

أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية
المعلومات في الجهات الحكومية السعودية

إعداد الطالب/

م. محمد الثقفي

إشراف/

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي:

2026

جدول المحتويات

4.....	قائمة الجداول:
5.....	فهرس الأشكال:
6.....	المستخلص:
8.....	الفصل الأول: الإطار العام للدراسة.....
8	المقدمة.....
9	مشكلة الدراسة.....
10	أهمية الدراسة.....
10.....	أولاً: الأهمية العلمية:
11	ثانياً: الأهمية التطبيقية.....
11	أهداف الدراسة:
12	تساؤلات الدراسة.....
12	فروض الدراسة.....
13	النظرية العلمية المتبعة لإعداد البحث.....
16.....	الفصل الثاني: الدراسات السابقة.....
16	مقدمة.....
17	الدراسات السابقة.....
19	الإطار النظري.....
19.....	أولاً: مفهوم إدارة المخاطر السيبرانية.....
19	ثانياً: أبعاد إدارة المخاطر السيبرانية.....
20.....	ثالثاً: مفهوم نجاح مشاريع تقنية المعلومات.....
20.....	رابعاً: العلاقة بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات.....
22.....	الفصل الثالث: منهجية الدراسة.....
22	مقدمة.....
22	المنهجية وطرق البحث.....
24	حدود البحث.....
24.....	أولاً: الحدود الموضوعية.....
24	ثانياً: الحدود البشرية.....
24.....	ثالثاً: الحدود المكانية.....
25.....	رابعاً: الحدود الزمانية.....
26.....	الفصل الرابع: النتائج والتوصيات.....
26	مقدمة.....
26	تحليل البيانات.....
26.....	فحص جودة البيانات.....
27	اختبار ثبات أداة الدراسة.....
28	التحليل الوصفي لمحاو الدراسة.....
29	تحليل الارتباط بين متغيرات الدراسة.....
30	تحليل الانحدار الخطي البسيط لاختبار الفرضية الرئيسية.....
31	تحليل الانحدار الخطي المتعدد لاختبار الفرضيات الفرعية.....

34	النتائج.....
35	التوصيات.....
38	المراجع.....
38	المراجع العربية.....
38	المراجع الأجنبية.....
39	الملاحق.....
39	ملحق (1): الاستبانة.....
39	عنوان الدراسة:.....
39	مقدمة الاستبانة:.....
39	تعليمات الإجابة:.....
42	ABSTRACT.....

قائمة الجداول:

#	اسم الجدول	رقم الصفحة
١	جدول (1-3): توزيع محاور الاستبانة وعدد العبارات	25
٢	جدول (2-3): ترميز مقياس ليكرت الخماسي	26
٣	جدول (1-4): نتائج فحص جودة البيانات	28
٤	جدول (2-4): معاملات الثبات لمحاور الدراسة	28
٥	جدول (3-4): التحليل الوصفي لمحاور الدراسة	29
٦	جدول (4-4): معاملات ارتباط بيرسون بين أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات .	30
٧	جدول (5-4) نتائج نموذج الانحدار الخطي البسيط:	31
٨	جدول (6-4): معاملات الانحدار للفرضية الرئيسة	32
٩	جدول (7-4): نتائج الانحدار الخطي المتعدد للفرضيات الفرعية	33
١٠	جدول (8-4): معاملات الانحدار لأبعاد إدارة المخاطر السيبرانية	33
١١	جدول (9-4): نتائج اختبار تعدد الارتباط الخطي VIF و Tolerance	34
١٢	جدول (10-4): ملخص نتائج اختبار فرضيات الدراسة :	35

فهرس الأشكال:

رقم الصفحة	اسم الشكل	#
16	شكل (1-1): نموذج الدراسة المقترح	١

المستخلص:

هدفت هذه الدراسة إلى تحليل أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، وذلك في ظل التوسع المتزايد في مشاريع التحول الرقمي وارتفاع مستوى الاعتماد على الأنظمة والمنصات الرقمية في تقديم الخدمات الحكومية. وقد ركزت الدراسة على أربعة أبعاد رئيسية لإدارة المخاطر السيبرانية، وهي: تحديد المخاطر السيبرانية، تقييم المخاطر السيبرانية، معالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية، كما تناولت نجاح مشاريع تقنية المعلومات من خلال مجموعة من المؤشرات المرتبطة بالالتزام بالوقت، والالتزام بالتكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية.

اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة رئيسية لجمع البيانات من عينة من العاملين في مجالات إدارة المشاريع، وتقنية المعلومات، والأمن السيبراني، والحوكمة والمخاطر في الجهات الحكومية السعودية والجهات ذات العلاقة. وقد بلغ عدد الاستجابات الصالحة للتحليل الإحصائي (80) استجابة. وتم تحليل البيانات باستخدام برنامج Jamovi من خلال مجموعة من الأساليب الإحصائية، شملت الإحصاءات الوصفية، واختبار الثبات باستخدام معامل كرونباخ ألفا، وتحليل الارتباط باستخدام معامل بيرسون، والانحدار الخطي البسيط والمتعدد.

أظهرت نتائج الدراسة أن أداة الدراسة تتمتع بدرجة عالية جداً من الثبات، حيث بلغ معامل كرونباخ ألفا للاستبانة ككل (0.966). كما أظهرت النتائج وجود علاقة ارتباط موجبة ودالة إحصائية بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات، حيث بلغ معامل الارتباط ($r = 0.645, p < 0.001$). وأوضحت نتائج الانحدار الخطي البسيط أن إدارة المخاطر السيبرانية تفسر ما نسبته (41.7%) من التباين في نجاح مشاريع تقنية المعلومات. كما بينت نتائج الانحدار الخطي المتعدد أن أبعاد إدارة المخاطر السيبرانية مجتمعة تفسر ما نسبته (44.5%) من التباين في نجاح مشاريع تقنية المعلومات.

وتوصلت الدراسة إلى أن إدارة المخاطر السيبرانية تمثل عاملاً مهماً في تعزيز فرص نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، وأن بُعد تحديد المخاطر السيبرانية يعد من أبرز الأبعاد المؤثرة في نجاح المشاريع عند تحليل الأبعاد بصورة مستقلة. وبناءً على ذلك، أوصت الدراسة بضرورة تعزيز ممارسات إدارة المخاطر السيبرانية في

مراحل تخطيط وتنفيذ ومتابعة مشاريع تقنية المعلومات، وتطوير منهجيات واضحة لتحديد وتقييم ومعالجة المخاطر السيبرانية، إضافة إلى رفع مستوى التكامل بين فرق إدارة المشاريع، والأمن السيبراني، والحوكمة والمخاطر.

الكلمات المفتاحية: إدارة المخاطر السيبرانية، نجاح مشاريع تقنية المعلومات، الجهات الحكومية السعودية، إدارة المشاريع، الأمن السيبراني، التحول الرقمي.

الفصل الأول: الإطار العام للدراسة

المقدمة

شهدت بيئة الأعمال المعاصرة تحولاً رقمياً واسع النطاق، أصبحت معه مشاريع تقنية المعلومات عنصراً رئيسياً في تطوير أداء المؤسسات وتحسين جودة الخدمات ورفع كفاءة العمليات. ولم تعد مشاريع تقنية المعلومات تقتصر على بناء الأنظمة أو تشغيل البنية التقنية فحسب، بل أصبحت وسيلة استراتيجية لدعم التحول الرقمي، وتعزيز الابتكار، وتحقيق القيمة المؤسسية، خاصة في القطاعات الحكومية التي تعتمد بشكل متزايد على الحلول الرقمية في تقديم خدماتها للمستفيدين.

وفي المملكة العربية السعودية، اكتسبت مشاريع تقنية المعلومات أهمية متزايدة في ضوء التوجه الوطني نحو التحول الرقمي وتحقيق مستهدفات رؤية المملكة 2030، حيث تسعى الجهات الحكومية إلى تطوير خدماتها الرقمية، وتحسين تجربة المستفيد، ورفع كفاءة الأداء الحكومي، وتعزيز التكامل بين الأنظمة والمنصات الرقمية. وقد أدى ذلك إلى زيادة حجم وتعقيد مشاريع تقنية المعلومات، ورفع مستوى الاعتماد عليها في تنفيذ المبادرات الاستراتيجية والخدمات الحكومية.

ومع هذا التوسع في استخدام التقنية، ظهرت تحديات جديدة ترتبط بالمخاطر السيبرانية التي قد تؤثر بشكل مباشر أو غير مباشر في نجاح مشاريع تقنية المعلومات. فالمخاطر السيبرانية لم تعد مجرد تهديدات فنية منفصلة عن إدارة المشاريع، بل أصبحت عاملاً مؤثراً في قدرة المشاريع على تحقيق أهدافها من حيث الالتزام بالوقت، وضبط التكلفة، وجودة المخرجات، واستمرارية الأعمال، ورضا أصحاب المصلحة. وتشمل هذه المخاطر الهجمات السيبرانية، وتسرب البيانات، وتعطل الأنظمة، وضعف الضوابط الأمنية، وعدم الامتثال للمتطلبات التنظيمية، وهي عوامل قد تؤدي إلى تعطيل سير المشروع أو زيادة تكاليفه أو التأثير في نتائجه النهائية.

ومن هنا تبرز أهمية إدارة المخاطر السيبرانية باعتبارها منهجية منظمة تهدف إلى تحديد المخاطر السيبرانية المحتملة، وتقييم مستوى تأثيرها واحتمالية حدوثها، ووضع آليات مناسبة لمعالجتها، ثم متابعتها ومراقبتها بصورة مستمرة. وتزداد أهمية هذه الإدارة في مشاريع تقنية المعلومات الحكومية، نظراً لحساسية البيانات، وأهمية استمرارية الخدمات، وارتباط هذه المشاريع بمتطلبات الحوكمة والامتثال والأمن السيبراني.

كما أن مفهوم نجاح مشاريع تقنية المعلومات تطور من التركيز التقليدي على مثلث الوقت والتكلفة والنطاق إلى مفهوم أكثر شمولاً يتضمن جودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية، ومدى إسهام المشروع في دعم التحول الرقمي. وبناءً على ذلك، فإن نجاح مشاريع تقنية المعلومات في الجهات الحكومية لا يعتمد فقط على الجوانب الفنية أو الإدارية، بل يتأثر كذلك بمدى قدرة الجهة على إدارة المخاطر السيبرانية التي قد تواجه المشروع خلال مراحلها المختلفة.

وانطلاقاً من ذلك، تسعى هذه الدراسة إلى تحليل أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، من خلال التركيز على أربعة أبعاد رئيسية لإدارة المخاطر السيبرانية، وهي: تحديد المخاطر السيبرانية، تقييم المخاطر السيبرانية، معالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية، وقياس مدى تأثيرها في نجاح مشاريع تقنية المعلومات.

