

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص. ماجستير إدارة مشاريع



العنوان باللغة العربية

تأثير إدارة المخاطر الرقمية على أستدامة المشاريع التقنية

في القطاع الحكومي السعودي

إعداد الطالبة/ ثناء إسحاق حلواني

إشراف/

د. الفيصل عبد الحميد

د. فايز جراد

العام الدراسي

2026

Midocean University

College of Management

Department of: Master of Project Management

Title in English

Digital Risk Management and the Sustainability of Government Technology
Projects
in the Saudi Arabian Public Sector

Prepared by:

Thanaa Ishaq Mohammed Halwani

Supervised by:

Dr. Alfaisal Abdulhameed | Dr. Fayez Jarad

Year: 2026

شكر وتقدير

الحمد لله الذي وقّني لإتمام هذا العمل، والصلاة والسلام على المبعوث رحمةً للعالمين

أتوجه بخالص الشكر والامتنان إلى المشرفين الكريمين الدكتور الفيصل عبد الحميد والدكتور فايز جراد، على ما أولياني من توجيه علمي دقيق، ومتابعة حثيثة، وتصحيح مسار في كل مرحلة من مراحل هذا البحث. فضلها عليّ أكبر من أن يُختصر في سطور

وأشكر جامعة ميدأوشن وكلية الإدارة على البيئة الأكاديمية الداعمة التي أتاحت لي الفرصة لإنجاز هذه الرسالة

كما أتوجه بالشكر الجزيل إلى جميع المشاركين في الاستبانة من منسوبي الجهات الحكومية السعودية، الذين آثروا المشاركة الطوعية ومنحوا من وقتهم الثمين. وقد حرصتُ على الوفاء بالتزاماتي الأخلاقية تجاههم بضمان سرية إجاباتهم التامة واستخدامها لأغراض البحث العلمي البحت وفق ما أُقرّ في الاستبانة

وأخيراً، شكر موصول لكل من أسهم من قريب أو بعيد في إنجاز هذا العمل

الباحثة

ثناء إسحاق محمد حلواني

إهداء

...إلى من علّمني أن العلم نور لا يُطفأ، وأن الأمانة في البحث فضيلة قبل أن تكون منهجاً

إلى روح والدَيَّ الكريمين، اللذين زرعاً في نفسي حبّ المعرفة، وعلّمني الصدق مع النفس

، إلى ابني وبناتي وأحفادي ، اللذين احتضنوا غيابي خلف الكتب والأبحاث بصبر لم أستحقه

.ودعموني في كل لحظة تعب

إلى كل موظف حكومي يؤمن بأن عمله الرقمي اليوم هو البنية التي تقف عليها خدمات الغد، وأن

.إدارة المخاطر ليست ترفاً تنظيمياً بل مسؤولية إنسانية قبل كل شيء

إلى وطني المملكة العربية السعودية، الذي أعطاني فرصة أن أسهم ولو بحبة رمل في صرح رؤيته

2030.

فهرس المحتويات:

الإهداء

شكر وتقدير

قائمة الجداول

Abstract — المستخلص

الفصل الأول

المقدمة العامة للدراسة

- 1.1 المقدمة
- 1.2 مشكلة الدراسة
- 1.3 أهمية الدراسة
- 1.4 أهداف الدراسة
- 1.5 تساؤلات الدراسة
- 1.6 فروض الدراسة
- 1.7 النظرية العلمية المتبعة
- 1.8 حدود الدراسة
- 1.9 مصطلحات الدراسة

الفصل الثاني: الدراسات السابقة والإطار النظري

- 2.1 مقدمة
- 2.2 الدراسات السابقة
- 2.3 الإطار النظري لإدارة المخاطر الرقمية
- 2.4 الإطار النظري لاستدامة المشاريع التقنية
- 2.5 التعليق العام وموقع الدراسة الحالية

الفصل الثالث: منهجية الدراسة

- 3.1 مقدمة
- 3.2 منهج الدراسة
- 3.3 مجتمع البحث والعينة
- 3.4 أداة الدراسة
- 3.5 صدق الأداة وثباتها
- 3.6 حدود البحث
- 3.7 الأساليب الإحصائية
- 3.8 الاعتبارات الأخلاقية

الفصل الرابع: النتائج والتوصيات

- 4.1 مقدمة
- 4.2 تحليل البيانات — الإحصاء الوصفي
- 4.3 النتائج — اختبار الفرضيات

4.4 مناقشة النتائج

4.5 الاستنتاجات الرئيسية

4.6 التوصيات

4.7 محدودية الدراسة وآفاق البحث

4.8 خاتمة

المراجع

المراجع الأجنبية

الملاحق

الاستبانة

قائمة الجداول

جدول (1-3): توزيع العينة حسب طبيعة الجهة الحكومية

جدول (2-3): توزيع العينة حسب المسمى الوظيفي

جدول (3-3): توزيع العينة حسب سنوات الخبرة

جدول (4-3): محاور الاستبانة وعدد العبارات

جدول (3-5): مقياس ليكرت الخماسي

جدول (3-6): معيار تفسير المتوسطات الحسابية

جدول (3-7): معاملات ألفا كرونباخ

جدول (4-1): المتوسطات الحسابية لعبارات المحور الأول

جدول (4-2): المتوسطات الحسابية لعبارات المحور الثاني

جدول (4-3): المتوسطات الحسابية لعبارات المحور الثالث

جدول (4-4): المتوسطات الحسابية لعبارات المحور الرابع

جدول (4-5): ملخص المتوسطات الكلية للمحاور

جدول (4-6): نتائج معامل ارتباط بيرسون للفرضية الرئيسية

جدول (4-7): نتائج معامل ارتباط بيرسون للفرضيات الفرعية

جدول (4-8): نتائج تحليل الانحدار الخطي البسيط

ANOVA جدول (4-9): متوسطات مجموعات الخبرة ونتائج

جدول (4-10): ملخص نتائج اختبار الفرضيات

المستخلص

هدفت هذه الدراسة إلى قياس أثر إدارة المخاطر الرقمية بأبعادها الثلاثة — إدارة مخاطر الأمن السيبراني، وإدارة مخاطر الامتثال التشريعي، وإدارة مخاطر استمرارية الأعمال — على استدامة المشاريع التقنية في القطاع الحكومي السعودي، وذلك في سياق التحول الرقمي الذي تقوده رؤية المملكة واعتمدت الدراسة المنهج الوصفي التحليلي الكمي، وطُبِّقت الاستبانة على عينة مؤلفة من (25). 2030 مستجيباً من العاملين في المشاريع التقنية بالجهات الحكومية السعودية، ممن يشغلون مناصب قيادية أو تقنية.

أظهرت نتائج الدراسة وجود علاقة ارتباطية موجبة ودالة إحصائياً بين إجمالي إدارة المخاطر الرقمية وأن نموذج الانحدار يُفسّر ما نسبته (39.9%)، ($r=0.632$ ، $p=0.001$) واستدامة المشاريع التقنية من التباين في مستوى الاستدامة. وعلى مستوى الأبعاد، ثبت أثر ذو دلالة إحصائية لإدارة مخاطر ($r=0.592$ ، $p=0.003$) وإدارة مخاطر استمرارية الأعمال، الامتثال التشريعي ($p=0.074$) في حين لم يبلغ بُعد الأمن السيبراني حد الدلالة الإحصائية، ($p=0.002$) كما كشفت. الدراسة عن غياب فروق ذات دلالة إحصائية في مستوى إدارة المخاطر الرقمية تُعزى لمتغير سنوات الخبرة. وبناءً على هذه النتائج، قدّمت الدراسة جملة من التوصيات العملية لصانعي القرار في الجهات الحكومية.

