

جامعة ميدأوشن

كلية الإدارة

تخصص إدارة المخاطر



العلاقة بين إدارة المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني: دراسة

تطبيقية في شركات تقنية المعلومات بالرياض

إعداد الطالب/

إبراهيم عبدالله المحارب

243001040

إشراف/

د. الفيصل عبد الحميد محمد حسن

العام الدراسي:

2025



4	مقدمة:
6	مشكلة الدراسة:
7	أهمية الدراسة:
8	أهداف الدراسة:
9	تساؤلات الدراسة:
10	فروض الدراسة:
10	نموذج الدراسة:
10	الدراسات السابقة:
20	الفجوة البحثية:
21	المنطلقات النظرية للدراسة:
21	المنهجية وطرق البحث:
25	مصادر جمع البيانات:
26	أدوات الدراسة:
28	حدود الدراسة:
29	المراجع:

مقدمة:

في ظل التوسع الرقمي الذي تشهده المؤسسات حول العالم، أصبحت أنظمة المعلومات تمثل العمود الفقري للأداء المؤسسي، ورافعة رئيسية لتحقيق الكفاءة والابتكار. ومع هذا التوسع، تزايدت التهديدات السيبرانية وتنوعت أساليبها، مما فرض تحديات أمنية معقدة تستوجب تدخلاً استباقياً لحماية الأصول الرقمية وضمان استمرارية الأعمال، ولم يعد من الممكن تجاهل تأثير هذه التهديدات على استقرار المؤسسات أو على قدرة مشاريعها التقنية على تحقيق الأهداف المرجوة. (Zhu, 2024).

إن إدارة مخاطر الأمن السيبراني تمثل حجر الأساس في مواجهة هذه التهديدات، فهي عملية متكاملة تشمل سلسلة من الأنشطة تبدأ بتحديد المخاطر، مروراً بتقييمها وتحليل احتمالية حدوثها، ثم تخطيط الاستجابة لها، وانتهاءً بمتابعة فعالية المعالجة وإعادة التقييم، ولا تُعنى فقط بالجانب الفني، بل تشمل أيضاً البعد الإداري والاستراتيجي، من خلال توزيع الأدوار، وتحديث السياسات، وتعزيز ثقافة الوعي الأمني داخل المؤسسة. (Jabbar et al., 2024)

وتتعدد أبعاد إدارة مخاطر الأمن السيبراني لتشمل أدوات التحليل الكمي والنوعي، والتخطيط الاستراتيجي للأمن، والحوكمة السيبرانية، واستخدام الحلول الذكية مثل التعلم الآلي والتحليلات التنبؤية، كما أن دمج هذه الأبعاد في أنشطة المؤسسة يعزز من قدرتها على التكيف مع البيئة التقنية المتغيرة، ويمنحها مرونة أكبر في التعامل مع التهديدات الجديدة والمعقدة. (Eltaeib et al., 2024).

و تُعد كفاءة تنفيذ مشاريع الأمن السيبراني مؤشراً جوهرياً على فاعلية السياسات الأمنية للمؤسسة. فنجاح المشروع لا يُقاس فقط بمدى الانتهاء منه ضمن الجدول الزمني أو الميزانية المقررة، بل يرتبط أيضاً بجودة مخرجاته، ودرجة تحقيقه للأهداف الأمنية، وفاعلية الأنظمة الناتجة عن المشروع في التصدي للتهديدات.. (Shimizu & Hashimoto, 2025)

كفاءة تنفيذ المشاريع تتأثر بعدة عوامل، منها: وضوح نطاق المشروع، كفاءة فريق العمل، جودة الأدوات المستخدمة، وقدرة المؤسسة على التنبؤ بالمخاطر ومعالجتها مبكرًا، فكلما زادت مرونة المشروع في التعامل مع المتغيرات الأمنية، زادت فرصته في النجاح وتحقيق أهدافه التشغيلية والأمنية .

(Al Jarrah et al., 2022)

فالعلاقة بين إدارة المخاطر وكفاءة تنفيذ المشاريع ليست علاقة عرضية أو مؤقتة، بل هي علاقة جوهرية تقوم على التكامل والتفاعل المستمر، فكل مرحلة من مراحل المشروع تتطلب إدراكًا للمخاطر المحتملة، وتخطيطًا وقائيًا للحد منها، ومتابعة دقيقة لآثارها، وعند غياب هذا الارتباط، فإن المشروع يصبح عرضة للانحراف، أو الفشل في مواجهة الهجمات السيبرانية المتقدمة Prikhodko et al., 2024).

ومن هذا المنطلق، تبرز أهمية الدمج المنهجي بين أنشطة إدارة المخاطر وخطط تنفيذ المشاريع، خاصةً في المشاريع ذات الطبيعة الأمنية، مثل مشاريع الأمن السيبراني. فهذه المشاريع تتطلب تكاملًا عاليًا بين الفرق الفنية والإدارية، واستجابة سريعة للمتغيرات، وتخطيطًا دقيقًا للتعامل مع الاحتمالات غير المتوقعة، وكل ذلك لن يتحقق إلا من خلال تطبيق فعال لممارسات إدارة المخاطر داخل منظومة المشروع.

وعليه، فإن هذا البحث يسعى إلى فهم العلاقة بين إدارة مخاطر الأمن السيبراني وكفاءة تنفيذ مشاريع الأمن السيبراني في بيئة مؤسساتية قائمة على التكنولوجيا، وذلك من خلال دراسة تطبيقية تركز على شركات تقنية المعلومات في مدينة الرياض، سعيًا لتقديم تصور واضح يُسهم في تحسين أداء هذه المشاريع، وتفعيل الدور الوقائي والتنموي لإدارة المخاطر داخل بيئة العمل الرقمية.

مشكلة الدراسة:

في ظل التحولات الرقمية المتسارعة التي تشهدها مؤسسات الأعمال، برزت مشاريع الأمن السيبراني كأحد المحاور الحيوية في حماية البنية التحتية للمعلومات، إلا أن هذه المشاريع باتت تواجه تحديات معقدة، لا سيما في مراحل التنفيذ، إذ أشارت عدة تقارير مهنية إلى تزايد معدلات تعثر مشاريع الأمن السيبراني نتيجة القصور في دمج إدارة المخاطر السيبرانية بشكل منهجي ضمن دورة حياة المشروع (Al-Janabi, Jabbar & Syms, 2024).

ويظهر ذلك بوضوح في ضعف الالتزام الزمني، وتجاوز الميزانيات، وضعف المرونة أمام التهديدات المتجددة، وهو ما يتطلب إعادة النظر في العلاقة بين كفاءة التنفيذ ومنهجيات إدارة المخاطر السيبرانية، و تتفق الدراسات الحديثة (Jabbar et al., 2024; Zhu, 2024; Araujo et al., 2024) على أن دمج ممارسات إدارة المخاطر السيبرانية مثل التقييم الاستباقي، والتحليلات التنبؤية، والاستجابة التلقائية — يسهم بشكل مباشر في تحسين تنفيذ المشاريع من حيث الجودة والمرونة والتكلفة، إلا أن هذه الممارسات غالبًا ما تُطبق بصورة جزئية أو غير مهيكلية، وتركز على الجوانب التقنية فقط دون ربطها بالأطر الإدارية والحوكومية.