مشكلة الدراسة

أصبحت مشاريع تقنية المعلومات في الجهات الحكومية السعودية من الركائز الأساسية لتنفيذ مبادرات التحول الرقمي وتحسين جودة الخدمات الحكومية، إلا أن هذه المشاريع تواجه مجموعة من التحديات التي قد تؤثر في قدرتها على تحقيق أهدافها. ومن أبرز هذه التحديات المخاطر السيبرانية التي قد تظهر خلال مراحل التخطيط أو التنفيذ أو التشغيل، وما قد ينتج عنها من آثار سلبية تشمل تأخير تنفيذ المشروع، أو زيادة التكاليف، أو التأثير في جودة المخرجات، أو تعطيل الخدمات الرقمية، أو إضعاف ثقة أصحاب المصلحة.

وعلى الرغم من أن الجهات الحكومية تولي اهتماماً متزايداً بالأمن السيبراني، إلا أن التعامل مع المخاطر السيبرانية في بعض مشاريع تقنية المعلومات قد يظل مرتبطاً بالجوانب الفنية فقط، دون دمج بصورة كافية ضمن عمليات إدارة المشروع منذ مراحلها الأولى. وقد يؤدي هذا الفصل بين إدارة المشروع وإدارة المخاطر السيبرانية إلى ضعف القدرة على التنبؤ بالمخاطر، أو تقدير أثرها، أو وضع خطط استجابة فعالة لها، مما قد ينعكس سلباً على مؤشرات نجاح المشروع.

كما أن نجاح مشاريع تقنية المعلومات لم يعد يقاس فقط بمدى الالتزام بالوقت والتكلفة، بل أصبح يرتبط أيضاً بجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية، واستمرارية الخدمات الرقمية. وبناءً على

ذلك، فإن إغفال إدارة المخاطر السيبرانية أو ضعف تطبيقها قد يمثل أحد العوامل المؤثرة في نجاح مشاريع تقنية المعلومات، خاصة في البيئات الحكومية التي تتعامل مع بيانات حساسة وخدمات رقمية حيوية.

وتتمثل مشكلة الدراسة في الحاجة إلى فهم مدى تأثير إدارة المخاطر السيبرانية بأبعادها المختلفة، وهي تحديد المخاطر، وتقييمها، ومعالجتها، ومتابعتها ومراقبتها، على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. كما تسعى الدراسة إلى تحديد ما إذا كانت هذه الأبعاد تسهم في تحسين فرص نجاح المشاريع، وإلى أي مدى يمكن اعتبار إدارة المخاطر السيبرانية عاملاً مؤثراً في تحقيق نتائج أفضل لمشاريع تقنية المعلومات.

وبناءً على ما سبق، يمكن صياغة مشكلة الدراسة في السؤال الرئيس الآتي:

ما أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية؟

أهمية الدراسة

تستمد هذه الدراسة أهميتها من أهمية الموضوع الذي تتناوله، حيث أصبحت إدارة المخاطر السيبرانية من القضايا الجوهرية المرتبطة بنجاح مشاريع تقنية المعلومات، خصوصاً في ظل التوسع الكبير في التحول الرقمي داخل الجهات الحكومية السعودية. كما تبرز أهمية الدراسة من ارتباطها ببيئة عمل حكومية تعتمد بشكل متزايد على الأنظمة والمنصات الرقمية، مما يجعل المخاطر السيبرانية عاملاً مؤثراً في استمرارية الخدمات وجودة المخرجات وتحقيق أهداف المشاريع التقنية.

ويمكن توضيح أهمية الدراسة من جانبين رئيسيين، هما الأهمية العلمية والأهمية التطبيقية، وذلك على النحو الآتي:

أولاً: الأهمية العلمية:

تسهم هذه الدراسة في إثراء الأدبيات العلمية المتعلقة بإدارة المخاطر السيبرانية وإدارة مشاريع تقنية المعلومات، من خلال دراسة العلاقة بينهما في سياق الجهات الحكومية السعودية. كما تساعد الدراسة في توضيح الدور الذي يمكن أن تؤديه إدارة المخاطر السيبرانية بأبعادها المختلفة في دعم نجاح مشاريع تقنية المعلومات، وهو موضوع لا يزال بحاجة إلى مزيد من البحث والتحليل، خاصة في البيئة الحكومية.

كما تقدم الدراسة إطاراً تحليلياً يربط بين أبعاد إدارة المخاطر السيبرانية، وهي تحديد المخاطر، وتقييمها، ومعالجتها، ومتابعتها ومراقبتها، وبين مؤشرات نجاح مشاريع تقنية المعلومات، مثل الالتزام بالوقت، وضبط التكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية.

ثانيًا: الأهمية التطبيقية

تتمثل الأهمية التطبيقية للدراسة في إمكانية استفادة الجهات الحكومية السعودية من نتائجها في تحسين ممارسات إدارة المخاطر السيبرانية داخل مشاريع تقنية المعلومات. كما يمكن أن تساعد نتائج الدراسة مديري المشاريع، وفرق الأمن السيبراني، وفرق الحوكمة والمخاطر، وصناع القرار على فهم أثر المخاطر السيبرانية في نجاح المشاريع التقنية، وأهمية دمج إدارة هذه المخاطر ضمن مراحل المشروع منذ التخطيط وحتى الإغلاق.

كما يمكن أن تسهم الدراسة في دعم الجهات الحكومية عند تطوير سياسات وإجراءات أكثر فاعلية لإدارة المخاطر السيبرانية، وتحسين التنسيق بين فرق إدارة المشاريع والأمن السيبراني، بما يسهم في تقليل احتمالية تعثر المشاريع، وتعزيز جودة المخرجات، وزيادة فرص نجاح مبادرات التحول الرقمي.

أهداف الدراسة:

تهدف هذه الدراسة بصورة رئيسية إلى تحليل أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، وذلك من خلال دراسة أبعاد إدارة المخاطر السيبرانية وقياس علاقتها وتأثيرها في مؤشرات نجاح المشاريع التقنية..

وتسعى الدراسة إلى تحقيق الأهداف الفرعية الآتية:

1. التعرف على مستوى تطبيق إدارة المخاطر السيبرانية في مشاريع تقنية المعلومات في الجهات الحكومية السعودية .
2. قياس أثر تحديد المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات .
3. قياس أثر تقييم المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات .
4. قياس أثر معالجة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات .
5. قياس أثر متابعة ومراقبة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات .
6. التعرف على مستوى نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية من وجهة نظر أفراد عينة الدراسة .

7. تقديم توصيات يمكن أن تسهم في تعزيز ممارسات إدارة المخاطر السيبرانية داخل مشاريع تقنية المعلومات،

بما يدعم تحسين فرص نجاح هذه المشاريع في الجهات الحكومية السعودية

تساؤلات الدراسة

تسعى هذه الدراسة إلى الإجابة عن السؤال الرئيس الآتي:

ما أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية؟

ويتفرع من هذا السؤال الرئيس عدد من التساؤلات الفرعية، وهي:

1. ما مستوى تطبيق إدارة المخاطر السيبرانية في مشاريع تقنية المعلومات في الجهات الحكومية السعودية؟

2. ما أثر تحديد المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية؟

3. ما أثر تقييم المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية؟

4. ما أثر معالجة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية؟

5. ما أثر متابعة ومراقبة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية

السعودية؟

6. ما مستوى نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية من وجهة نظر أفراد عينة

الدراسة؟

فروض الدراسة

في ضوء مشكلة الدراسة وتساؤلاتها وأهدافها، تسعى هذه الدراسة إلى اختبار الفرضية الرئيسة الآتية:

الفرضية الرئيسة:

يوجد أثر ذو دلالة إحصائية لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية

السعودية عند مستوى دلالة إحصائية $(\alpha \leq 0.05)$

ويتفرع من الفرضية الرئيسة الفرضيات الفرعية الآتية:

1. الفرضية الفرعية الأولى:

يوجد أثر ذو دلالة إحصائية لتحديد المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية عند مستوى دلالة إحصائية $(\alpha \leq 0.05)$

2. الفرضية الفرعية الثانية:

يوجد أثر ذو دلالة إحصائية لتقييم المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية عند مستوى دلالة إحصائية $(\alpha \leq 0.05)$

3. الفرضية الفرعية الثالثة:

يوجد أثر ذو دلالة إحصائية لمعالجة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية عند مستوى دلالة إحصائية $(\alpha \leq 0.05)$

4. الفرضية الفرعية الرابعة:

يوجد أثر ذو دلالة إحصائية لمتابعة ومراقبة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية عند مستوى دلالة إحصائية $(\alpha \leq 0.05)$

النظرية العلمية المتبعة لإعداد البحث

تستند هذه الدراسة إلى مدخل إدارة المخاطر بوصفه أحد المداخل الإدارية المهمة في دعم نجاح المشاريع، حيث يقوم هذا المدخل على أن قدرة المؤسسة على تحديد المخاطر، وتحليلها، ومعالجتها، ومتابعتها بصورة منهجية تسهم في تقليل الآثار السلبية المحتملة على أهداف المشروع. ويعد هذا المدخل مناسباً لطبيعة الدراسة الحالية، نظرًا لأن مشاريع تقنية المعلومات في الجهات الحكومية السعودية تواجه مجموعة من المخاطر التقنية والتنظيمية والتشغيلية، ومن أبرزها المخاطر السيبرانية التي قد تؤثر في سير المشروع ونتائجه.