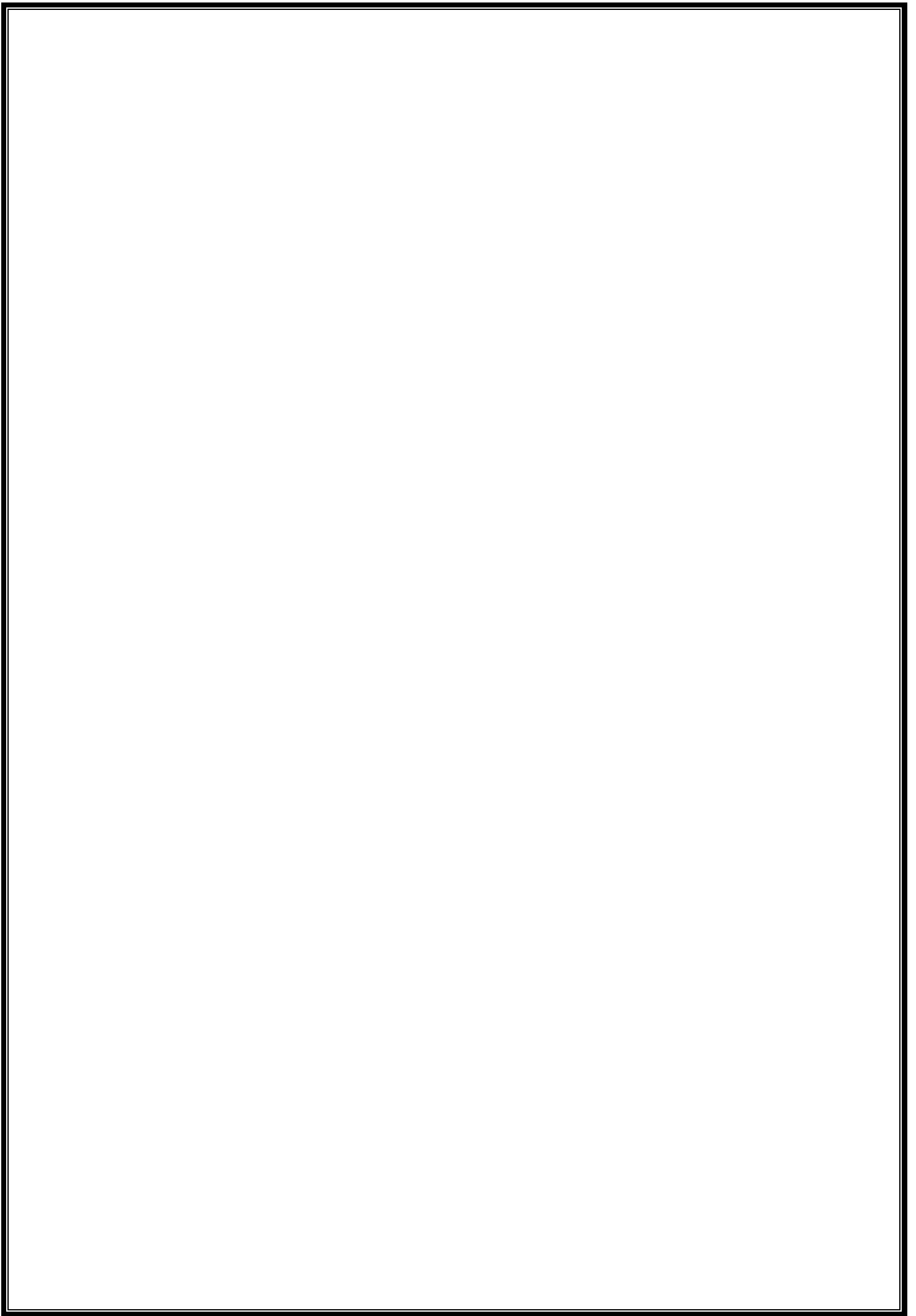
الكلمات المفتاحية: إدارة المخاطر الرقمية، الأمن السيبراني، الامتثال التشريعي، استمرارية الأعمال، استدامة المشاريع التقنية، القطاع الحكومي السعودي، رؤية 2030.

Abstract

This study aimed to measure the impact of digital risk management — across three key dimensions: cybersecurity risk management, regulatory compliance risk management, and business continuity risk management — on the sustainability of technology projects in the Saudi Arabian government sector, within the context of the digital transformation driven by Vision 2030. The study adopted a quantitative descriptive–analytical approach, applying a questionnaire to a sample of 25 respondents from employees working in technology projects within Saudi government entities.

Results revealed a statistically significant positive correlation between digital risk management and project sustainability ($r=0.632$, $p=0.001$), with the regression model explaining 39.9% of the variance in sustainability. Regulatory compliance risk ($r=0.570$, $p=0.003$) and business continuity risk ($r=0.592$, $p=0.002$) showed significant impacts, while cybersecurity risk management did not reach statistical significance ($p=0.074$). No significant differences were found based on years of experience. Based on these findings, the study presented practical recommendations for decision–makers in government entities.

Keywords: Digital Risk Management, Cybersecurity, Regulatory Compliance, Business Continuity, IT Project Sustainability, Saudi Government Sector, Vision 2030.



الفصل الأول

المقدمة العامة للدراسة

المقدمة 1.1

كما نعلم أن المملكة العربية السعودية تمر اليوم بمرحلة ،تحولاً رقمياً متسارعاً وشاملاً في إطار رؤية 2030 حيث أصبحت .المشاريع التقنية الحكومية ركيزة أساسية في تحديث منظومة الخدمات العامة وتعزيز كفاءتها وفي ظل هذا التحول، تتصاعد أهمية إدارة المخاطر الرقمية بوصفها أداة استراتيجية لا غنى عنها لضمان نجاح هذه المشاريع واستمرارها وتحقيق أهدافها على المدى البعيد.

وتظهر لمخاطر الرقمية في أشكال متعددة ومتداخلة؛ فمن الهجمات السيبرانية المتطورة التي تستهدف البنية التحتية الحكومية، إلى التهديدات المتعلقة بتسريب البيانات وانتهاك الخصوصية، وصولاً إلى مخاطر عدم الامتثال للتشريعات الرقمية الوطنية، ومخاطر انقطاع استمرارية الأعمال في أوقات الأزمات. كل هذه العوامل مجتمعة قادرة على إعاقة المسيرة التنموية للمشاريع التقنية الحكومية وتهديد استدامتها.

وتأتي هذه الدراسة في سياق البحث العلمي الميداني التطبيقي، لتسلط الضوء على واقع إدارة المخاطر الرقمية في القطاع الحكومي السعودي، وتقيس أثرها الفعلي على استدامة المشاريع التقنية وديمومتها. وقد اعتمدت الدراسة المنهج الوصفي التحليلي الكمي، مستخدمةً الاستبانة أداة رئيسية لجمع البيانات من العاملين في المشاريع التقنية بالجهات الحكومية السعودية.

وتتبع أهمية هذه الدراسة من كونها تعالج فجوة بحثية واضحة في الأدبيات العلمية العربية، التي تقتصر إلى الدراسات المتخصصة التي تربط بين إدارة المخاطر الرقمية واستدامة المشاريع التقنية في البيئة الحكومية السعودية تحديداً، كما تتسق أهدافها مع التوجهات الاستراتيجية لرؤية المملكة 2030.

1.2 مشكلة الدراسة

- بالرغم من التوسع الكبير في المشاريع التقنية الحكومية في إطار رؤية 2030، إلا أن كثيراً من الجهات الحكومية لا تزال تواجه تحديات جوهرية في إدارة مخاطرها الرقمية، مما يُفضي في أحيان كثيرة إلى تعثر مشاريعها التقنية أو تدهور مستوى خدماتها الرقمية. وقد تجلت هذه المشكلة في عدة مؤشرات:
- تكرار حوادث الاختراقات السيبرانية التي أثرت على استمرارية بعض الخدمات الرقمية الحكومية.
- ظهور حالات تعطل منصات حكومية بسبب غياب خطط التعافي من الكوارث أو عدم اختبارها دورياً.
- وجود مشاريع تقنية اضطرت إلى إعادة الهيكلة أو التوقف بسبب عدم الامتثال للتشريعات الرقمية الوطنية.
- محدودية الدراسات البحثية العربية المتخصصة في هذا المجال في السياق الحكومي السعودي.

وتتمثل مشكلة الدراسة في قلة وضوح أثر إدارة المخاطر الرقمية على استدامة المشاريع التقني

وتتضح :في التساؤل الرئيسي

ما أثر إدارة المخاطر الرقمية بأبعادها الثلاثة (الأمن السيبراني، الامتثال التشريعي، استمرارية

الأعمال) على استدامة المشاريع التقنية في القطاع الحكومي السعودي؟

أهمية الدراسة 1.3

أولاً: الأهمية العلمية

تُساهم هذه الدراسة في سد فجوة بحثية واضحة في الأدبيات العلمية العربية، إذ تُعدّ من الدراسات القليلة التي تتناول بصورة متخصصة العلاقة بين إدارة المخاطر الرقمية واستدامة المشاريع التقنية في القطاع الحكومي السعودي. كما تُضيف بُعداً ميدانياً كمياً يدعم الأطر النظرية القائمة بأدلة إحصائية من بيئة تنظيمية حكومية فعلية، ويُمثّل النموذج المفاهيمي الذي طورته الباحثة إضافةً منهجية يمكن توظيفها في دراسات مستقبلية.