و تُظهر الدراسات كدراسة (Al Jarrah et al. (2022 أن دمج إدارة المخاطر ضمن العمليات المؤسسية يعزز من فرص نجاح المشاريع ويقلل من الانحرافات الزمنية والمالية ، وما زال هذا التكامل محدودًا في البيئة المحلية، خاصة في شركات تقنية المعلومات السعودية، التي تُعد في موقع متقدم من حيث الاعتماد على البنية الرقمية، لكنها لا تزال تعاني من فجوات مؤسسية في مجال إدارة المخاطر، سواء من حيث الكفاءة أو المشاركة القيادية في التخطيط والتوجيه.(Eltaeib et al., 2024)

عند فحص الممارسات الفعلية في شركات تقنية المعلومات بالرياض، يلاحظ وجود اعتماد على أدوات حماية تقنية متقدمة، لكن دون ربطها بمنهجية شاملة لإدارة المخاطر تنطلق من تحديد المخاطر إلى التعلم المؤسسي من الحوادث، كما أن مؤشرات الأداء الخاصة بالمشاريع لا ترتبط غالبًا بمؤشرات إدارة المخاطر، مما يجعل تقييم كفاءة التنفيذ منفصلاً عن واقع التهديدات السيبرانية، وهذا الانفصال يُعد أساساً جوهرياً لمشكلة الدراسة، حيث يُطرح التساؤل حول ما مدى تأثير إدارة مخاطر الأمن السيبراني على كفاءة تنفيذ مشاريع الأمن السيبراني في البيئة السعودية؟

أهمية الدراسة:

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي :

أولاً: الأهمية العلمية (النظرية):

- ✓ تسهم الدراسة في إثراء الأدبيات النظرية العربية حول العلاقة بين إدارة المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني، وهو مجال بحثي حديث نسبياً في السياق المحلي.
- ✓ تُعد الدراسة من أوائل الأبحاث التطبيقية التي تدمج بين مفاهيم إدارة المشاريع والأمن السيبراني ضمن إطار واحد في بيئة تقنية سعودية.
- ✓ تقدم الدراسة نموذجاً تحليلياً واضحاً يمكن الاعتماد عليه في دراسات لاحقة لفحص العلاقة بين أبعاد إدارة المخاطر (مثل التحديد، التحليل، الاستجابة، المراقبة) ومؤشرات كفاءة التنفيذ.
- ✓ تفتح المجال أمام بحوث مقارنة مستقبلية بين البيئات التنظيمية المختلفة في ما يتعلق بإدارة المخاطر في المشاريع السيبرانية.

الأهمية العملية:

- ✓ توفر الدراسة دليلاً تطبيقياً يمكن الاستفادة منه في مؤسسات تقنية المعلومات لتحسين فعالية وكفاءة تنفيذ مشاريع الأمن السيبراني.
- ✓ تساعد النتائج على دعم متخذي القرار ومديري المشاريع في تبني ممارسات فعالة لإدارة المخاطر وتقليل الهدر المالي والزمني.
- ✓ تقدم الدراسة أدوات ومعايير تقييم واضحة تساعد على قياس جاهزية المؤسسات من حيث إدارة المخاطر السيبرانية.
- ✓ تواكب الدراسة توجهات المملكة نحو تعزيز التحول الرقمي وضمان استدامته من خلال الأمن السيبراني، بما يخدم رؤية السعودية 2030.
- ✓ تدعم تطوير قدرات العاملين في مجال المشاريع التقنية من خلال التركيز على ممارسات استباقية تحد من تأثير التهديدات.

أهداف الدراسة:

- تهدف هذه الدراسة إلى تحليل العلاقة بين إدارة المخاطر بأبعادها المختلفة وكفاءة تنفيذ مشاريع الأمن السيبراني في شركات تقنية المعلومات بمدينة الرياض، وتتفرع منه عدة أهداف فرعية :
- ✓ التعرف على مستوى تطبيق ممارسات إدارة المخاطر في مشاريع الأمن السيبراني لدى شركات تقنية المعلومات بالرياض.
 - ✓ تحليل أبعاد إدارة المخاطر المتمثلة في (تحديد المخاطر، تحليلها، الاستجابة لها، المراقبة) كما يتم تطبيقها فعلياً في البيئة المؤسسية.

- ✓ قياس كفاءة تنفيذ مشاريع الأمن السيبراني من حيث الالتزام بالوقت والتكلفة، وجودة المخرجات، وتحقيق الأهداف الأمنية.
- ✓ استكشاف العلاقة بين جودة إدارة المخاطر ومرونة المشاريع في التكيف مع التهديدات والمتغيرات السيبرانية.
- ✓ تقديم توصيات لتحسين أداء تنفيذ المشاريع الأمنية من خلال تطوير منظومة إدارة المخاطر داخل بيئة العمل التقنية.

تساؤلات الدراسة

- ما العلاقة بين إدارة المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني في شركات تقنية المعلومات بمدينة الرياض؟ ، ويتفرع منه عدد من الأسئلة الفرعية، تتمثل في:
- ✓ ما مدى تطبيق ممارسات إدارة المخاطر بأبعادها المختلفة (تحديد المخاطر، تحليلها، الاستجابة لها، مراقبتها) في مشاريع الأمن السيبراني؟
- ✓ ما مستوى كفاءة تنفيذ مشاريع الأمن السيبراني في شركات تقنية المعلومات من حيث (الالتزام بالوقت، التحكم في التكاليف، جودة المخرجات، مرونة التنفيذ، وتحقيق الأهداف الأمنية)؟
- ✓ ما مدى تأثير كل بُعد من أبعاد إدارة المخاطر على كفاءة تنفيذ مشاريع الأمن السيبراني؟
- ✓ ما أبرز التحديات التي تواجه تطبيق إدارة فعالة للمخاطر في مشاريع الأمن السيبراني في بيئة العمل المحلية؟
- ✓ ما التوصيات المقترحة لتحسين كفاءة تنفيذ مشاريع الأمن السيبراني من خلال تعزيز إدارة المخاطر؟

فروض الدراسة:

توجد علاقة ذات دلالة إحصائية بين إدارة المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني في شركات تقنية المعلومات بمدينة الرياض. ويتفرع منه عدد من فرضيات الفرعية، تتمثل في:

✓ H1-1: توجد علاقة ذات دلالة إحصائية بين تحديد المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني.

✓ H1-2: توجد علاقة ذات دلالة إحصائية بين تحليل وتقييم المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني.

✓ H1-3: توجد علاقة ذات دلالة إحصائية بين استجابة المخاطر (التخفيف والمعالجة) وكفاءة تنفيذ مشاريع الأمن السيبراني.