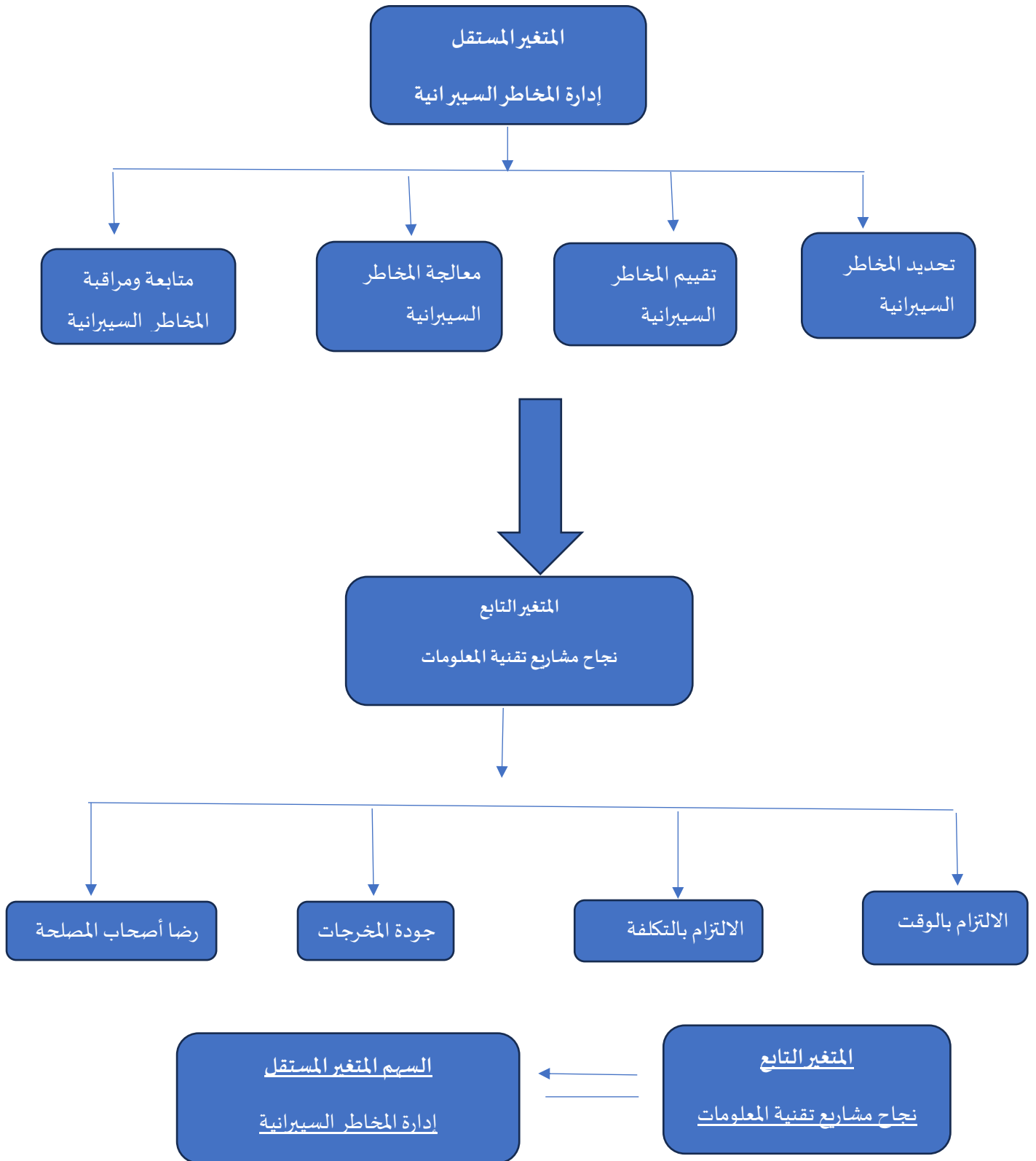
كما تعتمد الدراسة على فكرة التكامل بين إدارة المخاطر السيبرانية وإدارة مشاريع تقنية المعلومات، حيث لا ينظر إلى الأمن السيبراني باعتباره نشاطاً فنياً منفصلاً، بل باعتباره عنصراً مؤثراً في إدارة المشروع ونجاحه. فالمخاطر السيبرانية قد تؤثر في الوقت، والتكلفة، وجودة المخرجات، واستمرارية الخدمات، ورضا أصحاب المصلحة، ولذلك فإن إدارتها بصورة فعالة تمثل أحد العوامل الداعمة لتحقيق أهداف المشروع.

وتقوم الدراسة على أن إدارة المخاطر السيبرانية تمر بعدد من المراحل المترابطة، تبدأ بتحديد المخاطر السيبرانية المحتملة التي قد تواجه المشروع، ثم تقييم هذه المخاطر من حيث احتمالية الحدوث ومستوى التأثير، ثم وضع المعالجات المناسبة للحد من آثارها، وأخيراً متابعة ومراقبة هذه المخاطر خلال مراحل المشروع المختلفة. وتمثل هذه المراحل الأبعاد الرئيسة للمتغير المستقل في الدراسة.

أما المتغير التابع فيتمثل في نجاح مشاريع تقنية المعلومات، والذي لا يقتصر في هذه الدراسة على الالتزام بالوقت والتكلفة فقط، بل يشمل أيضاً جودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية، ودعم التحول الرقمي. وبناءً على ذلك، تفترض الدراسة أن وجود ممارسات فعالة لإدارة المخاطر السيبرانية يسهم في تعزيز فرص نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية.

وبناءً على ما سبق، تم بناء نموذج الدراسة على أساس وجود أثر لإدارة المخاطر السيبرانية، بأبعادها الأربعة، على نجاح مشاريع تقنية المعلومات.

ويوضح الشكل الآتي نموذج الدراسة المقترح:



شكل (1-1): نموذج الدراسة المقترح

الفصل الثاني: الدراسات السابقة

مقدمة

يتناول هذا الفصل عرضًا للأدبيات والدراسات السابقة ذات العلاقة بموضوع الدراسة، وذلك بهدف بناء خلفية علمية تسهم في فهم أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات. وتكتسب مراجعة الدراسات السابقة أهمية خاصة في هذه الدراسة، نظرًا لتداخل موضوعها بين أكثر من مجال معرفي، يتمثل في إدارة المشاريع، وإدارة المخاطر، والأمن السيبراني، والتحول الرقمي في القطاع الحكومي.

وتعد إدارة المخاطر السيبرانية من الموضوعات التي حظيت باهتمام متزايد في الأدبيات الحديثة، خاصة مع تصاعد الاعتماد على الأنظمة الرقمية وازدياد التهديدات السيبرانية التي قد تؤثر في استمرارية الأعمال وجودة الخدمات الرقمية. وتشير الأطر المهنية الحديثة إلى أن إدارة المخاطر السيبرانية تتطلب منهجية منظمة تشمل تحديد المخاطر، وتقييمها، ومعالجتها، ومتابعتها بصورة مستمرة، بما يسهم في تعزيز قدرة المؤسسات على حماية أصولها الرقمية وتحقيق أهدافها التنظيمية. وقد أكد إطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتقنية أن إدارة المخاطر السيبرانية تمثل أحد المكونات الأساسية في حوكمة الأمن السيبراني وإدارة المخاطر المؤسسية (NIST, 2024). كما يوضح معيار ISO/IEC 27005:2022 أن إدارة مخاطر أمن المعلومات تتضمن أنشطة تقييم المخاطر ومعالجتها بما يدعم تطبيق نظام إدارة أمن المعلومات داخل المؤسسات.

ومن جهة أخرى، تمثل مشاريع تقنية المعلومات أحد المحركات الرئيسة للتحول الرقمي داخل المؤسسات، إلا أن نجاح هذه المشاريع لا يعتمد على الجوانب الفنية فقط، بل يتأثر بمجموعة من العوامل الإدارية والتنظيمية والتقنية. ومن أبرز هذه العوامل قدرة فرق المشروع على إدارة المخاطر التي قد تؤثر في الوقت، والتكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية. وفي هذا السياق، يصبح الربط بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات ضرورة بحثية، خاصة في البيئات الحكومية التي تتعامل مع بيانات وخدمات رقمية ذات أهمية عالية.

وبناءً على ذلك، يستعرض هذا الفصل الدراسات السابقة المرتبطة بمحاور الدراسة، من خلال تناول الدراسات التي بحثت إدارة المخاطر السيبرانية، والدراسات التي تناولت نجاح مشاريع تقنية المعلومات، ثم الدراسات التي ربطت بين

إدارة المخاطر أو الأمن السيبراني ونجاح المشاريع التقنية. كما يتضمن الفصل إطارًا نظريًا يوضح المفاهيم الأساسية للدراسة وأبعادها، بما يمهّد لبناء المنهجية وتحليل النتائج في الفصول اللاحقة.

الدراسات السابقة

يتناول هذا الفصل عرضًا للأدبيات والدراسات السابقة ذات العلاقة بموضوع الدراسة، وذلك بهدف بناء خلفية علمية تسهم في فهم أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات. وتكتسب مراجعة الدراسات السابقة أهمية خاصة في هذه الدراسة نظرًا لتداخل موضوعها بين أكثر من مجال معرفي، يتمثل في إدارة المشاريع، وإدارة المخاطر، والأمن السيبراني، والتحول الرقمي في القطاع الحكومي.

وقد حظيت إدارة المخاطر السيبرانية باهتمام متزايد في الأدبيات الحديثة، خاصة مع توسع المؤسسات في استخدام الأنظمة الرقمية والمنصات الإلكترونية، وما يصاحب ذلك من ارتفاع في مستوى التهديدات السيبرانية التي قد تؤثر في استمرارية الأعمال وجودة الخدمات الرقمية. وتشير الأطر المهنية الحديثة إلى أن إدارة المخاطر السيبرانية تتطلب منهجية منظمة تشمل تحديد المخاطر، وتقييمها، ومعالجتها، ومتابعتها، وربطها بحوكمة المؤسسة وإدارة المخاطر المؤسسية. ويؤكد إطار الأمن السيبراني الصادر عن NIST أن الأمن السيبراني يمثل جزءًا من إدارة المخاطر المؤسسية وليس مجرد نشاط فني مستقل، كما يوضح معيار ISO/IEC 27005 أن إدارة مخاطر أمن المعلومات تدعم بناء نظام فعال لإدارة أمن المعلومات داخل المؤسسات.

ومن جهة أخرى، تمثل مشاريع تقنية المعلومات أحد المحركات الرئيسة للتحول الرقمي داخل الجهات الحكومية، إلا أن نجاح هذه المشاريع لا يعتمد فقط على كفاءة الحلول التقنية، بل يتأثر أيضًا بقدرة فرق المشروع على إدارة المخاطر، وضبط الوقت والتكلفة، وتحقيق جودة المخرجات، وإدارة توقعات أصحاب المصلحة. وفي هذا السياق، يصبح الربط بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات مهمًا، خصوصًا في البيئات الحكومية التي تتعامل مع بيانات وخدمات رقمية ذات أهمية عالية.

وبناءً على ذلك، يستعرض هذا الفصل الدراسات السابقة المرتبطة بمحاور الدراسة، من خلال تناول الدراسات التي بحثت إدارة المخاطر السيبرانية، والدراسات التي تناولت نجاح مشاريع تقنية المعلومات، ثم الدراسات التي ربطت بين إدارة المخاطر ونجاح المشاريع التقنية، وصولًا إلى تحديد الفجوة البحثية التي تسعى الدراسة الحالية إلى معالجتها.

تناولت العديد من الدراسات موضوع إدارة المخاطر في مشاريع تقنية المعلومات، وأكدت أن وجود ممارسات واضحة لإدارة المخاطر يسهم في تقليل احتمالية تعثر المشاريع وتحسين فرص نجاحها. فقد بينت بعض الدراسات أن أسباب فشل مشاريع تقنية المعلومات غالبًا ما ترتبط بعدم كفاية التخطيط، وضعف إدارة المخاطر، وعدم وضوح المتطلبات، وضعف التنسيق بين أصحاب المصلحة. كما أوضحت دراسة حديثة حول آليات الحد من فشل مشاريع تقنية المعلومات أن تحليل أسباب الفشل السابقة يمكن أن يساعد المؤسسات في بناء آليات أكثر فاعلية لتخفيف المخاطر في المشاريع الجديدة.

كما أشارت دراسات أخرى إلى أن نجاح مشاريع تقنية المعلومات لا يمكن قياسه من خلال الوقت والتكلفة والنطاق فقط، بل يجب النظر إليه من منظور أوسع يشمل جودة المخرجات، ورضا المستخدمين، وتحقيق القيمة المتوقعة،

ودعم الأهداف التنظيمية. وقد بينت دراسة حول قياس نجاح مشاريع تقنية المعلومات أن مفهوم النجاح في المشاريع التقنية يتضمن أبعادًا متعددة، مما يؤكد أهمية استخدام مؤشرات متنوعة عند تقييم نجاح هذه المشاريع .