ثانياً: الأهمية العملية

تتبع الأهمية العملية من توجيه نتائج الدراسة وتوصياتها مباشرةً لصانعي القرار في الجهات الحكومية السعودية، وتشمل: تحسين سياسات إدارة المخاطر الرقمية المعتمدة، وتعزيز آليات الامتثال للتشريعات وتطوير خطط استمرارية الأعمال، NDMO و DGA وإصدارات ECC الرقمية الوطنية كضوابط والتعافي من الكوارث، ودعم مستهدفات رؤية 2030 في محور التحول الرقمي

أهداف الدراسة 1.4

أولاً: الأهداف العلمية

1. لتعرف على مستوى تفعيل ممارسات إدارة المخاطر الرقمية بأبعادها الثلاثة في الجهات الحكومية السعودية.
2. قياس أثر كل بُعد من أبعاد إدارة المخاطر الرقمية على استدامة المشاريع التقنية بصورة مستقلة.
3. تحليل العلاقة الكلية بين المتغيرين وفق نموذج الانحدار الخطي البسيط .
4. إثراء الأدبيات البحثية العربية بدراسة ميدانية كمية في السياق الحكومي السعودي

ثانياً: الأهداف التطبيقية

1. تقديم توصيات عملية لصانعي القرار لتحسين ممارسات إدارة المخاطر الرقمية .
2. توفير نموذج مرجعي يمكن توظيفه في تصميم سياسات إدارة المخاطر المتوافقة مع رؤية 2030 .
3. رفع مستوى الوعي المؤسسي بأهمية إدارة المخاطر الرقمية

تساؤلات الدراسة 1.5

1. ما مستوى تفعيل ممارسات إدارة المخاطر الرقمية في الجهات الحكومية السعودية؟

2. ما أثر إدارة مخاطر الأمن السيبراني على استدامة المشاريع التقنية في القطاع

الحكومي السعودي؟

3. ما أثر إدارة مخاطر الامتثال التشريعي على استدامة المشاريع التقنية في القطاع

الحكومي السعودي؟

4. ما أثر إدارة مخاطر استمرارية الأعمال على استدامة المشاريع التقنية في القطاع

الحكومي السعودي؟

5. ما العلاقة الكلية بين إدارة المخاطر الرقمية واستدامة المشاريع التقنية؟

6. هل توجد فروق ذات دلالة إحصائية في مستوى إدارة المخاطر الرقمية تُعزى لمتغير

سنوات الخبرة؟

فروض الدراسة 1.6

الفرضية الرئيسية

بين إدارة المخاطر الرقمية واستدامة ($\alpha \leq 0.05$) توجد علاقة ذات دلالة إحصائية عند مستوى المشاريع التقنية في القطاع الحكومي السعودي.

الفرضيات الفرعية

H1: يوجد أثر ذو دلالة إحصائية لإدارة مخاطر الأمن السيبراني على استدامة المشاريع

التقنية في القطاع الحكومي السعودي.

H2: يوجد أثر ذو دلالة إحصائية لإدارة مخاطر الامتثال التشريعي على استدامة

المشاريع التقنية في القطاع الحكومي السعودي.

H3: يوجد أثر ذو دلالة إحصائية لإدارة مخاطر استمرارية الأعمال على استدامة

المشاريع التقنية في القطاع الحكومي السعودي.

H4: توجد فروق ذات دلالة إحصائية في مستوى تفعيل إدارة المخاطر الرقمية تُعزى

لمتغير سنوات الخبرة .

النظرية العلمية المتبعة لإعداد البحث 1.7

تستند هذه الدراسة إلى منظومة من الأطر النظرية والعلمية المعتمدة دولياً، وهي

(Enterprise Risk Management) أولاً: نظرية إدارة المخاطر المؤسسية

تُرسى هذه النظرية مبدأً أن إدارة المخاطر ليست نشاطاً هامشياً بل جزء لا يتجزأ من الإدارة هذه النظرية في إطار منهجي شامل ISO 31000:2018 الاستراتيجية للمؤسسة. وقد جسد معيار يُحدد مبادئ إدارة المخاطر وعملياتها، ويُرسخ ضرورة دمجها في صميم العمليات المؤسسية لتحقيق الأهداف الاستراتيجية.

NIST ثانياً: إطار الأمن السيبراني

الركيزة النظرية لبُعد الأمن (NIST CSF 2018) يُمثّل إطار المعهد الوطني للمعايير والتقنية والحماية، (Identify) السيبراني في هذه الدراسة. ويقوم على خمس وظائف محورية: التعرف وقد تبنت الهيئة. (Recover) والتعافي، (Respond) والاستجابة، (Detect) والكشف، (Protect) الإلزامية (ECC) الوطنية للأمن السيبراني مبادئه في صياغة الضوابط الأساسية للأمن السيبراني للجهات الحكومية السعودية.

(Organizational Resilience) ثالثاً: نظرية المرونة التنظيمية

تُشكل نظرية المرونة التنظيمية الأساس النظري لُبُعد استمرارية الأعمال في الدراسة، وتُعرّف بأنها قدرة المنظمة على التكيف مع التغيرات والتعافي من الأزمات والاستمرار في تحقيق أهدافها. وتتسجم هذه لإدارة استمرارية الأعمال، ومع مفهوم استدامة المشاريع التقنية الذي ISO 22301 النظرية مع معيار يُشكل المتغير التابع للدراسة.

PMBOK رابعاً: نموذج إدارة مشاريع

الإطار المنهجي لإدارة (PMI, 2021) الصادر عن معهد إدارة المشاريع PMBOK يُوفر دليل مخاطر المشاريع التقنية، ويُحدد العمليات الست الرئيسية لإدارة المخاطر: التخطيط، والتعريف، والتحليل النوعي، والتحليل الكمي، والتخطيط للاستجابة، والرقابة. وقد وُظف هذا الإطار في بناء النموذج المفاهيمي للدراسة وصياغة عبارات الاستبانة.

1.8 حدود الدراسة

1.8.1 الحدود الموضوعية

تقتصر الدراسة على قياس أثر إدارة المخاطر الرقمية بأبعادها الثلاثة على استدامة المشاريع التقنية وديمومتها، دون التطرق إلى أنواع المخاطر غير الرقمية أو القطاعات غير التقنية.

1.8.2 الحدود المكانية

تطبق الدراسة على الجهات الحكومية في المملكة العربية السعودية بمختلف أنواعها.

1.8.3 الحدود الزمنية

أُجريت الدراسة خلال العام الأكاديمي 2026م.

1.8.4 الحدود البشرية

تستهدف الدراسة العاملين في المشاريع التقنية في الجهات الحكومية ممن يشغلون مناصب قيادية أو تقنية ذات صلة مباشرة بموضوع الدراسة.

مصطلحات الدراسة 1.9

إدارة المخاطر الرقمية

منظومة متكاملة من الممارسات والإجراءات المؤسسية التي تتبناها الجهات الحكومية للتعامل مع المخاطر التقنية والسيبرانية، وتشمل ثلاثة أبعاد: إدارة مخاطر الأمن السيبراني، والامتثال التشريعي، واستمرارية الأعمال.

إدارة مخاطر الأمن السيبراني

مجموعة الإجراءات والضوابط الأمنية لحماية الأنظمة والمنصات التقنية الحكومية من التهديدات والفحوصات الدورية للثغرات وتأهيل الكوادر ECC وضوابط DevSecOps السيبرانية، وتشمل تطبيق التقنية.

إدارة مخاطر الامتثال التشريعي

مجموعة الآليات لضمان توافق المشاريع التقنية مع الأطر التشريعية الرقمية الوطنية كاشتراطات هيئة (NDMO) وسياسات مكتب إدارة البيانات الوطنية (DGA) الحكومة الرقمية.

إدارة مخاطر استمرارية الأعمال

مجموعة الخطط والإجراءات لضمان استمرار الخدمات التقنية في مواجهة الأزمات، تشمل خطط وتجارب المحاكاة وأنظمة النسخ الاحتياطي الموزعة (Disaster Recovery) التعافي من الكوارث.

استدامة المشاريع التقنية الحكومية

قدرة المشروع التقني الحكومي على الاستمرار في تقديم خدماته بكفاءة على المدى البعيد دون انقطاع ،غير مخطط، مع تحقيق الكفاءة المالية والمرونة الكافية للتوسع والاندماج مع المنظومة الرقمية الوطنية ،بما يتوافق مع مستهدفات رؤية 2030.

القطاع الحكومي السعودي

يُقصد به في سياق هذه الدراسة كافة الجهات الحكومية العاملة في المملكة العربية السعودية بمختلف تصنيفاتها الإدارية، سواء كانت وزارات أم هيئات عامة أم مؤسسات حكومية أم قطاعات إمارية وحكومة محلية، بشرط أن يكون لدى هذه الجهات مشاريع أو منصات تقنية رقمية قيد التشغيل أو التطوير.

رؤية المملكة 2030

الخطة الاستراتيجية الوطنية الشاملة التي أطلقتها المملكة العربية السعودية عام 2016م، وتستهدف من بين محاورها الرئيسية تسريع وتيرة التحول الرقمي وبناء حكومة رقمية فعّالة وكفؤة، وتُشكّل الإطار المرجعي الذي تستند إليه معظم التشريعات والسياسات الرقمية الوطنية المُشار إليها في هذه الدراسة NDMO وسياسات DGA واشتراطات ECC كضوابط

الفصل الثاني

الدراسات السابقة والإطار النظري

2.1 مقدمة

يُشكّل هذا الفصل الركيزة النظرية للدراسة، إذ يسعى إلى بناء فهم نظري متكامل لمتغيريها الرئيسيين: إدارة المخاطر الرقمية بأبعادها الثلاثة، واستدامة المشاريع التقنية الحكومية. ويعتمد الفصل على المراجع (Ferrari (2023 و NIST (2018 و ISO (2018 و PMI (2021: المُدرجة في البروبوزل مع الحرص على صياغة المحتوى بأسلوب تحليلي يعكس فهم الباحثة لهذه، (Zerioush (2024) المفاهيم.