✓ H1-4: توجد علاقة ذات دلالة إحصائية بين مراقبة ومراجعة المخاطر وكفاءة تنفيذ مشاريع الأمن السيبراني.

نموذج الدراسة

استنادًا إلى الدراسات مثل (Jabbar et al. ، Shimizu & Hashimoto (2025)، (2024)، (2024)، Eltaeib et al. (2024)، Rekunen et al. (2024)، وغيرها،

يمكن تصنيف أبعاد إدارة المخاطر في مشاريع الأمن السيبراني على النحو التالي:

✓ تحديد المخاطر (Risk Identification): التعرف المسبق على أنواع المخاطر السيبرانية المحتملة مثل الثغرات، والهجمات، ونقاط الضعف البشرية والتقنية.

✓ تحليل وتقييم المخاطر (Risk Analysis and Assessment): تقدير شدة وتأثير المخاطر المحتملة من حيث احتمالية الحدوث وحجم الضرر، باستخدام أدوات تحليل مثل CVSS ، EPSS، تقييم الأثر.

✓ استجابة المخاطر (Risk Response/ Mitigation): تطوير استراتيجيات وخطط للتعامل مع المخاطر المكتشفة، سواء عبر المنع، أو التخفيض، أو القبول، أو التحويل.

✓ مراقبة ومراجعة المخاطر (Monitoring and Review): المتابعة المستمرة لتغير طبيعة التهديدات وتحديث التقييمات والخطط، ضمن دورات مراجعة دورية.

ثانيًا: أبعاد المتغير التابع – كفاءة تنفيذ مشاريع الأمن السيبراني

استنادًا إلى دراسات مثل (Al-Janabi et al. (2024) ، (Latif (2024) ، (Alshehhi et al. (2024) ، (Prihodko et al. (2024) ، يمكن تصنيف أبعاد كفاءة التنفيذ في مشاريع الأمن السيبراني كما يلي:

✓ الالتزام بالجدول الزمني (Schedule Adherence): تنفيذ المهام ضمن الإطار الزمني المحدد دون تأخير.

✓ التحكم في التكاليف (Cost Control): إتمام المشروع ضمن الميزانية المحددة وتقليل الهدر المالي الناتج عن سوء التقدير أو الاستجابة الطارئة.

✓ تحقيق أهداف الأمان (Cybersecurity Goal Achievement): تنفيذ المشروع مع تحقيق الأهداف الأمنية المرجوة مثل حماية البيانات، تقليل عدد الحوادث، وتعزيز البنية التحتية.

✓ مرونة التنفيذ (Implementation Flexibility): قدرة المشروع على التكيف مع التغيرات

المفاجئة (تهديدات جديدة، تغييرات تنظيمية، تحديثات تقنية).

✓ جودة المخرجات (Output Quality): مدى التزام مخرجات المشروع (مثل النظام الأمني، أو

السياسة الأمنية) بالموصفات التقنية والمعايير المعتمدة.

✓ رضا أصحاب العلاقة (Stakeholder Satisfaction): قياس رضا الفرق الفنية، والإدارة،

والمستخدمين النهائيين عن نتائج المشروع ومدى توافقها مع التوقعات.

الدراسات السابقة:

دراسة Shimizu & Hashimoto (2025)

هدفت الدراسة إلى التعرف على أثر دمج أدوات تقييم الثغرات بأبعادها (المعرفة الثغرات المنقذة KEV ،
التنبؤ باستغلالها EPSS ، وشدتها التقنية CVSS) على كفاءة إدارة الثغرات في المؤسسات،
واستخدمت الدراسة المنهج التجريبي التطبيقي عبر تحليل كمي للبيانات، وتكوّنت العينة من 28,377
ثغرة مأخوذة من قواعد بيانات عالمية خلال 13 شهرًا.

وتوصلت نتائج الدراسة إلى أن الإطار المدمج قلل الحاجة إلى المعالجة العاجلة بنسبة 95%، ورفع
كفاءة التحديد والمعالجة بمعدل 14-18 ضعفًا مع تغطية $\leq 85\%$ من الثغرات المستغلة، وأوصت
الدراسة بتبني هذا الإطار كمنهجية قياسية في إدارة الثغرات السيبرانية داخل المؤسسات الحيوية.

دراسة Al-Janabi, Jabbar & Syms (2024)

هدفت الدراسة إلى التعرف على أثر دمج إدارة مخاطر الأمن السيبراني بأبعادها (تحديد المخاطر،
وتقييمها، وتخفيفها، والمراجعة المستمرة) ضمن دورة حياة مشاريع تكنولوجيا المعلومات على كفاءة

وأمان تنفيذ المشروع، واستخدمت الدراسة المنهج الوصفي من خلال تحليل حالة تطبيقية، وتكونت العينة من تطبيق إطار CYBITJET على مشروع نظام السجل الصحي الشخصي (PHR). وتوصلت النتائج إلى أن التطبيق المنتظم للإطار عزز الأمان ورفع مرونة التنفيذ، مما أدى إلى مستوى أمان وجودة تنفيذ أفضل، وأوصت الدراسة بضرورة دمج الإطار ضمن منهجيات إدارة مشاريع تكنولوجيا المعلومات وتوافقه مع معايير ISO/IEC 27001 و COBIT 2019 لضمان أمن وجودة أعلى.

دراسة Zhu (2024)

هدفت الدراسة إلى التعرف على أثر دمج الأطر النظرية بأبعادها (نظرية الألعاب، نظرية التحكم، والتعلم الآلي) على كفاءة استجابة المؤسسات وتصميم استراتيجيات مرنة ضد المخاطر السيبرانية، واستخدمت المنهج النظري المنهجي من خلال تحليل ومعالجة أطر نظرية متعددة، وتكونت العينة من تحليل نماذج نظرية فقط، وتوصلت الدراسة إلى أن الدمج الأولي لهذه النظريات يوفر إطارًا عمليًا لتصميم استجابات تلقائية ومرنة للهجمات، وأوصت بتحويل تلك الأطر إلى أدوات تنفيذية فعالة ضمن بيئة المؤسسات لتعزيز استراتيجيات الأمن السيبراني.

دراسة Araujo et al. (2024)

هدفت الدراسة إلى التعرف على أثر دمج مراحل إدارة المخاطر بأبعادها (الاستعداد، والرصد والكشف، والمقاومة، والاستجابة، والتعافي، والتعلم) على كفاءة تنفيذ الاستجابة ومتابعة الهجمات السيبرانية لدى المؤسسات؛ واستخدمت المنهج النظري المنهجي استنادًا إلى مراجعة أدبية لكُتب ومقالات علمية بين 2015 و2023؛ وتكونت العينة من 62 ورقة علمية تم تحليلها.