وفي مجال إدارة المخاطر، أوضحت دراسة تناولت أثر ممارسات إدارة المخاطر على نجاح مشاريع تقنية المعلومات أن ممارسات إدارة المخاطر، مثل تحديد المخاطر وتقييمها والاستجابة لها، ترتبط إيجابيًا بأداء المشاريع التقنية ونجاحها. وتؤكد هذه النتيجة أن إدارة المخاطر لا تعد نشاطًا إداريًا ثانويًا، بل تمثل عاملاً مهمًا في تحسين قدرة المشروع على التعامل مع التحديات وتحقيق أهدافه .

أما في مجال الأمن السيبراني، فقد ركزت بعض الدراسات على أهمية دمج الأمن السيبراني ضمن مشاريع التحول الرقمي، حيث إن إغفال الجوانب الأمنية أثناء التخطيط والتنفيذ قد يؤدي إلى مخاطر تؤثر في جودة المشروع واستمراريته. وأوضحت دراسة حول الأدوار الاستراتيجية لأمن المعلومات في مشاريع الرقمنة أن التعامل مع الأمن السيبراني في المشاريع التقنية يمكن أن يكون من خلال عدة مداخل، مثل الأمن أولاً، أو الأمن بالتصميم، أو الموازنة العملية بين متطلبات الأمن ومتطلبات المشروع .

وفي السياق السعودي، تبرز أهمية الأمن السيبراني في ظل وجود متطلبات تنظيمية وطنية تستهدف حماية الأصول المعلوماتية والتقنية للجهات الوطنية. فقد أوضحت الهيئة الوطنية للأمن السيبراني أن الضوابط الأساسية للأمن السيبراني تهدف إلى تعزيز الأمن السيبراني على المستوى الوطني وحماية الأصول التقنية والمعلوماتية للجهات الوطنية. كما تؤكد هيئة الحكومة الرقمية أهمية تطوير السياسات والمعايير والنماذج التشغيلية التي تدعم التحول الرقمي والتميز في القطاع الحكومي .

وتشير الدراسات السابقة في مجملها إلى أن إدارة المخاطر، سواء كانت مخاطر عامة أو مخاطر سيبرانية، تمثل عنصرًا مؤثرًا في نجاح مشاريع تقنية المعلومات. إلا أن كثيرًا من الدراسات ركزت على إدارة المخاطر العامة أو على الأمن السيبراني كموضوع مستقل، في حين لا تزال الحاجة قائمة لدراسة أثر إدارة المخاطر السيبرانية بأبعادها المحددة على نجاح مشاريع تقنية المعلومات في بيئة الجهات الحكومية السعودية. ومن هنا تأتي الدراسة الحالية لسد هذه الفجوة من خلال اختبار أثر تحديد المخاطر السيبرانية، وتقييمها، ومعالجتها، ومتابعتها ومراقبتها، على نجاح مشاريع تقنية المعلومات.

الإطار النظري

يتناول الإطار النظري المفاهيم الرئيسة التي تقوم عليها الدراسة، والمتمثلة في إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات، إضافة إلى توضيح العلاقة النظرية بينهما. ويهدف هذا القسم إلى بناء أساس علمي يساعد في تفسير نموذج الدراسة وفرضياتها، وربطها بالأدبيات والأطر المهنية ذات العلاقة.

أولاً: مفهوم إدارة المخاطر السيبرانية

تشير إدارة المخاطر السيبرانية إلى مجموعة من العمليات المنظمة التي تهدف إلى تحديد المخاطر المرتبطة بالأصول والأنظمة الرقمية، وتحليل احتمالية حدوثها ومستوى تأثيرها، ثم اختيار المعالجات المناسبة للحد من آثارها، ومتابعتها بصورة مستمرة. وتزداد أهمية هذا المفهوم في المؤسسات التي تعتمد على الأنظمة والمنصات الرقمية في تنفيذ أعمالها وتقديم خدماتها، حيث قد تؤدي المخاطر السيبرانية إلى تعطيل الخدمات، أو تسرب البيانات، أو التأثير في استمرارية الأعمال، أو إضعاف ثقة أصحاب المصلحة.

وتؤكد الأطر المهنية الحديثة أن إدارة المخاطر السيبرانية لا ينبغي أن تكون نشاطاً فنياً منفصلاً، بل يجب أن تكون جزءاً من منظومة الحوكمة وإدارة المخاطر المؤسسية. فقد أضاف إطار الأمن السيبراني الصادر عن NIST في نسخته الثانية وظيفة الحوكمة بوصفها مكوناً أساسياً يربط إدارة المخاطر السيبرانية بتوجهات المؤسسة وأهدافها وإدارتها للمخاطر. كما يوضح معيار ISO/IEC 27005:2022 أن إدارة مخاطر أمن المعلومات تدعم تطبيق نظام إدارة أمن المعلومات من خلال منهجية منظمة لإدارة المخاطر.

ثانياً: أبعاد إدارة المخاطر السيبرانية

تعتمد هذه الدراسة على أربعة أبعاد رئيسية لإدارة المخاطر السيبرانية، وهي: تحديد المخاطر السيبرانية، تقييم المخاطر السيبرانية، معالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية. وتمثل هذه الأبعاد مراحل مترابطة تساعد المؤسسة على التعامل مع المخاطر السيبرانية بطريقة منهجية.

يتمثل البعد الأول في تحديد المخاطر السيبرانية، ويقصد به التعرف على مصادر التهديدات ونقاط الضعف والأصول الرقمية التي قد تتعرض للخطر داخل مشروع تقنية المعلومات. وتعد هذه المرحلة أساساً مهماً لبقية مراحل إدارة المخاطر، لأن عدم تحديد المخاطر بصورة دقيقة قد يؤدي إلى ضعف تقييمها أو عدم اختيار المعالجة المناسبة لها.

أما البعد الثاني فهو تقييم المخاطر السيبرانية، ويقصد به تحليل المخاطر التي تم تحديدها من حيث احتمالية حدوثها ومستوى تأثيرها المحتمل على أهداف المشروع. ويساعد هذا التقييم في ترتيب المخاطر حسب الأولوية، وتوجيه الموارد نحو المخاطر الأكثر تأثيرًا على المشروع.

ويتمثل البعد الثالث في معالجة المخاطر السيبرانية، ويقصد به اختيار وتنفيذ الإجراءات المناسبة للتعامل مع المخاطر، سواء من خلال تقليل احتمالية حدوثها، أو الحد من أثرها، أو نقلها، أو قبولها وفقًا لمستوى المخاطر المقبول لدى الجهة. وتعد معالجة المخاطر خطوة مهمة لضمان عدم تحول المخاطر السيبرانية إلى عوائق تؤثر في سير المشروع أو مخرجاته.

أما البعد الرابع فهو متابعة ومراقبة المخاطر السيبرانية، ويقصد به تتبع المخاطر القائمة والمستجدة خلال مراحل المشروع، ومراجعة فعالية الضوابط والإجراءات المتخذة، وتحديث خطط الاستجابة عند الحاجة. وتبرز أهمية هذا البعد لأن المخاطر السيبرانية تتغير باستمرار نتيجة تطور التهديدات والتقنيات وبيئة العمل الرقمية.

ثالثًا: مفهوم نجاح مشاريع تقنية المعلومات

يشير نجاح مشاريع تقنية المعلومات إلى قدرة المشروع على تحقيق أهدافه المخططة وتقديم مخرجات ذات قيمة للمؤسسة وأصحاب المصلحة. ولم يعد نجاح المشروع يقاس فقط من خلال الالتزام بالوقت والتكلفة والنطاق، بل أصبح يشمل أبعادًا أوسع مثل جودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية، ودعم التحول الرقمي.

وتؤكد أدبيات إدارة المشاريع الحديثة أن نجاح المشروع يرتبط بتحقيق القيمة وليس فقط بإنجاز الأنشطة أو تسليم المخرجات. ويظهر ذلك في التوجهات الحديثة لإدارة المشاريع التي تركز على القيمة، وأصحاب المصلحة، والتكيف مع بيئة المشروع، وتحقيق النتائج التنظيمية. ويعد هذا التوجه مهمًا في مشاريع تقنية المعلومات، لأن هذه المشاريع غالبًا ما تكون مرتبطة بتغيير تنظيمي، وتحسين الخدمات، ورفع كفاءة العمليات، وليس مجرد تنفيذ حل تقني.

رابعًا: العلاقة بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات

تقوم العلاقة النظرية بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات على أن المخاطر السيبرانية قد تؤثر في مؤشرات نجاح المشروع إذا لم تتم إدارتها بصورة فعالة. فقد يؤدي ضعف إدارة هذه المخاطر إلى تأخير تنفيذ

المشروع، أو زيادة التكلفة، أو انخفاض جودة المخرجات، أو تعطيل الأنظمة، أو التأثير في ثقة المستخدمين وأصحاب المصلحة.

وفي المقابل، فإن تطبيق ممارسات فعالة لإدارة المخاطر السيبرانية يمكن أن يساهم في تعزيز فرص نجاح مشاريع تقنية المعلومات، من خلال تحسين قدرة فرق المشروع على التنبؤ بالمخاطر، وتقدير أثارها، ووضع خطط مناسبة للتعامل معها، ومتابعتها خلال مراحل المشروع المختلفة. كما أن دمج إدارة المخاطر السيبرانية ضمن عمليات إدارة المشروع يساعد في تعزيز التنسيق بين فرق المشروع، وفرق الأمن السيبراني، وفرق الحوكمة والمخاطر.

وتكتسب هذه العلاقة أهمية خاصة في الجهات الحكومية السعودية، نظرًا لارتباط مشاريع تقنية المعلومات بالخدمات الحكومية الرقمية، وحساسية البيانات، ومتطلبات الأمن السيبراني والامتثال. وتشير الهيئة الوطنية للأمن السيبراني إلى أن الضوابط الأساسية للأمن السيبراني تستهدف تعزيز الأمن السيبراني على المستوى الوطني وحماية الأصول المعلوماتية والتقنية للجهات الوطنية، وهو ما يعكس أهمية التعامل مع الأمن السيبراني بوصفه عنصرًا جوهريًا في البيئة الحكومية الرقمية.

وبناءً على ما سبق، فإن الدراسة الحالية تفترض وجود أثر لإدارة المخاطر السيبرانية بأبعادها الأربعة على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، حيث تمثل إدارة المخاطر السيبرانية المتغير المستقل، بينما يمثل نجاح مشاريع تقنية المعلومات المتغير التابع.

الفصل الثالث: منهجية الدراسة

مقدمة

يتناول هذا الفصل منهجية الدراسة والإجراءات التي تم اتباعها لتحقيق أهداف البحث والإجابة عن تساؤلاته واختبار فرضياته. ويعرض الفصل المنهج المستخدم في الدراسة، ومجتمع البحث، وعينة الدراسة، وأداة جمع البيانات، إضافة إلى حدود الدراسة والأساليب الإحصائية المستخدمة في تحليل البيانات.

وقد اعتمدت الدراسة على منهجية كمية تهدف إلى قياس أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، وذلك من خلال جمع البيانات باستخدام الاستبانة وتحليلها إحصائيًا لاختبار العلاقة والأثر بين متغيرات الدراسة. ويعد هذا المنهج مناسبًا لطبيعة الدراسة الحالية، نظرًا لأنها تسعى إلى قياس العلاقة بين متغير مستقل يتمثل في إدارة المخاطر السيبرانية بأبعادها الأربعة، ومتغير تابع يتمثل في نجاح مشاريع تقنية المعلومات.