وقد اختارت الباحثة أن يسير هذا الفصل وفق تسلسل منطقي يبدأ بمراجعة الدراسات السابقة ذات الصلة المباشرة بموضوع البحث، ثم ينتقل إلى بناء الإطار النظري لكل من متغيري الدراسة على حدة مع الربط المستمر بين كل مفهوم نظري وبين مؤشرات الميدانية التي ترجمتها عبارات الاستبانة، وينتهي بتعليق نقدي عام يُحدد بدقة موقع هذه الدراسة من الأدبيات السابقة والإضافة العلمية التي تُقدمها. وهذا التسلسل ليس شكلياً بل يعكس منهجية الباحثة في الانتقال من العام إلى الخاص، ومن النظري إلى الإجرائي القابل للقياس

الدراسات السابقة 2.2:

(NIST, 2018) للأمن السيبراني NIST أولاً: إطار

يُمثل هذا الإطار المرجع التأسيسي للبعد الأول من متغير الدراسة المستقل. وما يجعله ذا قيمة بحثية في هذه الدراسة تحديداً ارتباطه المباشر بالواقع التشريعي الحكومي السعودي؛ إذ اعتمدت الهيئة الوطنية الإلزامية. وتظهر القيمة المضافة لهذه الدراسة في ECC للأمن السيبراني مبادئه في صياغة ضوابط. اختبار مدى ترجمة هذه الضوابط إلى ممارسات فعلية وانعكاسها على استدامة المشاريع.

يتميز بمرونته العالية في التطبيق عبر قطاعات مختلفة، حيث انه لم NIST ويلاحظ أن إطار يُصمم في الأصل ليكون قائمة تحقق جامدة، بل منظومة توجيهية تسمح لكل مؤسسة ببناء ملف مخاطر خاص بها وفق طبيعة أصولها الرقمية ومستوى تعرضها للتهديدات. وهذه المرونة تحديداً هي ما يجعل تبني الهيئة الوطنية للأمن السيبراني لمبادئه أمراً منطقياً، إذ يُتيح للجهات الحكومية السعودية المتفاوتة في الحجم والتعقيد التقني أن تُطبق الإطار ذاته بدرجات مختلفة من العمق دون الإخلال بجوهر متطلباته.

(ISO, 2018) لإدارة المخاطر ISO ثانياً: معيار

يعتمد هذا المعيار المنهجية العامة لإدارة المخاطر المؤسسية، ويرسم الإطار النظري المرجعي لمتغير الدراسة المستقل ككل. والمنحنى الذي تستثمره هذه الدراسة منه توكيده على أن فاعلية إدارة المخاطر لا تُقاس بوجود الوثائق والسياسات بل بمستوى دمجها الفعلي في العمليات التشغيلية، وهو ما اجتهدت الاستبانة في قياسه عبر عبارات تعكس الممارسة الميدانية.

أنها تنظر إلى المخاطر بوصفها ظاهرة ملازمة لأي ISO 31000 ومن أبرز ما يُميز منهجية نشاط مؤسسي لا يمكن الاستغناء عنها بالكامل، بل يمكن فقط إدارتها إلى مستوى مقبول يتوازن مع الفرص المرجوة من النشاط ذاته. وهذا المنظور بالذات ينسجم مع طبيعة المشاريع التقنية الحكومية التي لا يمكنها التوقف عن التحول الرقمي خشية المخاطر، بل عليها أن تتعلم كيف تُدير هذه المخاطر بذكاء.

بينما تستمر في مسيرة التطوير والتحديث.

(PMI, 2021) لإدارة المشاريع PMBOK ثالثاً: دليل

يُضيف هذا الدليل إطاراً عملياً لإدارة مخاطر المشاريع، ويُربط استخدامه في هذه الدراسة بمتغير يُعدّ التعامل المنهجي مع المخاطر طوال دورة حياة المشروع، (PMI 2021) الاستدامة. فمن منظور شرطاً أساسياً لنجاحه واستمراره وقدرته على تحقيق أهدافه على المدى البعيد.

بُعداً مهماً يتصل مباشرةً بمشكلة هذه الدراسة، وهو التمييز بين نجاح PMBOK ويقدم دليل المشروع واستدامته؛ فالنجاح في هذا الدليل غالباً ما يُقاس بمعايير التسليم كالوقت والتكلفة والنطاق، بينما تمتد الاستدامة إلى ما بعد التسليم لتشمل قدرة المخرج على الاستمرار في تحقيق القيمة المرجوة منه. وهذا التمييز الدقيق هو ما دفع الباحثة لاختيار الاستدامة تحديداً، لا مجرد النجاح، متغيراً تابعاً لهذه الدراسة، إذ إن كثيراً من المشاريع التقنية الحكومية قد تُسلم بنجاح ظاهري ثم تتعثر لاحقاً في مرحلة التشغيل

في الرقمنة والاستدامة (Ferrari (2023 رابعاً: دراسة

تناولت هذه الدراسة العلاقة بين التحول الرقمي واستدامة المؤسسات، وتوصلت إلى نتيجة جوهرية تفيد بأن أثر التحول الرقمي على الاستدامة يتوقف جوهرياً على مستوى كفاءة إدارة المخاطر المصاحبة له. وتتسجم هذه النتيجة مع فرضيات الدراسة الحالية التي تقيس هذا الأثر في سياق القطاع الحكومي السعودي.

وتكمن القيمة الخاصة لهذه الدراسة في كونها لا تنظر إلى التحول الرقمي بوصفه خيراً مطلقاً بحد ذاته، بل تشترط لتحقيق أثره الإيجابي على الاستدامة وجود منظومة فعّالة لإدارة المخاطر المصاحبة له. وهذا الشرط بالذات هو جوهر ما تسعى هذه الدراسة إلى اختباره كمياً في البيئة الحكومية السعودية؛ إذ لا

يكفي أن تُطلق الجهة الحكومية مشاريع تقنية طموحة، بل يجب أن يصاحب ذلك استثمار موازٍ في إدارة

مخاطرها الرقمية حتى يتحقق الأثر الإيجابي المرجو على الاستدامة لا العكس

في إدارة المخاطر الحكومية (Zerioush (2024) خامساً: دراسة

تُعَدّ هذه الدراسة الأقرب صلةً بموضوع البحث الحالي، إذ تناولت واقع إدارة المخاطر في المشاريع

الحكومية في سياق التحول الرقمي. وخلصت إلى أن الجهات التي تعتمد ممارسات نشطة في إدارة

مخاطرها الرقمية تُحقق أداءً تشغيلياً أفضل وتكون أقل عرضةً للتعرض. وتتقاطع هذه النتيجة مع

الفرضيات الرئيسية للدراسة الحالية وتُعزز مسوّغ إجراءاتها في البيئة السعودية

مساهمة مهمة أخرى تتمثل في تأكيدها أن الفجوة بين السياسات المعلنة Zerioush وتُقدم دراسة

والتطبيق الفعلي هي السبب الأعظم وراء تعثر كثير من المشاريع الحكومية، لا غياب السياسات بحد

ذاته. فكثير من الجهات الحكومية تمتلك بالفعل أطراً وسياسات معتمدة لإدارة المخاطر الرقمية، لكن

التحدي الحقيقي يكمن في مدى ترجمة هذه السياسات إلى سلوك مؤسسي يومي فعلي. وهذا بالضبط ما

سعت استبانة هذه الدراسة إلى قياسه من خلال عبارات تصف الممارسة الفعلية لا مجرد وجود السياسة

المكتوبة.

الإطار النظري لإدارة المخاطر الرقمية

2.3.1 مفهوم إدارة المخاطر الرقمية

لا يمكن الحديث عن إدارة المخاطر الرقمية بمعزل عن السياق الذي نشأت فيه؛ فالتحول الرقمي المتسارع جعل المخاطر الرقمية جزءاً لا يتجزأ من الواقع التشغيلي اليومي، لا مجرد سيناريو استثنائي. وفي هذا الإطار، يمكن تعريف إدارة المخاطر الرقمية بأنها المنظومة المتكاملة من الإجراءات والسياسات المؤسسية الهادفة إلى تحديد المخاطر التقنية وتقييمها والتعامل معها ومراقبتها بصورة مستمرة. وقد تطور هذا المفهوم عبر ثلاث مراحل يمكن تمييزها بوضوح في الأدبيات الإدارية: المرحلة الأولى، وهي المرحلة التقنية البحتة التي اقتصر فيها إدارة المخاطر على أقسام تقنية المعلومات وحدها، وتعاملت مع المخاطر بوصفها مشكلة هندسية تُحل بالحلول التقنية فقط كجدران الحماية وبرامج مكافحة الفيروسات. أما المرحلة الثانية فهي مرحلة الحوكمة المؤسسية التي بدأت فيها المؤسسات تُدرك أن المخاطر الرقمية تتجاوز البُعد التقني لتشمل أبعاداً تنظيمية وقانونية ومالية، مما استدعى إشراك الإدارة العليا في صنع قرارات إدارة المخاطر. وأخيراً المرحلة الثالثة، وهي المرحلة الاستراتيجية التي تنتمي إليها هذه الدراسة، حيث أصبحت إدارة المخاطر الرقمية جزءاً من التخطيط الاستراتيجي للمؤسسة. ومرتبطة مباشرة بقدرتها على تحقيق أهدافها بعيدة المدى واستدامة مشاريعها.