وتوصلت النتائج إلى تحديد ست مراحل أساسية للمرونة السيبرانية التي تدعم كفاءة التنفيذ الكامل؛ وأوصت الدراسة بإدماج هذه المراحل في عمليات إدارة المخاطر والاستجابة كإطار معياري مؤسسي

دراسة (Jabbar et al. 2024)

هدفت الدراسة إلى التعرف على أثر دمج تقنيات الذكاء الاصطناعي بأبعاده (التحليلات التنبؤية، والتعلم الآلي، والاستجابة التلقائية للحوادث) على كفاءة إدارة مخاطر الأمن السيبراني في مشاريع تكنولوجيا المعلومات، وذلك في سياق مواجهة التهديدات المتزايدة والمعقدة. واستخدمت الدراسة المنهج التحليلي التطبيقي من خلال تصميم إطار عمل مدمج يتضمن التكامل بين تقنيات الذكاء الاصطناعي والمبادئ التقليدية لإدارة المشاريع، وتكونت العينة من حالات تطبيق افتراضية في مجالات متعددة مثل الطب الشرعي والرعاية الصحية.

وتوصلت نتائج الدراسة إلى أن دمج الذكاء الاصطناعي ضمن الإطار يساهم في التقييم الاستباقي للمخاطر، وكشف التهديدات في الوقت الحقيقي، والاستجابة التلقائية للحوادث، مما يعزز من مرونة المشاريع في مواجهة التهديدات السيبرانية المتطورة، وأوصت الدراسة بتعميم تطبيق الإطار في المشاريع ذات الحساسية العالية للبيانات ضمن القطاعات الحيوية.

دراسة (Eltaeib et al. 2024)

هدفت الدراسة إلى التعرف على أثر تبني إستراتيجية شاملة لإدارة مخاطر الأمن السيبراني بأبعادها (التخطيط الاستراتيجي، إشراك أصحاب المصلحة، وتمكين الحوكمة العليا) على قدرة المؤسسات في الوقاية من التهديدات السيبرانية والتعامل معها بفعالية في بيئات تقنية متغيرة، وذلك انطلاقاً من الحاجة إلى تجاوز حصر إدارة الأمن في أقسام تكنولوجيا المعلومات فقط، واستخدمت الدراسة المنهج التحليلي النظري من خلال تصميم إطار استراتيجي شامل يربط بين الأدوار القيادية وممارسات الأمن، وتكونت العينة من مراجعة ممارسات مؤسسية نموذجية وتحليل ثغراتها التنظيمية.

وتوصلت نتائج الدراسة إلى أن إشراك مجالس الإدارة وأصحاب القرار في التخطيط الأمني يعزز من صمود المؤسسات أمام التهديدات، وأن غياب التفاعل المؤسسي الكامل يُعد نقطة ضعف خطرة في أي نظام حماية. وأوصت الدراسة بتبني إطار متكامل لإدارة المخاطر السيبرانية يشمل التخطيط المؤسسي طويل المدى، وتفعيل دور الحوكمة، وإعادة النظر في توزيع المسؤوليات الأمنية لتصبح مؤسسية لا فنية فقط.

دراسة (Rekunen et al. (2024

هدفت الدراسة إلى التعرف على أثر تطبيق استراتيجيات إدارة المخاطر بأبعادها (التهديدات السيبرانية، الامتثال التنظيمي، الكفاءة التشغيلية، التكيف السوقي، الاستقرار المالي، التخطيط الاستراتيجي، وإدارة الموارد البشرية) على تعزيز القدرة التنافسية والمرونة المؤسسية في شركات تكنولوجيا المعلومات. واستخدمت الدراسة المنهج النوعي التحليلي بالاعتماد على تحليل ثيمي للأدبيات والتقارير الصناعية ومصادر البيانات الثانوية، وتكوّنت العينة من مراجعة تحليلية لوثائق وتقارير صادرة عن شركات رائدة في مجال تكنولوجيا المعلومات، ودراسات سابقة تغطي المخاطر الشائعة في هذا القطاع.

وتوصلت نتائج الدراسة إلى أن اعتماد إدارة مخاطر شاملة تشمل الأمن السيبراني والامتثال والتخطيط المالي يُعدّ أحد العوامل الحاسمة في الحفاظ على التنافسية والقدرة على التكيف مع بيئة تكنولوجيا متغيرة وسريعة النمو، كما أكدت على ضرورة إدارة المواهب البشرية كجزء من معادلة الصمود المؤسسي، وأوصت الدراسة بدمج إدارة المخاطر ضمن الرؤية الاستراتيجية للمؤسسة، وتحديث الأدوات باستمرار، مع توسيع الدراسات المستقبلية لتشمل أثر التكنولوجيا الناشئة وتغير أنماط التهديدات على فاعلية الاستراتيجيات.

دراسة (Al Jarrah et al. (2022

هدفت الدراسة إلى التعرف على أثر تكامل عمليات إدارة المشروع بأبعادها (بدء المشروع، التخطيط، التنفيذ، المراقبة والتحكم، والإغلاق) على نجاح تنفيذ المشروع في الأردن، مع اعتبار إدارة مخاطر المشروع كمتغير وسيط، واستخدمت الدراسة المنهج الكمي التحليلي، من خلال توزيع استبانة مكونة من ثلاثة محاور على عينة مكونة من 96 مدير مشروع منتمين إلى نقابة المهندسين الأردنيين، جمعية المقاولين الأردنيين، ومركز الملك عبدالله للتصميم والتطوير، وتكونت العينة من مشاريع إنشائية وهندسية متنوعة تمثل القطاع العام والخاص. وأُجريت التحليلات باستخدام برنامج Partial Least Squares (PLS 3.3.3).

وتوصلت نتائج الدراسة إلى أن إدارة مخاطر المشروع تلعب دورًا وسيطًا ذا دلالة إحصائية بين عمليات إدارة المشروع ونجاح تنفيذ المشروع، حيث تبين أن دمج ممارسات إدارة المخاطر ضمن خطوات المشروع يساهم في تحسين جودة التنفيذ وتقليل الفجوات المرتبطة بالزمن والتكلفة، وأوصت الدراسة بضرورة اعتماد منهج متكامل يربط إدارة المشروع بإدارة المخاطر كجزء أساسي في ثقافة تنفيذ المشاريع، خصوصًا لدى مديري المشاريع في الأردن.

دراسة (Al-Janabi et al. (2024)

هدفت الدراسة إلى التعرف على أثر دمج متطلبات الأمن السيبراني بأبعاده (الدمج المرحلي، الحوكمة، وإدارة المخاطر السيبرانية) على كفاءة تنفيذ مشاريع تكنولوجيا المعلومات في سياق إدارة دورة حياة المشروع، وذلك عبر تطوير إطار عمل متكامل يراعي الأمان منذ مراحل التخطيط وحتى إنهاء المشروع، واستخدمت الدراسة المنهج التطبيقي من خلال تصميم إطار "الإدارة السيبرانية القادرة على التكيف" وتطبيقه فعليًا عبر دراسة حالة على نظام السجل الصحي الشخصي (PHR). وتكونت العينة من سلسلة مراحل مشروع PHR كمثال واقعي لاختبار الإطار المقترح.