المنهجية وطرق البحث.

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، وذلك لملاءمته لطبيعة موضوع الدراسة وأهدافها. ويستخدم المنهج الوصفي التحليلي في وصف الظاهرة محل الدراسة وتحليل أبعادها والعلاقات بين متغيراتها، بما يساعد على فهم أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وقد تم استخدام الأسلوب الكمي في جمع وتحليل البيانات، حيث تم تصميم استبانة إلكترونية موجهة إلى العاملين في المجالات ذات العلاقة بمشاريع تقنية المعلومات، وإدارة المشاريع، والأمن السيبراني، والحوكمة والمخاطر. وهدفت الاستبانة إلى قياس مستوى تطبيق إدارة المخاطر السيبرانية وأثرها على نجاح مشاريع تقنية المعلومات من وجهة نظر أفراد عينة الدراسة.

وتتكون متغيرات الدراسة من متغير مستقل ومتغير تابع. ويتمثل المتغير المستقل في إدارة المخاطر السيبرانية، ويتضمن أربعة أبعاد رئيسية هي: تحديد المخاطر السيبرانية، تقييم المخاطر السيبرانية، معالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية. أما المتغير التابع فيتمثل في نجاح مشاريع تقنية المعلومات، والذي تم قياسه من خلال مؤشرات تشمل الالتزام بالوقت، والالتزام بالتكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية.

وقد تم تحليل البيانات باستخدام برنامج Jamovi، وذلك من خلال عدد من الأساليب الإحصائية المناسبة، شملت الإحصاءات الوصفية، ومعامل كرونباخ ألفا لاختبار ثبات أداة الدراسة، ومعامل ارتباط بيرسون لقياس العلاقة بين المتغيرات، والانحدار الخطي البسيط والمتعدد لاختبار فرضيات الدراسة.

-مجتمع البحث

يتكون مجتمع البحث من العاملين في الجهات الحكومية السعودية والجهات ذات العلاقة بمشاريع تقنية المعلومات، ممن لديهم ارتباط مباشر أو غير مباشر بمجالات إدارة المشاريع، وتقنية المعلومات، والأمن السيبراني، والحوكمة والمخاطر. ويشمل ذلك مديري المشاريع، ومديري البرامج، ومختصي الأمن السيبراني، ومختصي الحوكمة والمخاطر، ومديري تقنية المعلومات، وأعضاء مكاتب إدارة المشاريع، وغيرهم من الفئات المهنية ذات العلاقة بموضوع الدراسة. وقد تم اختيار هذا المجتمع نظرًا لارتباطه المباشر بموضوع الدراسة، حيث إن هذه الفئات المهنية تعد الأكثر قدرة على تقييم ممارسات إدارة المخاطر السيبرانية داخل مشاريع تقنية المعلومات، وبيان مدى أثر هذه الممارسات على نجاح المشاريع من حيث الالتزام بالوقت، والتكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية.

أما عينة الدراسة فقد تمثلت في عينة من العاملين في المجالات المشار إليها، ممن استجابوا للاستبانة الإلكترونية التي أعدت لهذا الغرض. وقد بلغ عدد الاستجابات الصالحة للتحليل الإحصائي (80) استجابة، وتم اعتمادها كاملة في التحليل بعد التحقق من اكتمال البيانات وعدم وجود قيم مفقودة أو أخطاء إدخال.

وتم جمع البيانات باستخدام استبانة إلكترونية صممت لقياس متغيرات الدراسة، حيث تضمنت الاستبانة محورًا خاصًا بالبيانات الديموغرافية، ومحاور تقيس أبعاد إدارة المخاطر السيبرانية، إضافة إلى محور يقيس نجاح مشاريع تقنية المعلومات. وقد استخدم مقياس ليكرت الخماسي لقياس استجابات أفراد العينة، وذلك من خلال خمس درجات تبدأ من لا أو أفق بشدة وتنتهي بـ أو أفق بشدة.

جدول (1-3): توزيع محاور الاستبانة وعدد العبارات

المحور	الرمز	عدد العبارات
تحديد المخاطر السيبرانية	CRI	5
تقييم المخاطر السيبرانية	CRA	5
معالجة المخاطر السيبرانية	CRT	5
متابعة ومراقبة المخاطر السيبرانية	CRM	5
نجاح مشاريع تقنية المعلومات	PS	15
الاجمالي	==	35

يوضح جدول (3-1) توزيع محاور الاستبانة وعدد العبارات المستخدمة في قياس متغيرات الدراسة. وقد بلغ إجمالي عدد عبارات الاستبانة (35) عبارة، منها (20) عبارة لقياس أبعاد إدارة المخاطر السيبرانية، و(15) عبارة لقياس نجاح مشاريع تقنية المعلومات.

حدود البحث

تتمثل حدود البحث في مجموعة من الحدود التي تحدد نطاق الدراسة ومجال تطبيقها، وذلك على النحو الآتي:

أولاً: الحدود الموضوعية

تقتصر هذه الدراسة على تحليل أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وقد ركزت الدراسة على أربعة أبعاد رئيسية لإدارة المخاطر السيبرانية، وهي: تحديد المخاطر السيبرانية، تقييم المخاطر السيبرانية، معالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية. كما تناولت الدراسة نجاح مشاريع تقنية المعلومات من خلال مؤشرات تشمل الالتزام بالوقت، والالتزام بالتكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية.

ثانياً: الحدود البشرية

اقتصرت الدراسة على عينة من العاملين في المجالات ذات العلاقة بمشاريع تقنية المعلومات، وإدارة المشاريع، والأمن السيبراني، والحوكمة والمخاطر، في الجهات الحكومية السعودية والجهات ذات العلاقة. وقد بلغ عدد الاستجابات الصالحة للتحليل الإحصائي (80) استجابة.

ثالثاً: الحدود المكانية

تم تطبيق الدراسة في بيئة الجهات الحكومية السعودية والجهات ذات العلاقة بمشاريع تقنية المعلومات، وذلك لارتباط هذه الجهات بمبادرات التحول الرقمي والخدمات الحكومية الرقمية، وما يرتبط بها من متطلبات أمنية وتنظيمية وتقنية.

رابعًا: الحدود الزمانية

تمثلت الحدود الزمانية للدراسة في الفترة التي تم خلالها إعداد الدراسة وتصميم أداة البحث وجمع البيانات وتحليلها إحصائيًا، وذلك خلال العام الدراسي 2026 .

جدول (2-3): ترميز مقياس ليكرت الخماسي

الترميز	درجة الاستجابة
1	لا أوافق بشدة
2	لا أوافق
3	محايد
4	أوافق
5	أوافق بشدة

اعتمدت الدراسة على مقياس ليكرت الخماسي لقياس استجابات أفراد العينة تجاه عبارات الاستبانة، حيث تم ترميز الاستجابات من (1) إلى (5)، بحيث تشير الدرجة الأعلى إلى مستوى موافقة أعلى على العبارة.

الفصل الرابع: النتائج والتوصيات

مقدمة

يتناول هذا الفصل عرض نتائج الدراسة الميدانية وتحليلها إحصائياً، وذلك بهدف الإجابة عن تساؤلات الدراسة واختبار فرضياتها المتعلقة بأثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وقد تم الاعتماد على البيانات التي تم جمعها من خلال الاستبانة الإلكترونية، حيث بلغ عدد الاستجابات الصالحة للتحليل الإحصائي (80) استجابة.

وقد تم تحليل البيانات باستخدام برنامج Jamovi، من خلال تطبيق مجموعة من الأساليب الإحصائية المناسبة لطبيعة الدراسة، شملت فحص جودة البيانات، واختبار ثبات أداة الدراسة باستخدام معامل كرونباخ ألفا، والتحليل الوصفي لمحاور الدراسة، وتحليل الارتباط باستخدام معامل بيرسون، إضافة إلى تحليل الانحدار الخطي البسيط والمتعدد لاختبار أثر إدارة المخاطر السيبرانية وأبعادها على نجاح مشاريع تقنية المعلومات. ويعرض هذا الفصل نتائج التحليل الإحصائي بشكل متسلسل، بدءاً من فحص جودة البيانات، ثم اختبار الثبات، ثم التحليل الوصفي، ثم تحليل العلاقة والأثر بين متغيرات الدراسة، وصولاً إلى عرض النتائج النهائية والتوصيات المقترحة.

تحليل البيانات

فحص جودة البيانات

قبل البدء في التحليل الإحصائي، تم فحص جودة البيانات للتأكد من صلاحيتها للتحليل، وذلك من خلال مراجعة عدد الاستجابات، والقيم المفقودة، ونطاق القيم، ومدى توافق البيانات مع مقياس ليكرت الخماسي المستخدم في الدراسة. وقد أظهرت نتائج الفحص أن جميع الاستجابات مكتملة وصالحة للتحليل، حيث لم تظهر أي قيم مفقودة في عبارات المقياس، كما أن جميع القيم كانت ضمن نطاق مقياس ليكرت الخماسي من (1) إلى (5) .

جدول (1-4): نتائج فحص جودة البيانات

المؤشر	النتيجة	التقييم
عدد الاستجابات	80	صالح للتحليل
القيم المفقودة	0	لا توجد قيم مفقودة
أقل قيمة	1	ضمن نطاق مقياس ليكرت
أعلى قيمة	5	ضمن نطاق مقياس ليكرت
القيم خارج النطاق	0	لا توجد أخطاء إدخال

يوضح جدول (1-4) أن عدد الاستجابات الصالحة للتحليل الإحصائي بلغ (80) استجابة، كما لم تظهر أي قيم مفقودة في بيانات الدراسة. كذلك تبين أن جميع القيم تقع ضمن نطاق مقياس ليكرت الخماسي من (1) إلى (5)، مما يدل على سلامة البيانات وخلوها من أخطاء الإدخال أو القيم الخارجة عن النطاق المقبول. وبناءً على ذلك، تم اعتماد جميع الاستجابات في التحليل الإحصائي اللاحق.

اختبار ثبات أداة الدراسة

تم اختبار ثبات أداة الدراسة باستخدام معامل كرونباخ ألفا (Cronbach's Alpha)، وذلك بهدف التحقق من الاتساق الداخلي لعبارات الاستبانة ومدى ملاءمتها لقياس متغيرات الدراسة. ويعد معامل كرونباخ ألفا من الأساليب الإحصائية الشائعة لقياس الثبات، حيث تشير القيم المرتفعة إلى وجود اتساق داخلي جيد بين العبارات التي تقيس المحور نفسه.