البُعد الأول: إدارة مخاطر الأمن السيبراني 2.3.2

NIST يُعدّ الأمن السيبراني الوجه الأكثر حضوراً في منظومة المخاطر الرقمية. وقد صاغ إطار منهجية واضحة تقوم على خمس وظائف: التعرف والحماية والكشف والاستجابة والتعافي (2018) وتعكس عبارات المحور الأول من DevSecOps، لاستبانة هذا البُعد عبر أربعة مؤشرات: مدى تطبيق وكفاءة الكوادر التقنية في مواجهة التهديدات، ECC وانتظام فحص الثغرات، ومستوى تطبيق ضوابط ومن المهم التمييز هنا بين نمطين من التعامل مع الأمن السيبراني في سياق المشاريع التقنية: النمط يتعامل مع الثغرات والحوادث بعد وقوعها، والنمط الثاني استباقي (Reactive) الأول تفاعلي التي DevSecOps يدمج اعتبارات الأمن منذ اللحظة الأولى لتصميم النظام. ومنهجية (Proactive) تقيسها الاستبانة تُجسّد بالضبط هذا التحول من النمط التفاعلي إلى الاستباقي، إذ تعني عملياً أن فرق التطوير والأمن والتشغيل تعمل معاً منذ البداية بدلاً من أن يُضاف الأمن كطبقة لاحقة بعد اكتمال البناء. وهذا التحول له انعكاس مباشر على استدامة المشروع؛ إذ إن الثغرات التي تُكتشف بعد الإطلاق تكون أكثر كلفة وأصعب معالجة من تلك التي تُعالج في مرحلة التصميم.

البُعد الثاني: إدارة مخاطر الامتثال التشريعي 2.3.3

نشأ هذا البُعد من واقع التطور المتسارع للمنظومة التشريعية الرقمية في المملكة. والخطورة هنا أن

إغفاله قد يُجبر المشروع على التوقف الكلي أو إعادة الهيكلة بعد الإطلاق. وترتبط عبارات المحور

الثاني بهذا البُعد من خلال قياس: مدى اشتراط التوافق مع DGA منذ كراسات الشروط NDMO ،

والالتزام بسياسات ووجود آلية مستمرة لمتابعة التحديثات التشريعية

ويكتسب هذا البُعد أهمية خاصة في السياق السعودي تحديداً بسبب الوتيرة السريعة لصدور

التشريعات الرقمية الجديدة مقارنةً بدول أخرى أبطأ في هذا المجال؛ فالجهات الحكومية السعودية تجد

نفسها أمام تحدٍ مزدوج: مواكبة التحول الرقمي من جهة، ومواكبة التشريعات التي تُنظّم هذا التحول من

جهة أخرى في آن واحد. وهذا التزام بين التطوير التقني والتطوير التشريعي، إن لم يُدر بعناية، قد

يجعل المشروع التقني عرضة لأن يُصبح غير متوافق مع تشريع صدر بعد بدء تنفيذه، مما يستدعي

مرونة تصميمية عالية تسمح بالتكيف مع المتطلبات التنظيمية المستجدة دون الحاجة لإعادة بناء

المشروع من الصفر.

البُعد الثالث: إدارة مخاطر استمرارية الأعمال 2.3.4

يتناول هذا البُعد قدرة المشروع التقني على الصمود أمام الأزمات واستعادة عمله بسرعة. وما يُميزه

أن التقصير فيه لا يظهر في الأوقات الاعتيادية بل في لحظات الأزمة تحديداً. وتقيس عبارات المحور

وانتظام تجارب المحاكاة، واعتماد Disaster Recovery الثالث هذا البُعد من خلال: توافر خطط

.النسخ الاحتياطي الموزع، ووضوح خطط تفويض الصلاحيات وقت الأزمات

ويُمكن فهم هذا البُعد بصورة أعمق من خلال التمييز بين مفهومين متكاملين: استمرارية تقنية النظام

فالأولى تُعنى (Business Continuity) واستمرارية الأعمال المؤسسية (System Continuity)

باستعادة الأنظمة والبيانات فنياً بعد الحادث، بينما تمتد الثانية لتشمل استمرارية القرار الإداري وتوزيع

الأدوار والصلاحيات أثناء الأزمة ذاتها، حتى قبل اكتمال التعافي التقني الكامل. وهذا التمييز يُفسر لماذا

شملت عبارات هذا المحور في الاستبانة، إلى جانب الجوانب التقنية كالنسخ الاحتياطي، جانباً إدارياً

صريحاً يتعلق بوضوح خطط تفويض الصلاحيات، إذ إن غياب هذا الوضوح الإداري قد يُعطل التعافي

.حتى لو كانت الحلول التقنية جاهزة

الإطار النظري لاستدامة المشاريع التقنية

2.4.1 مفهوم الاستدامة في سياق المشاريع التقنية

حين يُطرح مفهوم الاستدامة في سياق المشاريع التقنية، فإنه يتجاوز المعنى البيئي الشائع ليُشير إلى قدرة المشروع على الاستمرار في تحقيق قيمته وأهدافه بعد الإطلاق. وفي البيئة الحكومية السعودية تحمل الاستدامة بُعداً إضافياً يتعلق بالتوافق مع المنظومة الرقمية الوطنية ومستهدفات رؤية 2030.

ويجدر التمييز هنا بين ثلاثة مستويات متدرجة لفهم استدامة المشروع التقني: المستوى الأول هو الاستمرار التقني البحت، أي بقاء النظام يعمل فنياً دون تعطل. والمستوى الثاني هو الاستمرار الوظيفي أي بقاء النظام محققاً للغرض الذي أنشئ من أجله وتلبيته لاحتياجات مستخدميهِ المتغيرة. أما المستوى الثالث والأعمق فهو الاستمرار الاستراتيجي، أي بقاء المشروع منسجماً مع التوجهات المؤسسية والوطنية الكبرى حتى وإن تطورت هذه التوجهات بعد إطلاق المشروع. وقد سعت هذه الدراسة إلى قياس المستويات الثلاثة معاً من خلال أبعادها الأربعة، بحيث لا تكتفي بقياس الاستمرارية التقنية وحدها بل تمتد لتشمل الأبعاد الإدارية والاستراتيجية الأعمق.

أبعاد الاستدامة في الدراسة الحالية 2.4.2

تنقسم أبعاد الاستدامة في هذه الدراسة إلى قسمين

القسم الأول — الأبعاد العامة: تشمل الكفاءة المالية (قدرة المشروع على تحقيق أهدافه في حدود ميزانيته)، والمرونة والقابلية للتوسع (قدرة المنصة على التكيف مع الاحتياجات المتغيرة والاندماج مع الأنظمة الوطنية).

وتعد هاتان السمتان مشتركتين بين أي مشروع تقني ناجح بصرف النظر عن قطاعه، إذ لا يختلف قياسهما جوهرياً بين مشروع تقني حكومي وآخر في القطاع الخاص.

القسم الثاني — الأبعاد الخاصة بهذه الدراسة: تشمل الاستمرارية التشغيلية (قدرة المشروع

على تقديم خدماته دون انقطاع غير مخطط له في السياق الحكومي السعودي)، والنضج الإداري الرقمي

مستوى نضج المؤسسة في التعامل مع المخاطر الرقمية وتحديات التحول الرقمي وفق ما أكدته

وهذان البُعدان يكتسبان طابعاً خاصاً في السياق الحكومي، إذ ترتبط الاستمرارية (Ferrari, 2023)

التشغيلية بثقة المواطن في الخدمة العامة ذاتها، ويرتبط النضج الإداري الرقمي بمدى انسجام الجهة مع

منظومة التحول الرقمي الوطني الأشمل ومستهدفات رؤية 2030 تحديداً، لا بمعايير عامة للنضج

المؤسسي كما تُقاس في أي قطاع آخر

2.5 الربط بين الإطار النظري وعبارات الاستبانة

،حرصاً على تحقيق الاتساق المنهجي الكامل بين الإطار النظري لهذا الفصل وأداة الدراسة الميدانية تعرض الباحثة في هذا المبحث خريطة تفصيلية تُبين كيف تُترجم كل عبارة من عبارات الاستبانة الست عشرة مفهوماً نظرياً محدداً من الأطر التي استعرضتها هذه الدراسة. وتُمثّل هذه الخريطة ضمانة الذي أُشير إليه في الفصل الثالث، إذ تُظهر بوضوح أن (Construct Validity) إضافية لصدق البناء كل عبارة لم تُصنع اعتباطاً بل استُمدت من مرجعية نظرية أو تشريعية محددة.