وتوصلت نتائج الدراسة إلى أن دمج ممارسات الأمن السيبراني في كل مرحلة من مراحل المشروع يعزز من الوضع الأمني العام، ويزيد من قابلية التكيف والاستجابة للمخاطر المحتملة، كما أظهر الإطار قابلية عالية للتطبيق والتوسع في قطاعات متعددة، وأوصت الدراسة بتبني الإطار كمكوّن أساسي في منهجيات إدارة مشاريع تكنولوجيا المعلومات، وضمان التكامل المستمر بين متطلبات الأمان وعمليات التطوير والتنفيذ.

دراسة (Prikhodko et al. (2024

هدفت الدراسة إلى التعرف على أثر تطبيق ممارسات إدارة مخاطر المشاريع بأبعادها (تحديد المخاطر، تحليلها، مراقبتها، وتخفيفها) على كفاءة تنفيذ المشاريع وضمان نجاحها في البيئات المتغيرة، واستخدمت الدراسة المنهج التحليلي الوصفي من خلال تحليل الإجراءات الأساسية لإدارة المخاطر في مراحل مختلفة من المشروع، وتكوّنت العينة من مراجعة تجريبية لممارسات تقييم المخاطر والتخطيط في مشروعات صناعية وهندسية متعددة.

وتوصلت نتائج الدراسة إلى أن التقييم المبكر للمخاطر وتحليلها الدقيق يساعد في تحديد تأثيراتها المحتملة وتقليل آثارها على جودة تنفيذ المشروع، كما أن الرقابة المستمرة والتخطيط الوقائي يُعدّان عنصرين حاسمين في ضمان استقرار التنفيذ وتحقيق النتائج المرجوة، وأوصت الدراسة بضرورة دمج أدوات تحليل المخاطر ضمن جميع مراحل إدارة المشروع، والتأكيد على تدريب الفرق على أساليب السيطرة الوقائية لضمان أقصى درجات الفعالية.

دراسة (Alshehhi et al. (2024

هدفت الدراسة إلى التعرف على أثر تطبيق إدارة المخاطر بأبعادها (تحديد المخاطر، تصنيفها، التخفيف الاستباقي، واستخدام التحليلات التنبؤية) على كفاءة تنفيذ مشاريع البناء، وذلك في ضوء

التحديات المتكررة التي تواجه هذا القطاع مثل التأخيرات وتجاوز الميزانيات، واستخدمت الدراسة المنهج الوصفي التحليلي، من خلال تحليل بيانات مشاريع بناء متنوعة ومقارنة مستويات الأداء بين المشاريع التي تبنت ممارسات استباقية في إدارة المخاطر وتلك التي لم تطبقها، وتكوّنت العينة من مشروعات بناء مختلفة في بيئات متقاربة، خضعت لقياسات الكفاءة والفعالية.

وتوصلت نتائج الدراسة إلى وجود علاقة إيجابية قوية بين تبني إدارة مخاطر استباقية وارتفاع كفاءة تنفيذ المشروع، إذ أظهرت المشاريع التي اعتمدت هذه الممارسات انخفاضاً ملحوظاً في التأخيرات والتكاليف الزائدة، وزيادة القدرة على التكيف مع الظروف الطارئة، وأوصت الدراسة بأهمية اعتماد استراتيجيات إدارة المخاطر المبكرة، وتدريب أصحاب المصلحة على أساليب التقييم والتقليل، إضافة إلى دمج الحلول التقنية مثل التحليلات التنبؤية ونماذج المحاكاة لتحسين اتخاذ القرار في إدارة المشاريع.

دراسة (Babenko et al. (2022

هدفت الدراسة إلى التعرف على أثر تطبيق نموذج قائم على المعرفة لإدارة مخاطر مشاريع تكنولوجيا المعلومات بأبعاده (قواعد البيانات الخاصة بالمخاطر، مستودعات المعرفة، التحديث التفاعلي للمعلومات، والتعلم من الخبرات المكتسبة) على كفاءة اتخاذ القرار وإدارة تنفيذ المشاريع التقنية في بيئة ديناميكية. واستخدمت الدراسة المنهج التطويري النظري من خلال تصميم نموذج معرفي تراكمي يعكس كيفية إدخال المعلومات وتحليلها وصياغة القواعد التفسيرية لتغذية نظام خبير مخصص لإدارة مخاطر مشاريع تكنولوجيا المعلومات، وتكوّنت العينة من تحليل وظيفي لأنظمة إدارة مشاريع قابلة للتغير في متطلباتها ومجالاتها.

وتوصلت نتائج الدراسة إلى أن استخدام قاعدة معرفية مرنة تتضمن سجلاً للمخاطر، وحلولاً سابقة، وخبرات ضمنية من أصحاب العلاقة، يسهم في تحسين آليات التنبؤ بالمخاطر واتخاذ قرارات فعالة ومبنية على معرفة تراكمية، مما يعزز قدرة المؤسسات على التعامل مع التحديات المتغيرة، وأوصت الدراسة بتبني النماذج المعرفية القائمة على الخبرة التراكمية كأداة قياسية لإدارة المخاطر في المشاريع التقنية المعقدة، وتفعيل مستودعات المعرفة المؤسسية لضمان التعلم المستمر والتحسين الذاتي في إدارة المشاريع.

دراسة (Latif 2024)

هدفت الدراسة إلى التعرف على أثر ممارسات تقييم المخاطر بأبعادها (تحديد التهديدات، التقييم الكمي والنوعي، وتحليل العوامل التنظيمية المؤثرة) على تحسين أداء المشاريع خلال مختلف مراحل دورة حياتها. واستخدمت الدراسة المنهج الكمي، من خلال إجراء استبيانات ومقابلات مع 50 من مديري المشاريع وأعضاء الفرق في مؤسسات متنوعة، بهدف جمع بيانات أولية حول ممارسات تقييم المخاطر المطبقة ومدى فعاليتها، وتكوّنت العينة من عدد من المشاريع ذات الطابع المؤسسي المتنوع (تقني، هندسي، خدمي).

وقد توصلت نتائج الدراسة إلى وجود ارتباط إيجابي بين تطبيق تقييم شامل ومنهجي للمخاطر وتحقيق أداء أعلى للمشاريع، حيث أظهرت التحليلات الإحصائية والنصية أن استخدام أدوات تقييم المخاطر يسهم في خفض التكاليف، وتقليص الانحرافات الزمنية، وتحسين التكيف مع التغيرات، وأوصت الدراسة بتعزيز ثقافة التقييم الوقائي للمخاطر في المؤسسات، وتدريب العاملين على استخدام أدوات التحليل الكمي والنوعي، إلى جانب تخصيص موارد كافية لتفعيل هذا الجانب الحيوي في إدارة المشاريع.