وقد تم حساب معامل كرونباخ ألفا لكل محور من محاور الدراسة، إضافة إلى حساب الثبات الكلي للاستبانة. ويوضح الجدول الآتي نتائج اختبار الثبات:

جدول (2-4): معاملات الثبات لمحاور الدراسة

المحور	عدد العبارات	Cronbach's Alpha	مستوى الثبات
تحديد المخاطر السيبرانية	5	0.890	مرتفع جدًا
تقييم المخاطر السيبرانية	5	0.893	مرتفع جدًا
معالجة المخاطر السيبرانية	5	0.923	ممتاز
متابعة ومراقبة المخاطر السيبرانية	5	0.932	ممتاز
نجاح مشاريع تقنية المعلومات	15	0.929	ممتاز
الاستبانة ككل	35	0.966	ممتاز

يوضح جدول (2-4) أن قيم معامل كرونباخ ألفا لجميع محاور الدراسة جاءت مرتفعة، حيث بلغت قيمة معامل الثبات لمحور تحديد المخاطر السيبرانية (0.890)، وبلغت لمحور تقييم المخاطر السيبرانية (0.893)، في حين بلغت لمحور معالجة المخاطر السيبرانية (0.923)، وبلغت لمحور متابعة ومراقبة المخاطر السيبرانية (0.932). كما بلغت قيمة معامل الثبات لمحور نجاح مشاريع تقنية المعلومات (0.929).

أما معامل الثبات الكلي للاستبانة فقد بلغ (0.966)، وهي قيمة مرتفعة جداً، مما يدل على أن أداة الدراسة تتمتع بدرجة عالية من الاتساق الداخلي. وبناءً على ذلك، يمكن الاعتماد على الاستبانة في التحليلات الإحصائية اللاحقة، بما في ذلك التحليل الوصفي، وتحليل الارتباط، والانحدار الخطي لاختبار فرضيات الدراسة.

التحليل الوصفي لمحاور الدراسة

تم استخدام المتوسطات الحسابية والانحرافات المعيارية للتعرف على اتجاهات أفراد عينة الدراسة نحو محاور الاستبانة، وذلك من خلال قياس مستوى الموافقة على أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات. ويعكس المتوسط الحسابي مستوى موافقة أفراد العينة، في حين يوضح الانحراف المعياري مدى تشتت استجاباتهم حول المتوسط.

ويوضح الجدول الآتي نتائج التحليل الوصفي لمحاور الدراسة:

جدول (3-4): التحليل الوصفي لمحاور الدراسة

المحور	N	المتوسط الحسابي	الانحراف المعياري	الحد الأدنى	الحد الأعلى	مستوى الموافقة
تحديد المخاطر السيبرانية	80	4.24	0.744	2.00	5.00	مرتفع
تقييم المخاطر السيبرانية	80	3.98	0.797	1.00	5.00	مرتفع
معالجة المخاطر السيبرانية	80	4.03	0.791	1.00	5.00	مرتفع
متابعة ومراقبة المخاطر السيبرانية	80	3.99	0.839	1.00	5.00	مرتفع
نجاح مشاريع تقنية المعلومات	80	4.03	0.607	1.67	5.00	مرتفع
إدارة المخاطر السيبرانية ككل	80	4.06	0.714	2.00	5.00	مرتفع

يوضح جدول (3-4) أن المتوسطات الحسابية لجميع محاور الدراسة جاءت ضمن مستوى موافقة مرتفع، حيث تراوحت المتوسطات الحسابية بين (3.98) و (4.24)، مما يشير إلى وجود اتجاه إيجابي لدى أفراد عينة الدراسة تجاه ممارسات إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات.

وقد حصل محور تحديد المخاطر السيبرانية على أعلى متوسط حسابي بلغ (4.24) بانحراف معياري (0.744)، مما يدل على أن أفراد العينة يدركون بدرجة مرتفعة أهمية تحديد المخاطر السيبرانية في مشاريع تقنية المعلومات. كما بلغ المتوسط الحسابي لمحور إدارة المخاطر السيبرانية ككل (4.06) بانحراف معياري (0.714)، وهو ما يعكس مستوى مرتفعاً من تطبيق ممارسات إدارة المخاطر السيبرانية من وجهة نظر المشاركين.

أما محور نجاح مشاريع تقنية المعلومات فقد بلغ متوسطه الحسابي (4.03) بانحراف معياري (0.607)، مما يشير إلى أن أفراد العينة يرون أن مشاريع تقنية المعلومات تحقق مستوى مرتفعاً من النجاح من حيث الالتزام بالوقت، والتكلفة، وجودة المخرجات، ورضا أصحاب المصلحة، وتحقيق الأهداف الاستراتيجية.

وبناءً على هذه النتائج، يمكن القول إن اتجاهات أفراد العينة جاءت إيجابية نحو كل من إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات، وهو ما يدعم الانتقال إلى تحليل العلاقة والأثر بين متغيرات الدراسة.

تحليل الارتباط بين متغيرات الدراسة

تم استخدام معامل ارتباط بيرسون **Pearson Correlation** لقياس طبيعة العلاقة بين أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات. ويهدف هذا التحليل إلى تحديد ما إذا كانت هناك علاقة ارتباط ذات دلالة إحصائية بين المتغيرات، قبل الانتقال إلى تحليل الانحدار لاختبار أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.

ويوضح الجدول الآتي نتائج تحليل الارتباط بين أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات:

جدول (4-4): معاملات ارتباط بيرسون بين أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات .

النتيجة	مستوى الدلالة	معامل الارتباط مع نجاح مشاريع تقنية المعلومات	المتغير
علاقة موجبة دالة إحصائياً	< 0.001	0.618	تحديد المخاطر السيبرانية
علاقة موجبة دالة إحصائياً	< 0.001	0.578	تقييم المخاطر السيبرانية
علاقة موجبة دالة إحصائياً	< 0.001	0.581	معالجة المخاطر السيبرانية
علاقة موجبة دالة إحصائياً	< 0.001	0.552	متابعة ومراقبة المخاطر السيبرانية
علاقة موجبة دالة إحصائياً	< 0.001	0.645	إدارة المخاطر السيبرانية ككل

يوضح جدول (4-4) وجود علاقات ارتباط موجبة ودالة إحصائياً بين جميع أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات، حيث بلغت قيمة معامل الارتباط بين تحديد المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات (0.618) عند مستوى دلالة ($p < 0.001$)، وهي علاقة موجبة دالة إحصائياً.

كما بلغت قيمة معامل الارتباط بين تقييم المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات (0.578)، وبلغت بين معالجة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات (0.581)، في حين بلغت بين متابعة ومراقبة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات (0.552)، وجميعها عند مستوى دلالة ($p < 0.001$).

أما العلاقة بين إدارة المخاطر السيبرانية ككل ونجاح مشاريع تقنية المعلومات فقد بلغت (0.645) عند مستوى دلالة ($p < 0.001$)، وهي علاقة موجبة متوسطة إلى قوية ودالة إحصائية. وتشير هذه النتيجة إلى أنه كلما ارتفع مستوى تطبيق ممارسات إدارة المخاطر السيبرانية، ارتفع مستوى نجاح مشاريع تقنية المعلومات من وجهة نظر أفراد عينة الدراسة.

وبناءً على نتائج الارتباط، يمكن الانتقال إلى تحليل الانحدار الخطي لاختبار أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.

تحليل الانحدار الخطي البسيط لاختبار الفرضية الرئيسية

تم استخدام تحليل الانحدار الخطي البسيط لاختبار أثر إدارة المخاطر السيبرانية ككل على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وقد تم اعتبار إدارة المخاطر السيبرانية المتغير المستقل، بينما تم اعتبار نجاح مشاريع تقنية المعلومات المتغير التابع.

وتنص الفرضية الرئيسية للدراسة على ما يلي:

يوجد أثر ذو دلالة إحصائية لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية

السعودية عند مستوى دلالة إحصائية ($\alpha \leq 0.05$).

جدول (4-5) نتائج نموذج الانحدار الخطي البسيط:

المتغير المستقل	R	R ²	Adjusted R ²	F	df1	df2	Sig.
إدارة المخاطر السيبرانية	0.645	0.417	0.409	55.7	1	78	< 0.001

يوضح جدول (5-4) أن قيمة معامل الارتباط بلغت ($R = 0.645$)، مما يشير إلى وجود علاقة موجبة بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات. كما بلغت قيمة معامل التحديد ($R^2 = 0.417$)، وهذا يعني أن إدارة المخاطر السيبرانية تفسر ما نسبته (41.7%) من التباين في نجاح مشاريع تقنية المعلومات.

كما بلغت قيمة اختبار النموذج ($F = 55.7$) عند مستوى دلالة ($p < 0.001$)، وهي قيمة دالة إحصائيًا عند مستوى ($\alpha \leq 0.05$). وتشير هذه النتيجة إلى أن نموذج الانحدار الخطي البسيط مناسب إحصائيًا لاختبار أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.

جدول (6-4): معاملات الانحدار للفرضية الرئيسة

المتغير	B	SE	Beta	t	Sig
الثابت	1.806	0.3029	—	5.96	< 0.001
إدارة المخاطر السيبرانية	0.549	0.0735	0.645	7.46	< 0.001

يوضح جدول (6-4) أن معامل الانحدار غير المعياري لإدارة المخاطر السيبرانية بلغ ($B = 0.549$)، وهذا يعني أن زيادة مستوى تطبيق إدارة المخاطر السيبرانية بدرجة واحدة تؤدي إلى زيادة متوقعة في نجاح مشاريع تقنية المعلومات بمقدار (0.549) درجة.

كما بلغت قيمة معامل الانحدار المعياري ($Beta = 0.645$)، وبلغت قيمة ($t = 7.46$) عند مستوى دلالة ($p < 0.001$)، وهي قيمة دالة إحصائيًا عند مستوى ($\alpha \leq 0.05$) وبناءً على ذلك، يتضح وجود أثر موجب ودال إحصائيًا لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.

وعليه، يتم قبول الفرضية الرئيسة للدراسة، والتي تنص على وجود أثر ذو دلالة إحصائية لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية.

تحليل الانحدار الخطي المتعدد لاختبار الفرضيات الفرعية

تم استخدام تحليل الانحدار الخطي المتعدد لاختبار أثر أبعاد إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وقد تم إدخال أبعاد إدارة المخاطر السيبرانية بوصفها متغيرات مستقلة، وهي: تحديد المخاطر السيبرانية، تقييم المخاطر السيبرانية، معالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية، في حين تم اعتبار نجاح مشاريع تقنية المعلومات المتغير التابع.

ويهدف هذا التحليل إلى تحديد الأبعاد الأكثر تأثيراً في نجاح مشاريع تقنية المعلومات عند إدخال جميع أبعاد إدارة المخاطر السيبرانية في النموذج نفسه.

جدول (7-4): نتائج الانحدار الخطي المتعدد للفرضيات الفرعية

النموذج	R	R ²	Adjusted R ²	F	df1	df2	Sig
الانحدار الخطي المتعدد	0.667	0.445	0.416	15.1	4	75	< 0.001

يوضح جدول (7-4) أن قيمة معامل الارتباط بلغت ($R = 0.667$)، مما يشير إلى وجود علاقة موجبة بين أبعاد إدارة المخاطر السيبرانية مجتمعة ونجاح مشاريع تقنية المعلومات. كما بلغت قيمة معامل التحديد ($R^2 = 0.445$)، وهذا يعني أن أبعاد إدارة المخاطر السيبرانية مجتمعة تفسر ما نسبته (44.5%) من التباين في نجاح مشاريع تقنية المعلومات.