جدول (1-2): الربط بين محاور الاستبانة والإطار النظري والتشريعي

المحور	العبارات (م)	المرجعية النظرية/التشريعية
الأمن السيبراني	1 – 4	وضوابط (2018) NIST إطار الصادرة عن الهيئة ECC الوطنية للأمن السيبراني
الامتثال التشريعي	5 – 8	اشتراطات هيئة الحكومة وسياسات (DGA) الرقمية مكتب إدارة البيانات الوطنية (NDMO)
استمرارية الأعمال	9 – 12	ومبدأ (2018) ISO معيار المرونة التنظيمية (Organizational Resilience)
استدامة المشاريع (تابع)	13 – 16	نموذج PMBOK (PMI, 2021) ودراسة Ferrari في النضج الرقمي (2023) المؤسسي

ويلاحظ على أن يعكس كل محور تسلسلاً منطقياً يبدأ بالمؤشرات الأكثر تقنية وملموسية (كتطبيق في المحور الأول) وينتهي بالمؤشرات الأكثر إدارية واستراتيجية (كوجود آلية مستمرة DevSecOps للمتابعة في المحور الثاني، وخطط تفويض الصلاحيات في المحور الثالث). وهذا التدرج من التقني إلى إلى (NIST) الإداري يعكس بدوره التدرج النظري الذي تناولته هذه الدراسة من النظريات التقنية البحتة. النظريات الإدارية الأشمل (المرونة التنظيمية ونظرية إدارة المخاطر المؤسسية).

كما تجدر الإشارة إلى أن هذا الربط المباشر بين النظرية والأداة الميدانية هو ما مكّن الباحثة من تفسير النتائج الإحصائية التي سيعرضها الفصل الرابع تفسيراً نظرياً متماسكاً؛ فحين تظهر نتيجة دالة إحصائياً لبُعد الامتثال التشريعي، فإن هذه الدلالة لا تبقى رقماً مجرداً، بل تُقرأ في ضوء ما أسسته هذه في حماية استدامة المشاريع التقنية NDMO وسياسات DGA الدراسة نظرياً حول دور اشتراطات الحكومية.

من هذا الجدول أن بناء الاستبانة لم يكن عشوائياً في ترتيب عباراتها؛ فقد حرصت الباحثة

2.6 التعليق العام وموقع الدراسة الحالية من الدراسات السابقة

تكشف قراءة المراجع والدراسات السابقة مجتمعةً عن ثلاثة توجهات

أولها الاتفاق على أهمية إدارة المخاطر كعامل مؤثر في نجاح المشاريع واستدامتها

وثانيها تركّز معظم الأطر الدولية على المستوى المفاهيمي دون اختبار ميداني كمي في بيئات

حكومية محددة.

وثالثها غياب الدراسات العربية المتخصصة الكمية في السياق الحكومي السعودي.

وهنا تحديداً تبرز إضافة الدراسة الحالية؛ فهي لا تكتفي بالتظير بل تنزل إلى الميدان لتقيس واقع هذه العلاقة في جهات حكومية سعودية فعلية، وتختبر إحصائياً أيّ أبعاد إدارة المخاطر الرقمية يحدث أكبر أثر في الاستدامة، مما يجعلها إضافة حقيقية للأدبيات.

:ويمكن تلخيص الإضافة العلمية لهذه الدراسة في ثلاث نقاط جوهرية

أولاً، تفكيك متغير إدارة المخاطر الرقمية إلى ثلاثة أبعاد قابلة للقياس المنفصل بدلاً من التعامل معه كمفهوم واحد متجانس كما فعلت أغلب الدراسات السابقة.

ثانياً، اختبار هذه العلاقة ميدانياً وكمياً في بيئة حكومية سعودية محددة زمنياً ومكانياً، بدلاً من الاكتفاء بالتظير العام كما هو الحال في أغلب الأطر الدولية المستعرضة.

وثالثاً، تقديم خريطة نظرية-إجرائية واضحة (الموضحة في الجدول 2-1) تربط كل عبارة استبانة بمرجعيتها النظرية أو التشريعية، وهو ما يُعزز إمكانية تكرار هذه الدراسة أو البناء عليها في أبحاث مستقبلية مشابهة.

الفصل الثالث

منهجية الدراسة

3.1 مقدمة

يُعنى هذا الفصل بعرض الإجراءات المنهجية التي اتبعتها الباحثة في تصميم الدراسة وجمع البيانات وتحليلها. وإن كان الفصل السابق قد رسم الإطار النظري، فإن هذا الفصل يُجيب عن سؤال مختلف: كيف تُرجمت تلك الأفكار النظرية إلى إجراءات بحثية ميدانية قابلة للقياس

3.2 منهج الدراسة

اعتمدت الدراسة المنهج الوصفي التحليلي الكمي، وهو الأنسب لطبيعة مشكلة البحث وأهدافه. فمن جهة يسعى إلى وصف واقع ممارسات إدارة المخاطر الرقمية في الجهات الحكومية السعودية كما هو قائم دون تدخل أو تجريب، ومن جهة أخرى يسعى إلى تحليل العلاقة بين هذه الممارسات ومستوى التي اعتمدت (Zeriuoh (2024 الاستدامة بأدوات إحصائية دقيقة. ويتسق هذا المنهج مع توجه دراسة المنهج ذاته في استكشاف واقع إدارة المخاطر الحكومية.

وقد استبعدت الباحثة عمداً استخدام المنهج التجريبي نظراً لاستحالة التحكم في متغيرات إدارة المخاطر الرقمية داخل بيئات حكومية فعلية، كما استبعدت الاكتفاء بالمنهج النوعي وحده رغم ما يوفره من عمق تفسيري، ذلك أن طبيعة الفرضيات المصاغة تتطلب قياساً كمياً دقيقاً لدرجة الارتباط وقوة الأثر بين المتغيرات، وهو ما لا يتحقق إلا من خلال أدوات القياس الكمي كمعامل ارتباط بيرسون وتحليل الانحدار. ومع ذلك، أدركت الباحثة أن المنهج الكمي وحده لا يخلو من محدودية في تفسير الأسباب العميقة وراء بعض النتائج، وهو ما عالجتُه جزئياً من خلال ربط كل نتيجة رقمية بمناقشة تحليلية مستفيضة في الفصل الرابع

مجتمع البحث والعينة 3.3

مجتمع الدراسة 3.3.1

يتكون مجتمع الدراسة من العاملين في المشاريع التقنية في الجهات الحكومية السعودية ممن يشغلون مناصب قيادية أو تقنية ذات صلة مباشرة بموضوع الدراسة. ولم يُقَيِّد مجتمع الدراسة بجهة بعينها بل شمل الجهات الحكومية بأنواعها مما يمنح النتائج قدراً أكبر من الشمولية.

3.3.2 عينة الدراسة

وبلغ إجمالي Google Forms. اعتمدت الباحثة أسلوب العينة العشوائية المتاحة عبر منصة الاستجابات الصحيحة القابلة للتحليل (25) استجابة. وعلى الرغم من أن هذا الحجم متواضع نسبياً، إلا أنه مقبول في ضوء طبيعة المجتمع غير المحدود وخصوصية الفئة المستهدفة.

3.3.3 خصائص عينة الدراسة

جدول (3-1): توزيع العينة حسب طبيعة الجهة الحكومية

النسبة المئوية	التكرار	طبيعة الجهة الحكومية
56%	14	هيئة عامة / مؤسسة حكومية
32%	8	وزارة
12%	3	قطاع إماري / قطاع بلدي وحكومة محلية
100%	25	المجموع

تُهيمن الهيئات العامة على العينة بنسبة 56%، يليها العاملون في الوزارات بنسبة 32%، ثم القطاعات الإمارة بنسبة 12%. ويعكس هذا التوزيع التنوع المؤسسي للجهات الحكومية السعودية مما يُعزز تمثيلية العينة

جدول (3-2): توزيع العينة حسب المسمى الوظيفي

النسبة المئوية	التكرار	المسمى الوظيفي
52%	13	مدير إدارة / رئيس قسم
24%	6	مدير
24%	6	مهندس أنظمة
100%	25	المجموع

تُهيمن فئة مديري الإدارات ورؤساء الأقسام على العينة بنسبة 52%، وهو مؤشر إيجابي على جودة العينة إذ تمثل هذه الفئة أكثر الشرائح احتكاكاً بواقع إدارة المخاطر الرقمية يومياً

جدول (3-3): توزيع العينة حسب سنوات الخبرة

النسبة المئوية	التكرار	سنوات الخبرة
48%	12	أكثر من 10 سنوات
36%	9	من 5 إلى 10 سنوات
16%	4	أقل من 5 سنوات
100%	25	المجموع

تبلغ نسبة من يمتلكون خبرة لا تقل عن خمس سنوات 84% من العينة، مما يُضفي مصداقية عالية على الاستجابات

3.4 أداة الدراسة

اعتمدت الدراسة الاستبانة أداة رئيسية لجمع البيانات. وقد صُممت بالاستناد إلى الأطر الدولية مع مراعاة خصوصية البيئة الحكومية، (NIST, 2018; ISO, 2018; PMI, 2021) المعتمدة السعودية والتشريعات الرقمية الوطنية.