الفجوة البحثية:

أجمعت معظم الدراسات السابقة على أهمية إدارة المخاطر كعامل مؤثر في تحسين الأداء المؤسسي وجودة تنفيذ المشاريع، سواء في سياقات تقنية، هندسية، أو حتى تنظيمية. فعلى سبيل المثال، أكدت دراسة (labbar et al. (2024) و Eltaeib et al. (2024) على أن دمج أطر الذكاء الاصطناعي والتخطيط الاستراتيجي في إدارة مخاطر الأمن السيبراني يعزز من مرونة وكفاءة تنفيذ المشاريع التقنية، وهو ما يتفق مع توجه الدراسة الحالية نحو ربط إدارة المخاطر بمخرجات تنفيذ المشاريع السيبرانية.

كما تتفق دراسات مثل (Al Janabi et al. (2024) و Babenko et al. (2022) مع الدراسة الحالية في تبني منهج شمولي لدمج إدارة المخاطر في دورة حياة المشروع منذ المراحل الأولية، مما يعكس إدراكًا متزايدًا بأهمية التكامل بين التخطيط الأمني والإداري في المشاريع التقنية.

أما على صعيد الاختلافات، فإن عددًا من الدراسات ركز على أحد الطرفين دون الربط المباشر بينهما؛ فبعضها اهتم فقط بجانب إدارة المخاطر (مثل دراسة Prikhodko et al., 2024 و Rekunen et al., 2024)، بينما ركزت دراسات أخرى على كفاءة تنفيذ المشاريع من منظور تقني عام دون

تخصيصها لمشاريع الأمن السيبراني، مثل دراسة (Latif (2024) و Alshehhi et al. (2024).

إضافة إلى ذلك، تختلف الدراسة الحالية عن الدراسات السابقة من حيث البيئة التطبيقية والسياق المحلي، حيث تستهدف دراسة بيئة مشاريع الأمن السيبراني في شركات تقنية المعلومات بمدينة الرياض، بينما تباينت البيئات في الدراسات الأخرى ما بين نماذج نظرية (Zhu, 2024) ، وتحليلات مؤسسية دولية، أو دراسات حالة منفردة في بيئات خارج السعودية.

رغم تعدد الدراسات التي تناولت كلاً من "إدارة المخاطر" و"كفاءة تنفيذ المشاريع"، إلا أن قلة قليلة منها تناولت العلاقة التكاملية بين المتغيرين ضمن سياق مشاريع الأمن السيبراني تحديداً، بل وتندر تماماً الدراسات التي عالجت هذه العلاقة في بيئة عربية، خاصةً داخل المملكة العربية السعودية. كما أن الدراسات التي دمجت البعدين ركزت في أغلبها على الأطر النظرية أو دراسات الحالة غير المعممة. ومن هنا تنبع أصالة الدراسة الحالية، حيث تسعى إلى سد فجوة تطبيقية واضحة من خلال ربط إدارة المخاطر بأبعادها المختلفة بكفاءة تنفيذ مشاريع الأمن السيبراني، في بيئة محلية حديثة ومعاصرة تتمثل في شركات تقنية المعلومات بالرياض، بما يعزز من إمكانية بناء إطار عملي قابل للتطبيق في مختلف القطاعات الحيوية داخل المملكة.

المنطلقات النظرية للدراسة:

أولاً: إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management

في ظل التحول الرقمي المتسارع والتكامل العميق لتقنيات المعلومات في العمليات المؤسسية، باتت إدارة مخاطر الأمن السيبراني عنصراً حاسماً في ضمان استمرارية الأعمال وسلامة الأصول الرقمية. وقد عرّف (Jabbar et al. (2024 إدارة المخاطر السيبرانية بأنها: "إطار متكامل يشمل تحديد التهديدات السيبرانية، وتحليلها، وتقييمها، والاستجابة لها، والرقابة المستمرة على تأثيراتها المحتملة، باستخدام منهجيات تقليدية وتقنيات ذكية."

كما أشار (Eltaeib et al. (2024 إلى أن إدارة المخاطر لم تعد وظيفة تقنية بحتة بل مسؤولية مؤسسية متكاملة تستدعي تفعيل الحوكمة العليا وإشراك مجالس الإدارة في اتخاذ القرار، ما يعكس تحولاً في البنية المفاهيمية لدور إدارة الأمن داخل المؤسسات.

أبعاد إدارة المخاطر السيبرانية:

- ✓ **تحديد المخاطر: (Risk Identification):** هي العملية التي يتم من خلالها اكتشاف وتصنيف كافة أنواع التهديدات التي قد تؤثر على أصول المشروع الرقمية، وأكد Al Janabi et al. (2024) أن التحديد المبكر للمخاطر يزيد من قدرة المؤسسة على الاستجابة الفعالة والتقليل من الخسائر المحتملة.
- ✓ **تحليل وتقييم المخاطر: (Risk Assessment):** يشمل استخدام أدوات كمية ونوعية لتقدير احتمالية تحقق المخاطر وتأثيرها، وقد بينت (Latif 2024) أن اعتماد منهجيات تقييم شاملة يسهم في تحسين الأداء العام للمشروعات ورفع كفاءتها التشغيلية.
- ✓ **الاستجابة للمخاطر: (Risk Response):** تعني تصميم وتنفيذ استراتيجيات مناسبة لكل خطر، وتتراوح هذه الاستراتيجيات بين التخفيف، التجنب، التحويل، أو القبول، وأشارت دراسة (Zhu 2024) إلى فعالية استخدام نظريات التحكم والتعلم الآلي في تصميم استجابات مرنة وسريعة للهجمات.
- ✓ **الرصد والمراجعة المستمرة: (Monitoring and Review):** وهي العملية التي يتم من خلالها تتبع المخاطر بشكل دوري، وتحديث السياسات والإجراءات تبعاً لتغير المشهد السيبراني، وأوضحت Shimizu & Hashimoto (2025) أن استخدام أدوات مثل KEV و EPSS يعزز من دقة التقييم وفعالية المعالجة بنسبة تزيد عن 85%.

ثانيًا: كفاءة تنفيذ مشاريع الأمن السيبراني

تُعد كفاءة تنفيذ مشاريع الأمن السيبراني من المؤشرات الجوهرية لنجاح مؤسسات تكنولوجيا المعلومات في تحقيق الأمان الرقمي وضمان تقديم خدمات موثوقة، وقد عرّفها Al-Janabi et al. (2024)

بأنها "مستوى النجاح في تحقيق أهداف المشروع ضمن الحدود الزمنية والمالية المقررة، مع المحافظة على مستوى عالٍ من الجودة والامتثال للمتطلبات الأمنية."

وأوضحت (Alshehhi et al. (2024 أن الكفاءة التنفيذية لا تقتصر على مؤشرات الأداء التقليدية، بل تشمل القدرة على التكيف مع التهديدات السيبرانية المتغيرة والاستجابة لها بسرعة، بما يحمي سلامة البيانات واستمرارية الخدمة.

أبعاد كفاءة تنفيذ مشاريع الأمن السيبراني:

✓ **الالتزام بالجدول الزمني: (Time Efficiency)** ويقصد به قدرة المشروع على إنجاز مراحلها ضمن الإطار الزمني المخطط له. وأكدت دراسة (Alshehhi et al. (2024 أن إدارة المخاطر الاستباقية ساهمت في تقليل التأخيرات بنسبة كبيرة في مشاريع البناء، ويمكن إسقاط النتائج على المشاريع السيبرانية.