كما بلغت قيمة اختبار النموذج ($F = 15.1$) عند مستوى دلالة ($p < 0.001$)، وهي قيمة دالة إحصائياً عند مستوى ($\alpha \leq 0.05$). وتشير هذه النتيجة إلى أن نموذج الانحدار الخطي المتعدد مناسب إحصائياً لاختبار أثر أبعاد إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.

جدول (8-4): معاملات الانحدار لأبعاد إدارة المخاطر السيبرانية

المتغير المستقل	B	SE	Beta	t	Sig	القرار
تحديد المخاطر السيبرانية	0.316	0.0968	0.387	3.266	0.002	دال إحصائياً
تقييم المخاطر السيبرانية	0.093	0.1284	0.122	0.721	0.473	غير دال إحصائياً
معالجة المخاطر السيبرانية	0.151	0.1800	0.197	0.837	0.405	غير دال إحصائياً
متابعة ومراقبة المخاطر السيبرانية	0.028	0.1495	0.039	0.188	0.852	غير دال إحصائياً

يوضح جدول (8-4) أن بُعد تحديد المخاطر السيبرانية كان البُعد الوحيد الذي ظهر له أثر موجب ودال إحصائيًا على نجاح مشاريع تقنية المعلومات، حيث بلغت قيمة معامل الانحدار غير المعياري ($B = 0.316$)، وبلغت قيمة معامل الانحدار المعياري ($Beta = 0.387$)، كما بلغت قيمة ($t = 3.266$) عند مستوى دلالة ($p = 0.002$)، وهي قيمة أقل من مستوى الدلالة المعتمد ($\alpha \leq 0.05$) وتشير هذه النتيجة إلى أن تحديد المخاطر السيبرانية يسهم في تعزيز نجاح مشاريع تقنية المعلومات عند إدخال أبعاد إدارة المخاطر السيبرانية مجتمعة في النموذج.

أما أبعاد تقييم المخاطر السيبرانية، ومعالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية، فلم تظهر أثرًا منفردًا دالًا إحصائيًا داخل نموذج الانحدار المتعدد، حيث جاءت قيم الدلالة الإحصائية لها أكبر من (0.05) ولا يعني ذلك عدم أهمية هذه الأبعاد من الناحية العملية، إذ أظهرت نتائج الارتباط السابقة وجود علاقات موجبة ودالة بينها وبين نجاح مشاريع تقنية المعلومات، إلا أن أثرها المنفرد لم يظهر عند إدخالها مع بقية الأبعاد في النموذج نفسه.

جدول (9-4): نتائج اختبار تعدد الارتباط الخطي VIF وTolerance

المتغير المستقل	VIF	Tolerance	التقييم
تحديد المخاطر السيبرانية	1.90	0.526	مقبول
تقييم المخاطر السيبرانية	3.85	0.260	مقبول
معالجة المخاطر السيبرانية	7.45	0.134	مرتفع نسبيًا لكنه مقبول
متابعة ومراقبة المخاطر السيبرانية	5.78	0.173	مرتفع نسبيًا لكنه مقبول

يوضح جدول (9-4) نتائج فحص تعدد الارتباط الخطي بين المتغيرات المستقلة باستخدام معامل تضخم التباين VIF وقيمة Tolerance. وقد تراوحت قيم VIF بين (1.90) و (7.45)، وهي لم تتجاوز الحد الأعلى الشائع (10) كما جاءت جميع قيم Tolerance أعلى من (0.10).

وبناءً على ذلك، لا توجد مشكلة حادة في تعدد الارتباط الخطي تمنع استخدام نموذج الانحدار الخطي المتعدد. ومع ذلك، فإن ارتفاع قيم VIF نسبيًا لبعض الأبعاد، مثل معالجة المخاطر السيبرانية ومتابعة ومراقبة المخاطر السيبرانية، يشير إلى وجود ترابط قوي نسبيًا بين أبعاد إدارة المخاطر السيبرانية، وهو أمر متوقع نظرًا لأنها تمثل أبعادًا مترابطة ضمن مفهوم واحد.

النتائج

في ضوء التحليلات الإحصائية التي تم إجراؤها، توصلت الدراسة إلى مجموعة من النتائج المرتبطة بأثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وقد أظهرت النتائج أن إدارة المخاطر السيبرانية تمثل عاملاً مهمًا في تفسير نجاح مشاريع تقنية المعلومات، حيث بينت نتائج الانحدار الخطي البسيط وجود أثر موجب ودال إحصائيًا لإدارة المخاطر السيبرانية ككل على نجاح مشاريع تقنية المعلومات.

كما أظهرت نتائج تحليل الارتباط وجود علاقات موجبة ودالة إحصائيًا بين جميع أبعاد إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات، مما يشير إلى أن ارتفاع مستوى تطبيق ممارسات إدارة المخاطر السيبرانية يرتبط بارتفاع مستوى نجاح المشاريع التقنية. وفي المقابل، بينت نتائج الانحدار الخطي المتعدد أن بُعد تحديد المخاطر السيبرانية كان البُعد الوحيد الذي ظهر له أثر منفرد دال إحصائيًا عند إدخال جميع الأبعاد في النموذج نفسه.

ويمكن تلخيص نتائج اختبار فرضيات الدراسة في الجدول الآتي:

جدول (10-4): ملخص نتائج اختبار فرضيات الدراسة :

رمز الفرضية	نص الفرضية	النتيجة الإحصائية	القرار
الفرضية الرئيسية	يوجد أثر ذو دلالة إحصائية لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية.	$R^2 = 0.417, p < 0.001$	مقبولة
الفرضية الفرعية الأولى	يوجد أثر ذو دلالة إحصائية لتحديد المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.	$Beta = 0.387, p = 0.002$	مقبولة
الفرضية الفرعية الثانية	يوجد أثر ذو دلالة إحصائية لتقييم المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.	$Beta = 0.122, p = 0.473$	غير مدعومة إحصائيًا
الفرضية الفرعية الثالثة	يوجد أثر ذو دلالة إحصائية لمعالجة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.	$Beta = 0.197, p = 0.405$	غير مدعومة إحصائيًا
الفرضية الفرعية الرابعة	يوجد أثر ذو دلالة إحصائية لمراقبة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات.	$Beta = 0.039, p = 0.852$	غير مدعومة إحصائيًا

يوضح جدول (10-4) أن الفرضية الرئيسية للدراسة قد تم قبولها، حيث أظهرت نتائج الانحدار الخطي البسيط وجود

أثر موجب ودال إحصائيًا لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات

عند مستوى دلالة ($p < 0.001$)

كما بلغت قيمة معامل التحديد ($R^2 = 0.417$)، مما يعني أن إدارة المخاطر السيبرانية تفسر ما نسبته (41.7%) من التباين في نجاح مشاريع تقنية المعلومات.

كما تم قبول الفرضية الفرعية الأولى، حيث أظهرت نتائج الانحدار الخطي المتعدد وجود أثر موجب ودال إحصائيًا لتحديد المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات، إذ بلغت قيمة معامل الانحدار المعياري ($Beta = 0.387$) عند مستوى دلالة ($p = 0.002$).

أما الفرضيات الفرعية الثانية والثالثة والرابعة، والمتعلقة بتقييم المخاطر السيبرانية، ومعالجة المخاطر السيبرانية، ومتابعة ومراقبة المخاطر السيبرانية، فلم تظهر أثرًا منفردًا دالًا إحصائيًا داخل نموذج الانحدار الخطي المتعدد، حيث جاءت مستويات الدلالة لها أكبر من (0.05) وبناءً على ذلك، تعد هذه الفرضيات غير مدعومة إحصائيًا في نموذج الانحدار المتعدد.

ومع ذلك، فإن عدم دعم هذه الفرضيات في نموذج الانحدار المتعدد لا يعني عدم أهمية هذه الأبعاد من الناحية العملية، حيث أظهرت نتائج الارتباط وجود علاقات موجبة ودالة إحصائيًا بينها وبين نجاح مشاريع تقنية المعلومات. وقد يرجع عدم ظهور أثرها المنفرد إلى الترابط المرتفع نسبيًا بين أبعاد إدارة المخاطر السيبرانية، باعتبارها أبعادًا متكاملة ضمن مفهوم واحد.

التوصيات

في ضوء النتائج التي توصلت إليها الدراسة، والتي أظهرت وجود أثر موجب ودال إحصائيًا لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية، تقدم الدراسة عددًا من التوصيات التي يمكن أن تسهم في تعزيز ممارسات إدارة المخاطر السيبرانية وتحسين فرص نجاح المشاريع التقنية، وذلك على النحو الآتي:

1. تعزيز دمج إدارة المخاطر السيبرانية ضمن منهجية إدارة المشاريع التقنية، بحيث يتم التعامل مع المخاطر السيبرانية منذ مراحل التخطيط الأولى للمشروع، وليس بعد بدء التنفيذ أو عند ظهور التحديات الأمنية.
2. تطوير آليات واضحة لتحديد المخاطر السيبرانية في مشاريع تقنية المعلومات، نظرًا لأن نتائج الدراسة أظهرت أن بُعد تحديد المخاطر السيبرانية كان الأكثر تأثيرًا في نجاح مشاريع تقنية المعلومات عند تحليل الأبعاد بصورة مستقلة.

3. إعداد سجل مخاطر سيبرانية خاص بكل مشروع تقني، يتضمن المخاطر المحتملة، ومصادرها، واحتمالية حدوثها، ومستوى تأثيرها، والإجراءات المقترحة للتعامل معها، والجهات المسؤولة عن متابعتها.
 4. تعزيز التنسيق بين فرق إدارة المشاريع وفرق الأمن السيبراني والحوكمة والمخاطر، بما يضمن وجود فهم مشترك للمخاطر السيبرانية وتأثيرها المحتمل على وقت المشروع وتكلفته وجودة مخرجاته.
 5. إدراج متطلبات الأمن السيبراني ضمن وثائق المشروع الأساسية، مثل وثيقة نطاق العمل، وخطة المشروع، وخطة إدارة المخاطر، وخطة الاختبارات، وذلك لضمان وضوح المتطلبات الأمنية منذ بداية المشروع.
 6. تفعيل المتابعة الدورية للمخاطر السيبرانية خلال مراحل المشروع المختلفة، وعدم الاكتفاء بتحديد المخاطر في بداية المشروع فقط، نظرًا لأن المخاطر السيبرانية قد تتغير مع تغير بيئة المشروع أو التقنية المستخدمة.
 7. رفع الوعي لدى مديري المشاريع وفرق العمل بأهمية إدارة المخاطر السيبرانية، من خلال برامج تدريبية وورش عمل متخصصة توضح أثر المخاطر السيبرانية على نجاح المشاريع التقنية.
 8. الاستفادة من نتائج تحليل المخاطر في دعم اتخاذ القرار داخل المشاريع، خاصة عند المفاضلة بين البدائل التقنية، أو تحديد الأولويات، أو التعامل مع التحديات التي قد تؤثر في استمرارية المشروع.
 9. ربط مؤشرات نجاح مشاريع تقنية المعلومات بمستوى إدارة المخاطر السيبرانية، بحيث لا يتم تقييم نجاح المشروع فقط من خلال الوقت والتكلفة، بل من خلال جودة المخرجات، واستمرارية الخدمة، والامتثال الأمني، ورضا أصحاب المصلحة.
 10. إجراء دراسات مستقبلية أوسع تشمل عينات أكبر وقطاعات مختلفة، وذلك لمقارنة أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات بين الجهات الحكومية والقطاع الخاص أو بين قطاعات حكومية متعددة.
- وبذلك يكون هذا الفصل قد عرض نتائج التحليل الإحصائي للدراسة، وبيّن مستوى ثبات أداة الدراسة، والاتجاهات العامة لاستجابات أفراد العينة، وطبيعة العلاقة بين إدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات. كما

أوضحت نتائج الدراسة وجود أثر موجب ودال إحصائيًا لإدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات، مع إبراز أهمية تحديد المخاطر السيبرانية بوصفه البُعد الأكثر تأثيرًا في نموذج الانحدار المتعدد. وانتهى الفصل بتقديم عدد من التوصيات العملية التي يمكن أن تساعد الجهات الحكومية السعودية على تعزيز إدارة المخاطر السيبرانية داخل مشاريع تقنية المعلومات.