وقد بُنيت الاستبانة في صورتها النهائية اتساقاً تاماً مع النموذج المفاهيمي الذي عرضه الفصل الأول والذي حدّد مسبقاً في وثيقة اقتراح البحث (البروبوزل) ثلاثة أبعاد مستقلة ومتغيراً تابعاً واحداً. ولم تُدخل الباحثة أي تعديل جوهري على هذا النموذج أثناء صياغة الاستبانة، بل التزمت بترجمته حرفياً إلى عبارات قابلة للقياس، بما يضمن تسلسلاً منهجياً كاملاً من مشكلة الدراسة كما صيغت في البروبوزل مروراً بالإطار النظري في الفصل الثاني، وصولاً إلى أداة القياس ذاتها.

جدول (3-4): محاور الاستبانة وعدد العبارات

عدد العبارات	المحور	الرقم
عبارات 4	إدارة مخاطر الأمن السيبراني	المحور الأول
عبارات 4	إدارة مخاطر الامتثال التشريعي	المحور الثاني
عبارات 4	إدارة مخاطر استمرارية الأعمال	المحور الثالث
عبارات 4	استدامة المشاريع التقنية (المتغير التابع)	المحور الرابع
عبارة 16	الإجمالي	

وُظف مقياس ليكرت الخماسي لقياس استجابات أفراد العينة:

جدول (3-5): مقياس ليكرت الخماسي

الدرجة	الاستجابة
5	موافق بشدة
4	موافق
3	محايد
2	غير موافق
1	غير موافق بشدة

جدول (3-6): معيار تفسير المتوسطات الحسابية

المدى	مستوى الموافقة
4.21 – 5.00	مرتفع جداً
3.41 – 4.20	مرتفع
2.61 – 3.40	متوسط
1.81 – 2.60	منخفض
1.00 – 1.80	منخفض جداً

3.5 صدق الأداة وثباتها

الصدق الظاهري

عُرضت الاستبانة على المشرفين الأكاديميين د. الفیصل عبد الحمید ود. فايز جراد، اللذين أبدیا ملاحظاتهما وتعديلاتهما. وقد أخذت هذه التعديلات بعين الاعتبار في النسخة النهائية مما يُعزز الصدق الظاهري.

صدق البناء

حرصت الباحثة على ربط كل عبارة بمؤشر ميداني ملموس مستوحى من الأطر الدولية والتشريعات الرقمية الوطنية، بما يضمن أن تعكس كل عبارة جانباً حقيقياً من الظاهرة المدروسة.

ثبات الأداة — معامل ألفا كرونباخ

جدول (3-7): معاملات ألفا كرونباخ لمحاور الاستبانة

المحور	معامل ألفا	التفسير
المحور الأول: الأمن السيبراني	0.287	*مقبول
المحور الثاني: الامتثال التشريعي	0.521	مقبول
المحور الثالث: استمرارية الأعمال	0.742	جيد
المحور الرابع: الاستدامة	0.608	جيد
الأداة الكلية	0.815	جيد جداً

المعامل المنخفض لمحور الأمن السيبراني يُعزى إلى محدودية حجم العينة وتجانس الإجابات (*).

ويبقى الثبات الكلي (0.815) في المستوى الجيد جداً.

3.6 حدود البحث

الحدود الموضوعية: تقتصر على قياس أثر إدارة المخاطر الرقمية بأبعادها الثلاثة على الاستدامة

.دون أنواع المخاطر الأخرى

.الحدود المكانية: الجهات الحكومية في المملكة العربية السعودية بمختلف أنواعها

.الحدود الزمنية: العام الأكاديمي 2026م

.الحدود البشرية: العاملون في المشاريع التقنية الحكومية ممن يشغلون مناصب قيادية أو تقنية

3.7 الأساليب الإحصائية

وُظِّفَتْ فِي هَذِهِ الدِّرَاسَةِ أَرْبَعَةُ أَسَالِيبَ إِحْصَائِيَّةٍ رَئِيسِيَّةٍ، اخْتِيرَتْ بِعَنَايَةٍ بَحِثٍ يَخْدُمُ كُلَّ أُسْلُوبٍ هَدَفًا

:بَحْثِيًّا مُحَدَّدًا مِنْ أَهْدَافِ الدِّرَاسَةِ وَتَسْأُؤَلَاتِهَا

أولاً: الإحصاء الوصفي

استُخدم الإحصاء الوصفي، متمثلاً في التكرارات والنسب المئوية للمتغيرات الديموغرافية، والمتوسطات الحسابية والانحرافات المعيارية لعبارات ومحاور الاستبانة، للإجابة عن التساؤل الأول المتعلق بمستوى تفعيل ممارسات إدارة المخاطر الرقمية. ويُعدّ هذا الأسلوب نقطة الانطلاق الضرورية لأي تحليل استدلالي لاحق، إذ يُقدم صورة أولية عن واقع الظاهرة المدروسة قبل الانتقال إلى اختبار العلاقات بينها.

(Pearson Correlation) ثانياً: معامل ارتباط بيرسون

وُظّف معامل ارتباط بيرسون لقياس قوة العلاقة واتجاهها بين كل بُعد من أبعاد إدارة المخاطر الرقمية وبين استدامة المشاريع التقنية. وقد اختير هذا المعامل تحديداً، دون غيره من معاملات الارتباط اللامعلمية، نظراً لكون بيانات الدراسة كمية مستمرة (ناتجة عن حساب متوسطات مقياس ليكرت)، وهو الشرط الأساسي لاستخدام هذا المعامل بصورة صحيحة إحصائياً.

(Simple Linear Regression) ثالثاً: تحليل الانحدار الخطي البسيط

استُخدم تحليل الانحدار الخطي البسيط لاختبار الفرضية الرئيسية وقياس الأثر التنبؤي لإدارة الذي يُوضح النسبة (R^2) المخاطر الرقمية على استدامة المشاريع، من خلال تقدير معامل التحديد (Beta) المئوية من التباين في المتغير التابع التي يُفسّرها المتغير المستقل، إضافة إلى معامل الانحدار الذي يُقدّر مقدار التغير المتوقع في الاستدامة مقابل كل وحدة تغير في إدارة المخاطر الرقمية.

(One-Way ANOVA) رابعاً: تحليل التباين الأحادي

وُظف تحليل التباين الأحادي للإجابة عن الفرضية الرابعة المتعلقة بالفروق في مستوى إدارة المخاطر، الرقمية تبعاً لمتغير سنوات الخبرة، الذي يضم ثلاث فئات (أقل من 5 سنوات، من 5 إلى 10 سنوات للعينات المستقلة كون المتغير التصنيفي (t) أكثر من 10 سنوات). وقد فُصل هذا الاختبار على اختبار (Type I) لتفادي تضخم خطأ النوع الأول ANOVA (الخبرة) يضم أكثر من فئتين، مما يستدعي استخدام الذي قد ينتج عن إجراء مقارنات ثنائية متعددة (Error I).

في إجراء جميع SciPy وPandas بمكتبتيه Python وقد استخدم برنامج التحليل الإحصائي التحليلات الإحصائية المذكورة أعلاه، بعد تحويل استجابات مقياس ليكرت النصية إلى قيم رقمية (من 1 إلى 5) وفق الترميز الموضح في الجدول (3-5)

3.8 الاعتبارات الأخلاقية

التزمت الباحثة في جميع مراحل هذه الدراسة، من تصميم الاستبانة إلى جمع البيانات وتحليلها وعرض نتائجها، بمنظومة صارمة من الاعتبارات الأخلاقية للبحث العلمي، تفصيلها على النحو الآتي:

▶ الطوعية التامة: أبلغ جميع المستجيبين، من خلال المقدمة التعريفية للاستبانة، بأن مشاركتهم طوعية بالكامل، وأن لهم الحق الكامل في الانسحاب من الاستبيان أو عدم إكماله في أي وقت دون أي تبعات.