✓ **ضبط التكاليف: (Cost Control)** يشير إلى كفاءة المشروع في استخدام الميزانية دون تجاوز أو هدر، كما أوضحت (Al Jarrah et al. (2022، والتي أثبتت أن دمج إدارة المخاطر ضمن دورة حياة المشروع يقلل من الانحرافات المالية.

✓ **جودة التنفيذ الفني: (Technical Quality)** وتعني الالتزام بالمعايير التقنية والأمنية. وذكرت (Shimizu & Hashimoto (2025 أن إدخال أدوات تصنيف الثغرات التقنية ساعد في رفع جودة المعالجة والوقاية بنسبة تتجاوز 90%.

✓ **المرونة التشغيلية والاستجابة للطوارئ: (Operational Resilience)** تقيس مدى قدرة المشروع على الاستمرار في تقديم خدماته في ظل التهديدات. وقد أظهرت Araujo et al.

(2024) أن المشاريع التي اعتمدت دورة استجابة كاملة تمر بمراحل: "الاستعداد - الكشف -

المقاومة - التعافي - التعلم" تحقق قدرة أكبر على الصمود.

✓ تحقيق الأهداف الأمنية: (Security Compliance) يشمل مدى الالتزام بالمتطلبات الأمنية

والاستجابة للهجمات المحتملة. وأكدت Al-Janabi et al. (2024) أن تطبيق إطار

CYBITJET على نظام PHR أدى إلى رفع أمان النظام وجودة تسليمه في بيئة حساسة مثل

الرعاية الصحية.

المنهجية وطرق البحث:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، نظرًا لملاءمته لطبيعة الموضوع محل

البحث، والمتمثل في دراسة العلاقة بين إدارة مخاطر الأمن السيبراني وكفاءة تنفيذ مشاريع الأمن

السيبراني في شركات تقنية المعلومات بمدينة الرياض. ويُعد هذا المنهج من أكثر المناهج استخدامًا في

العلوم الإدارية والمعلوماتية، حيث يُمكن الباحث من تشخيص الواقع الفعلي للظاهرة المدروسة، ووصف

خصائصها، وتحليل أبعادها، والكشف عن طبيعة العلاقات بين المتغيرات دون تدخل مباشر في

الظروف المحيطة.

مجتمع وعينة الدراسة

سيكوّن مجتمع الدراسة من جميع العاملين في مجال إدارة مشاريع الأمن السيبراني في شركات

تقنية المعلومات بمدينة الرياض، وبشكل خاص أولئك الذين يباشرون المهام المتعلقة بإدارة المخاطر،

أمن المعلومات، وإدارة المشاريع التقنية. وقد تم اختيار هذا المجتمع نظرًا لارتباطه الوثيق بموضوع

الدراسة، ولاعتباره البيئة الأكثر تمثيلاً للتطبيقات الفعلية لممارسات إدارة مخاطر الأمن السيبراني ضمن دورة حياة المشاريع.

وسيتم اختيار عينة الدراسة باستخدام الأسلوب العشوائي الطبقي لضمان تمثيل مختلف الفئات المهنية ذات العلاقة، كـ مديري المشاريع، مسؤولي أمن المعلومات، محلي المخاطر، ومهندسي النظم. وسيحدد الحجم النهائي للعينة بناءً على معايير إحصائية مناسبة لطبيعة المجتمع، على أن يتم جمع البيانات من الأفراد الذين تنطبق عليهم شروط الدراسة من خلال استبانة محكمة.

وسيُراعى في اختيار العينة تحقيق التوزيع العادل بين المستويات الوظيفية المختلفة، بما يُعزز موضوعية النتائج ودرجة تعميمها على مجتمع الدراسة، كما سيُستخدم أسلوب الحصر الجزئي للعينة في حال كانت أعداد الفئة المستهدفة محدودة.

مصادر جمع البيانات

ستعتمد الدراسة على مصدرين أساسيين لجمع البيانات، وهما:

➤ البيانات الأولية (Primary Data):

وسيتم جمعها مباشرة من أفراد عينة الدراسة من العاملين في شركات تقنية المعلومات بمدينة الرياض، وذلك باستخدام أداة الاستبانة التي سيتم تصميمها وتطويرها بما يتوافق مع أهداف الدراسة وأبعاد متغيراتها. وستمكن هذه البيانات الباحث من استقصاء الآراء والاتجاهات الفعلية للممارسين في الميدان حول إدارة مخاطر الأمن السيبراني وكفاءة تنفيذ المشاريع، وتحليل العلاقات بين المتغيرات المدروسة.

➤ البيانات الثانوية (Secondary Data):

وستستقى من الدراسات السابقة، والمراجع النظرية، والكتب العلمية، والمقالات المحكمة، والتقارير الدولية والمهنية ذات الصلة بالموضوع، والتي نُشرت في الفترة ما بين 2021 و2025. وسيتم توظيف هذه البيانات في بناء الإطار النظري للدراسة، وتحديد المتغيرات وأبعادها، وصياغة الفروض والأسئلة، ومقارنة نتائج الدراسة الحالية بالبحوث السابقة بهدف إبراز أوجه الاتفاق والاختلاف والفجوة البحثية.

أدوات الدراسة:

ستعتمد الدراسة على الاستبانة كأداة رئيسية لجمع البيانات الأولية من عينة الدراسة، نظرًا لما تتميز به من سهولة في التوزيع، وسرعة في جمع البيانات، وملاءمة لقياس اتجاهات وآراء الأفراد حول الظواهر الإدارية والفنية، لا سيما عند التعامل مع متغيرات مثل "إدارة مخاطر الأمن السيبراني" و"كفاءة تنفيذ المشاريع".

وسيتم بناء الاستبانة استنادًا إلى الإطار النظري والدراسات السابقة ذات العلاقة، بحيث تشمل محورين رئيسيين:

- المحور الأول: يقيس أبعاد إدارة مخاطر الأمن السيبراني (مثل: تحديد المخاطر، تقييمها، تخفيفها، المراجعة المستمرة).
 - المحور الثاني: يقيس أبعاد كفاءة تنفيذ مشاريع الأمن السيبراني (مثل: الالتزام الزمني، الالتزام المالي، جودة التنفيذ، تحقيق الأهداف الأمنية، ومرونة التكيف).
- وسيتم إعداد فقرات الاستبانة بصيغة مغلقة باستخدام مقياس ليكرت الخماسي (من 1 = لا أوافق بشدة، إلى 5 = أوافق بشدة)، بما يتيح قياس مدى الاتفاق مع كل فقرة بدقة كمية قابلة للتحليل.

كما سيتم عرض الاستبانة على مجموعة من المحكمين المتخصصين في مجالات الإدارة وتكنولوجيا المعلومات والأمن السيبراني للتحقق من صدقها الظاهري والمنطقي، وسيُجرى اختبار الثبات الإحصائي باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) للتأكد من اتساق الفقرات داخليًا وقابليتها للاعتماد في الدراسة الميدانية..