المراجع

المراجع العربية

الهيئة الوطنية للأمن السيبراني. (2026). الضوابط الأساسية للأمن السيبراني. ECC 2-2024 المملكة العربية السعودية.

هيئة الحكومة الرقمية. (2021). سياسات الحكومة الرقمية. المملكة العربية السعودية.

هيئة الحكومة الرقمية. (2026). الإطار التنظيمي لأعمال الحكومة الرقمية. المملكة العربية السعودية.

رؤية السعودية 2030. (د.ت). برنامج التحول الوطني. المملكة العربية السعودية.

المراجع الأجنبية

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), 9–30.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper, CSWP 29.

Project Management Institute. (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7th ed.). Project Management Institute.

Project Management Institute. (2021). *The standard for project management*. Project Management institute

الملاحق

ملحق (1): الاستبانة

عنوان الدراسة:

أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية

مقدمة الاستبانة:

تهدف هذه الاستبانة إلى جمع البيانات اللازمة لإجراء دراسة علمية حول أثر إدارة المخاطر السيبرانية على نجاح مشاريع تقنية المعلومات في الجهات الحكومية السعودية. وتستخدم البيانات التي يتم جمعها لأغراض البحث العلمي فقط، مع الالتزام بسرية المعلومات وعدم استخدامها إلا في نطاق الدراسة.

تعليمات الإجابة:

يرجى قراءة العبارات بعناية، ثم اختيار درجة الموافقة التي تعبر عن وجهة نظرك، وفق مقياس ليكرت الخماسي الآتي:

الترميز	درجة الاستجابة
1	لا أوافق بشدة
2	لا أوافق
3	محايد
4	أوافق
5	أوافق بشدة

أولاً: البيانات الديموغرافية:

م	السؤال	خيارات الإجابة
1	نوع الجهة التي تعمل بها	جهة حكومية / جهة شبه حكومية / شركة خاصة / جهة رقابية / أخرى
2	المسمى الوظيفي	مدير مشروع / مدير برنامج / أخصائي أمن سيبراني / مختص حوكمة ومخاطر / مدير تقنية معلومات / مدير مخاطر / مكتب إدارة مشاريع / مدير أمن سيبراني / أخرى
3	سنوات الخبرة	أقل من 3 سنوات / من 3 إلى أقل من 5 سنوات / من 5 إلى أقل من 10 سنوات / 10 سنوات فأكثر
4	مدى ارتباط بمشاريع تقنية المعلومات	ارتباط مباشر / ارتباط غير مباشر / لا يوجد ارتباط
5	مدى ارتباط عملك بإدارة المخاطر أو الأمن السيبراني	ارتباط مباشر / ارتباط غير مباشر / لا يوجد ارتباط

ثانيًا: محاور الاستبانة

يهدف هذا الجزء إلى قياس متغيرات الدراسة من خلال مجموعة من العبارات المرتبطة بإدارة المخاطر السيبرانية ونجاح مشاريع تقنية المعلومات، وذلك وفق مقياس ليكرت الخماسي.

المحور الأول: تحديد المخاطر السيبرانية:

الرمز	العبارة
CRI1	يتم تحديد المخاطر السيبرانية المحتملة في مراحل مبكرة من مشاريع تقنية المعلومات.
CRI2	يتم حصر مصادر التهديدات السيبرانية التي قد تؤثر على سير المشروع.
CRI3	يتم تحديد الأصول والأنظمة والبيانات الحساسة المرتبطة بالمشروع.
CRI4	يتم إشراك فرق الأمن السيبراني والحوكمة والمخاطر في عملية تحديد المخاطر.
CRI5	توجد آلية واضحة لتوثيق المخاطر السيبرانية التي يتم تحديدها أثناء المشروع.

المحور الثاني: تقييم المخاطر السيبرانية:

الرمز	العبارة
CRA1	يتم تقييم احتمالية حدوث المخاطر السيبرانية المرتبطة بمشاريع تقنية المعلومات.
CRA2	يتم تقييم أثر المخاطر السيبرانية على وقت المشروع وتكلفته وجودة مخرجاته.
CRA3	يتم تصنيف المخاطر السيبرانية حسب مستوى الأولوية والخطورة.
CRA4	يتم الاعتماد على معايير واضحة عند تقييم المخاطر السيبرانية.
CRA5	تساعد نتائج تقييم المخاطر السيبرانية في دعم قرارات إدارة المشروع.

المحور الثالث: معالجة المخاطر السيبرانية:

الرمز	العبارة
CRT1	يتم وضع خطط مناسبة لمعالجة المخاطر السيبرانية التي قد تؤثر على المشروع.
CRT2	يتم تحديد الإجراءات الوقائية للحد من احتمالية حدوث المخاطر السيبرانية.
CRT3	يتم تحديد الإجراءات التصحيحية للتعامل مع المخاطر السيبرانية عند وقوعها.
CRT4	يتم توزيع المسؤوليات بوضوح لمعالجة المخاطر السيبرانية داخل المشروع.
CRT5	تسهم معالجة المخاطر السيبرانية في تقليل تعثر مشاريع تقنية المعلومات.

المحور الرابع: متابعة ومراقبة المخاطر السيبرانية:

الرمز	العبارة
CRM1	تتم متابعة المخاطر السيبرانية بشكل دوري خلال مراحل تنفيذ المشروع.
CRM2	يتم تحديث سجل المخاطر السيبرانية عند ظهور مخاطر جديدة أو تغير مستوى المخاطر القائمة.
CRM3	تتم مراجعة فعالية الإجراءات المتخذة لمعالجة المخاطر السيبرانية.
CRM4	يتم رفع تقارير دورية عن حالة المخاطر السيبرانية لأصحاب المصلحة في المشروع.
CRM5	تساعد متابعة ومراقبة المخاطر السيبرانية في تحسين التحكم بسير المشروع.

المحور الخامس: نجاح مشاريع تقنية المعلومات

الرمز	العبارة
PS1	تحقق مشاريع تقنية المعلومات أهدافها المخططة بدرجة مناسبة.
PS2	يتم تنفيذ مشاريع تقنية المعلومات ضمن الجداول الزمنية المحددة.
PS3	يتم التحكم في تكاليف مشاريع تقنية المعلومات ضمن الحدود المعتمدة.
PS4	تحقق مخرجات مشاريع تقنية المعلومات مستوى مناسباً من الجودة.
PS5	تتلبى مخرجات مشاريع تقنية المعلومات احتياجات المستخدمين وأصحاب المصلحة.
PS6	تسهم مشاريع تقنية المعلومات في تحسين كفاءة العمل داخل الجهة.
PS7	تدعم مشاريع تقنية المعلومات تحقيق الأهداف الاستراتيجية للجهة.
PS8	يتم التعامل بفاعلية مع التحديات التي تظهر أثناء تنفيذ مشاريع تقنية المعلومات.
PS9	يوجد رضا لدى أصحاب المصلحة عن نتائج مشاريع تقنية المعلومات.
PS10	تساعد مشاريع تقنية المعلومات في تحسين جودة الخدمات الرقمية المقدمة.
PS11	تسهم مشاريع تقنية المعلومات في دعم مبادرات التحول الرقمي.
PS12	يتم تسليم مخرجات مشاريع تقنية المعلومات وفق المتطلبات المتفق عليها.
PS13	تحقق مشاريع تقنية المعلومات قيمة مضافة للجهة أو المستخدمين.
PS14	يتم الحفاظ على استمرارية الخدمات أو الأنظمة بعد تنفيذ مشاريع تقنية المعلومات.
PS15	يمكن اعتبار مشاريع تقنية المعلومات ناجحة عند تقييم نتائجها النهائية.

نشكركم على وقتكم ومشاركتكم في تعبئة هذه الاستبانة، ونؤكد أن جميع البيانات المقدمة ستستخدم لأغراض البحث العلمي فقط، مع المحافظة على سرية المعلومات وعدم استخدامها إلا في نطاق هذه الدراسة.

Abstract

This study aimed to examine the impact of cybersecurity risk management on the success of information technology projects in Saudi government entities. The study was conducted in light of the growing reliance on digital transformation initiatives and the increasing importance of cybersecurity in protecting digital services, systems, and information assets.

The study adopted a descriptive analytical approach and used a questionnaire as the main data collection instrument. The questionnaire measured four dimensions of cybersecurity risk management: cybersecurity risk identification, cybersecurity risk assessment, cybersecurity risk treatment, and cybersecurity risk monitoring and control. It also measured information technology project success through indicators related to time, cost, quality of deliverables, stakeholder satisfaction, and achievement of strategic objectives.

A total of 80 valid responses were collected and analyzed using Jamovi. The statistical methods included descriptive statistics, Cronbach's Alpha reliability test, Pearson correlation analysis, simple linear regression, and multiple linear regression. The results showed a high level of internal consistency for the questionnaire, with an overall Cronbach's Alpha value of 0.966.

The findings revealed a positive and statistically significant relationship between cybersecurity risk management and information technology project success. The simple linear regression results indicated that cybersecurity risk management explained 41.7% of the variance in information technology project success. The multiple regression results also showed that the dimensions of cybersecurity risk management collectively explained 44.5% of the variance in project success. Among the individual dimensions, cybersecurity risk identification was the only dimension that had a statistically significant individual effect on information technology project success.

Based on these findings, the study recommended strengthening the integration of cybersecurity risk management into information technology project management practices, developing clear mechanisms for identifying cybersecurity risks, maintaining cybersecurity risk registers for IT projects, and enhancing coordination between project management teams, cybersecurity teams, and governance and risk functions.

Keywords: Cybersecurity Risk Management, Information Technology Project Success, Saudi Government Entities, Project Management, Cybersecurity, Digital Transformation.

Midocean University

College of Management

Department of Project Management

**The Impact of Cybersecurity Risk Management on the Success of Information Technology
Projects in Saudi Government Entities**

Prepared by:

Eng. Mohammed Althagafi

Supervised by:

Dr. Al Faisal Abdulhamid

Dr. Fayez Jarad

Year:2026