th ed.). Kogan Page.
- 25-Nocco, B. W., & Stulz, R. M. (2021). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, 33(1), 8-20.
- 26-Slapnicar, S., & et al. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44(8). Elsevier Inc.
- 27-Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards: A Review and Comprehensive Overview. *MDPI*, 11(14). Basel, Switzerland.
- 28-Mirwali Azizi, Hakimi, M., Frishta Amiri, & Amir Kror Shahidzay. (2024). The Role of IT (Information Technology) Audit

in Digital Transformation: Opportunities and Challenges. *Open Access Indonesia Journal of Social Sciences*, 7(2).

29-Mohammad Aljanabi & et al. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian Journal of Cybersecurity*, Vol.2023.

30-GISF. (2024). *Developing a Security Risk Management (SRM) Strategy and Policy: A Cross-Functional Guide*. Global Interagency Security Forum.

رابع عشر: الملاحق

الملحق (1): نموذج الاستبيان

(سيتم إدراج الاستبيان كاملاً بعد التحكيم)

الملحق (2): قائمة المحكمين

(سيتم إدراج أسماء المحكمين وصفاتهم العلمية)

الملحق (3) : خطاب تسهيل المهمة

(سيتم إدراج الخطاب الموجه إلى غرفة الأحساء)

الملحق (4) : قائمة المصطلحات والمفاهيم الأساسية

المصطلح	التعريف الإجرائي
إدارة المخاطر السيبرانية	العملية المنهجية لتحديد وتقييم ومعالجة ومراقبة المخاطر المرتبطة بالأمن السيبراني في المنشأة.

تحديد المخاطر	عملية التعرف على الأصول الرقمية الحيوية، والتهديدات المحتملة، والثغرات الأمنية، والضوابط الحالية.
تقييم المخاطر	عملية تحليل احتمالية حدوث المخاطر السيبرانية وأثرها المحتمل على المنشأة، وتصنيفها حسب الأولوية.
معالجة المخاطر	وضع وتنفيذ استراتيجيات وضوابط للتعامل مع المخاطر السيبرانية المحددة (تجنب، تخفيف، نقل، قبول).
مراقبة المخاطر	المتابعة المستمرة للمخاطر وفعالية الضوابط، وتحديث سجل المخاطر بشكل دوري.
استمرارية الأعمال	قدرة المنشأة على مواصلة تقديم خدماتها ومنتجاتها بمستويات مقبولة بعد وقوع حادث معطل.
الجاهزية	قدرة المنشأة على التخطيط والاستعداد المسبق لمواجهة الأحداث المعطلة المحتملة.
الاستجابة	قدرة المنشأة على التعامل الفوري مع الحادث المعطل عند وقوعه.
التعافي	قدرة المنشأة على استعادة العمليات الحيوية والوظائف الأساسية بعد وقوع الحادث.
التكيف	قدرة المنشأة على التعلم من الحوادث السابقة وتحسين الاستراتيجيات بشكل مستمر.
الضوابط السيبرانية	الإجراءات والتدابير الأمنية التي تهدف إلى حماية سرية المعلومات وسلامتها وتوافرها.
RTO (Recovery Time Objective)	الوقت المستهدف لاستعادة الخدمة أو النشاط بعد وقوع الحادث.

الحد الأقصى المقبول لفقدان البيانات المقاسة بالوقت.	RPO (Recovery Point Objective)
---	--------------------------------

خامس عشر : خاتمة

تهدف هذه الخطة إلى تقديم إطار منهجي متكامل لدراسة أثر ممارسات إدارة المخاطر السيبرانية على استمرارية الأعمال في منشآت القطاع الخاص المنتسبة لغرفة الأحساء. وتأتي أهمية هذه الدراسة من كونها تسد فجوة بحثية في منطقة الأحساء، وترتبط بإطار تنظيمي وطني حديث هو الضوابط السيبرانية الصادرة عن الهيئة الوطنية للأمن السيبراني. (NCNICC-1:2025)

ومن المتوقع أن تسهم نتائج الدراسة في تقديم رؤى عملية لصناع القرار في غرفة الأحساء والجهات المعنية، وتقديم توصيات قابلة للتطبيق لتعزيز ممارسات إدارة المخاطر السيبرانية، وتحسين استمرارية الأعمال، ودعم الاقتصاد المحلي في المنطقة الشرقية. كما يُتوقع أن تفتح الدراسة آفاقاً لبحوث مستقبلية في مجال الأمن السيبراني واستمرارية الأعمال في السياق السعودي والعربي.