الأساليب الإحصائية المستخدمة

سيتم تحليل البيانات التي سيتم جمعها من خلال الاستبانة باستخدام مجموعة من الأساليب الإحصائية الوصفية والاستدلالية، وذلك باستخدام برنامج SPSS أو ما يماثله من برامج التحليل الإحصائي، على النحو التالي:

1. التحليل الإحصائي الوصفي: (Descriptive Statistics) ويشمل ذلك حساب المتوسطات الحسابية، والانحرافات المعيارية، والتكرارات، والنسب المئوية، وذلك بهدف وصف خصائص عينة الدراسة وتحليل اتجاهاتها العامة نحو فقرات الاستبانة.
2. اختبار صدق وثبات الأداة:

- سيتم التحقق من الثبات الداخلي باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) لجميع أبعاد الدراسة للتأكد من اتساق الأداة.
- كما سيتم استخدام التحليل العاملي الاستكشافي (Exploratory Factor Analysis) إن لزم، للتأكد من صلاحية الفقرات لقياس المتغيرات المستهدفة.

3. التحليل الإحصائي الاستدلالي: (Inferential Statistics) ويشمل:

- اختبار الفروض باستخدام معامل الارتباط بيرسون (Pearson Correlation) لقياس قوة واتجاه العلاقة بين المتغيرات.
- الانحدار الخطي المتعدد (Multiple Linear Regression) لاختبار أثر أبعاد إدارة مخاطر الأمن السيبراني على كفاءة تنفيذ المشاريع.
- كما قد يتم استخدام تحليل التباين (ANOVA) لدراسة الفروق الدالة إحصائيًا بين استجابات المبحوثين وفقًا للمتغيرات الديموغرافية.

وستُفسَّر النتائج الإحصائية وفق مستوى دلالة معنوية ($\alpha \leq 0.05$) ، وسيتم الربط بين النتائج المستخلصة والأدبيات السابقة لتحديد مدى الاتفاق أو التباين معها.

حدود الدراسة:

- **حدود موضوعية :** ستقتصر الدراسة على تناول العلاقة بين إدارة مخاطر الأمن السيبراني بأبعادها (تحديد المخاطر، تقييمها، تخفيفها، المراجعة المستمرة، الحوكمة، والتخطيط الاستراتيجي) وكفاءة تنفيذ مشاريع الأمن السيبراني بأبعادها (الالتزام الزمني، الالتزام المالي، جودة التنفيذ، تحقيق الأهداف الأمنية، ومرونة التكيف).
- **حدود مكانية:** ستُجرى الدراسة في شركات تقنية المعلومات بمدينة الرياض، نظرًا لاحتضان المدينة لعدد كبير من الشركات الرائدة في المجال، والتي تشهد تطبيقًا عمليًا لإدارة المشاريع والعمليات الأمنية
- **حدود زمانية :** تم إعداد الدراسة في عام 2025.
- **حدود بشرية:** سيتكوّن الإطار البشري للدراسة من العاملين في مجالات إدارة المشاريع، وإدارة المخاطر، وأمن المعلومات داخل شركات تقنية المعلومات بمدينة الرياض، وتحديدًا ممن لديهم خبرة عملية في تنفيذ مشاريع الأمن السيبراني.

- Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework. *Digital*, 4(4), 866–897. <https://doi.org/10.3390/digital4040043>
- Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework. *Digital*, 4(4), 866–897. <https://doi.org/10.3390/digital4040043>
- Alshehhi, H. S. M. A., Al Mazrouei, M. A. H., & Alnuaimi, A. M. A. (2024). The Function of Risk Management in Improving Construction Project Implementation Efficiency. *International Journal of Academic Research in Business and Social Sciences*, 14(1), 1–12.
- Alvarez, A. (2023, October). *What's Missing in Your Vulnerability Management Strategy—Exploring CVSS, EPSS, KEV, and Beyond*. Medium. <https://medium.com/@alexalvarez/whats-missing-in-your-vulnerability-management-strategy>
- Alvarez, A. (2023, October). *What's Missing in Your Vulnerability Management Strategy—Exploring CVSS, EPSS, KEV, and Beyond*. Medium. <https://medium.com/@alexalvarez/whats-missing-in-your-vulnerability-management-strategy>
- Araujo, R., Cruz, T., & Proença, H. (2024). A Conceptual Model of Cyber Resilience Based on a Systematic Literature Review. *Sustainability*, 16(1), 101. <https://doi.org/10.3390/su16010101>
- Babenko, V., Kulczyk, Z., Kuzmenko, O., Petrova, M., Zavidna, L., & Syniavska, O. (2022). IT Project Risk Management Model. In *Studies in Distributed Intelligence* (pp. 29–39). Springer. https://doi.org/10.1007/978-3-030-96956-6_3
- Deloitte. (2024). *CISO's Guide to Using AI in Cybersecurity Risk Management*. Deloitte Insights. <https://www2.deloitte.com/us/en/insights/focus/cybersecurity-ai.html>
- Eltaeib, T., Abdelrahman, O. H., & Ahmed, F. (2024). Proposed Framework for a Comprehensive Cybersecurity Risk Management

Strategy. Proceedings of the International Conference on Cybersecurity & Digital Trust, 1–6.

- Iyobor, E. E., Hossain, M. M., Al-Dubai, A. Y., & Al-Dubai, S. (2024). *AI-driven Vulnerability Management Framework for Cyber–Physical Production Systems (CPPS)*. *Applied Sciences*, 14(4), 1642. <https://doi.org/10.3390/app14041642>
- Jabbar, H., Al-Janabi, S., & Syms, F. (2024). AI-Integrated Cyber Security Risk Management Framework for IT Projects. *Digital*, 4(4), 76–81. <https://doi.org/10.3390/digital4040076>
- Latif, M. H. (2024). Risk Assessment to Improve the Performance of Projects. *Deleted Journal*, 4(1), 1–13.
- Prikhodko, A. N., & Sokolova, L. V. (2024). Project Risk Management: Risks Identification, Analysis, Control and Minimization. *Scientific Bulletin of the National Mining University*, 15(2), 19–23.
- Rekunen, I., & Hural, O. (2024). Risk Management Strategies for Maintaining Competitiveness in IT Firms. *Naukovì Praci MAUP*, 3(75), 84–92.
- Shimizu, N., & Hashimoto, M. (2025). *Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2506.01220>
- Zhu, Q. (2024). *Foundations of Cyber Resilience: The Confluence of Game, Control, and Learning Theories* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2404.01205>

Mid–Ocean University

College of Management

Department of risk management



**"The Relationship Between Risk Management and the
Efficiency of Cybersecurity Project Implementation: An
Applied Study in Information Technology Companies in
Riyadh"**

Preparation:

Ibrahim Abdullah Al–Mohareb

243001040

Supervision:

Dr. Al–Faisal Abdelhamid Mohamed Hassan

1445–2025