▶ السرية والخصوصية التامة: لم تطلب الاستبانة أي معلومات تعريفية شخصية كالاسم أو البريد الإلكتروني أو رقم الهاتف، كما لم تستفسر عن أي تفاصيل تقنية حساسة أو ثغرات أمنية خاصة بالجهة الحكومية التي ينتمي إليها المستجيب، حرصاً على عدم تعريض أي جهة لمخاطر أمنية من خلال المشاركة في البحث العلمي.

▶ الاستخدام الأكاديمي الحصري: أكد صراحةً للمستجيبين في مقدمة الاستبانة أن البيانات المجمعة ستستخدم حصرياً لأغراض البحث العلمي، وأن النتائج ستعرض في صورة مؤشرات إحصائية مجمعة (كمتوسطات ونسب مئوية) لا إجابات فردية يمكن أن تُنسب إلى مستجيب بعينه.

▶ الأمانة العلمية والنزاهة الأكاديمية: التزمت الباحثة بتوثيق جميع المصادر والمراجع المعتمدة في هذه الدراسة توثيقاً دقيقاً، وعزو كل فكرة أو نتيجة إلى مصدرها الأصلي، مع الحرص التام على صياغة المحتوى النظري بأسلوب الباحثة الخاص تحليلاً لا نسخاً، وعدم

اللجوء إلى أي شكل من أشكال الاقتباس غير الموثق أو إعادة الصياغة المُخلّة بحقوق الملكية الفكرية للمصادر المُستخدمة.

الشفافية في عرض النتائج: التزمت الباحثة بعرض جميع النتائج الإحصائية كما أسفر ◀

H1 عنها التحليل الفعلي للبيانات، بما في ذلك النتائج غير الدالة إحصائياً (كنتيجة الفرضية

دون أي محاولة لتعديل البيانات أو انتقاء النتائج بما يخدم فرضيات الدراسة، إيماناً من ،(H4و

الباحثة بأن قيمة البحث العلمي تكمن في صدقه لا في توافقه مع التوقعات المسبقة.

الفصل الرابع

النتائج والتوصيات

4.1 مقدمة

يُقدّم هذا الفصل ثمرة الجهد الميداني للدراسة، إذ يعرض النتائج الإحصائية التي أسفر عنها تحليل بيانات الاستبانة ويُفسّرها في ضوء أهداف البحث وفرضياته. ثم يتبعها مناقشة في ضوء الأدبيات السابقة، واستنتاجات، وتوصيات عملية.

4.2 تحليل البيانات — الإحصاء الوصفي

المحور الأول: إدارة مخاطر الأمن السيبراني 4.2.1

جدول (4-1): المتوسطات الحسابية والانحرافات المعيارية للمحور الأول

المستوى	الانحراف	المتوسط	العبرة	م
مرتفع جداً	1.04	4.36	دمج متطلبات الأمن السيبراني في دورة حياة الأنظمة (DevSecOps)	1
مرتفع جداً	0.79	4.28	ممارسات دورية لفحص الثغرات البرمجية وحماية قنوات نقل البيانات	2
مرتفع جداً	0.58	4.40	في تقليل حوادث شلل الخدمات ECC تطبيق ضوابط الرقمية	3
مرتفع	0.75	4.04	امتلاك الكوادر التقنية وعياً كافياً بالمهارات السيبرانية	4
مرتفع جداً	0.45	4.27	المتوسط الكلي للمحور	

تكشف نتائج المحور الأول عن مستوى مرتفع جداً لممارسات الأمن السيبراني (م=4.27). تصدرت بمتوسط (4.40) مما يُشير إلى أولوية الامتثال للتشريعات الوطنية. وجاءت ECC عبارة تطبيق ضوابط .عبارة الكوادر التقنية أدناها (4.04) مما يُلمح إلى حاجة مستمرة لتطوير القدرات البشرية

المحور الثاني: إدارة مخاطر الامتثال التشريعي

جدول (4-2): المتوسطات الحسابية والانحرافات المعيارية للمحور الثاني

المستوى	الانحراف	المتوسط	العبرة	م
مرتفع جداً	0.65	4.44	اشتراط مواءمة المشاريع مع تشريعات هيئة الحكومة الرقمية (DGA)	5
مرتفع جداً	0.59	4.52	الالتزام بسياسات حوكمة وحماية البيانات الوطنية (NDMO)	6
مرتفع	0.93	4.04	مساهمة التشريعات المسبقة في تجنب التوقف أو التعديل الجذري	7
مرتفع	0.78	4.12	وجود آلية مستمرة لمتابعة التحديثات التشريعية وتحديث السياسات	8
مرتفع جداً	0.48	4.28	المتوسط الكلي للمحور	

حقّق محور الامتثال التشريعي أعلى متوسط كلي (4.28). وتصدّرت عبارة الالتزام بسياسات

بمتوسط استثنائي (4.52) هو الأعلى في الدراسة كلها، مما يُشير إلى ترسخ ثقافة حوكمة NDMO

البيانات في الممارسة الحكومية السعودية بفعل الإلزامية التشريعية وآليات المتابعة والرقابة.

المحور الثالث: إدارة مخاطر استمرارية الأعمال 4.2.3

جدول (3-4): المتوسطات الحسابية والانحرافات المعيارية للمحور الثالث

المستوى	الانحراف	المتوسط	العبارة	م
مرتفع جداً	0.75	4.32	(Disaster Recovery) توافر خطط التعافي من الكوارث وجاهزيتها	9
مرتفع	0.75	4.16	الالتزام بسياسات حوكمة البيانات وأنظمة الحماية أثناء الأزمات	10
مرتفع	0.73	4.12	إجراء تجارب محاكاة دورية لاختبار مرونة الأنظمة	11
مرتفع	0.89	4.04	اعتماد أنظمة نسخ احتياطي مشفرة وموزعة جغرافياً	12
مرتفع	0.59	4.16	المتوسط الكلي للمحور	

جاء محور استمرارية الأعمال بمتوسط كلي (4.16). وتصدّرت عبارة توافر خطط التعافي من الكوارث (4.32)، في حين جاءت أنظمة النسخ الاحتياطي الموزعة أدناها (4.04) مما قد يعكس تحدي التكلفة والبنية التحتية.

المحور الرابع: استدامة المشاريع التقنية (المتغير التابع)

جدول (4-4): المتوسطات الحسابية والانحرافات المعيارية للمحور الرابع

المستوى	الانحراف	المتوسط	العبارة	م
مرتفع	0.93	3.88	نجاح المشاريع في تقديم خدماتها دون انقطاع تشغيلي غير مخطط	13
مرتفع	0.76	4.20	مساهمة الحوكمة الرقمية في الكفاءة المالية وضبط الإنفاق	14
مرتفع جداً	0.72	4.24	مرونة المنصات التقنية للتوسع والاندماج مع الأنظمة الوطنية	15
مرتفع جداً	0.66	4.24	عكس النضج الإداري للمفهوم الحقيقي لديمومة المشاريع التقنية	16
مرتفع	0.53	4.14	المتوسط الكلي للمحور	

بلغ المتوسط الكلي للمتغير التابع (4.14). وتلفت عبارة الاستمرارية التشغيلية الانتباه بأدنى متوسط وأعلى انحراف (0.93) مما يكشف عن تفاوت واقعي في تجربة الانقطاع التشغيلي بين (3.88) الجهات.

ملخص المتوسطات الكلية

جدول (4-5): ملخص المتوسطات الكلية لمحاور الدراسة

المستوى	الانحراف	المتوسط الكلي	المحور	م
مرتفع جداً	0.45	4.27	إدارة مخاطر الأمن السيبراني	1
مرتفع جداً	0.48	4.28	إدارة مخاطر الامتثال التشريعي	2
مرتفع	0.59	4.16	إدارة مخاطر استمرارية الأعمال	3

مرتفع	0.53	4.14	استدامة المشاريع التقنية (تابع)	4
-------	------	------	---------------------------------	---

4.3 النتائج — اختبار الفرضيات

4.3.1 الفرضية الرئيسية

جدول (4-6): نتائج معامل ارتباط بيرسون للفرضية الرئيسية

القرار	مستوى الدلالة (p)	معامل الارتباط (r)	المتغيران
✓ قبول الفرضية	0.001	0.632	إدارة المخاطر الرقمية ← استدامة المشاريع

دالة إحصائية، ($r=0.632$) تشير النتائج إلى وجود علاقة ارتباطية موجبة ومتوسطة إلى قوية

وبناءً عليه تُقبل الفرضية الرئيسية. ($p=0.001$)

4.3.2 الفرضيات الفرعية

جدول (4-7): نتائج معامل ارتباط بيرسون للفرضيات الفرعية

القرار	p مستوى	r معامل	البُعد	الفرضية
X رفض	0.074	0.363	إدارة مخاطر الأمن السيبراني	H1
✓ قبول	0.003	0.570	إدارة مخاطر الامتثال التشريعي	H2
✓ قبول	0.002	0.592	إدارة مخاطر استمرارية الأعمال	H3

4.3.3 نتائج تحليل الانحدار

جدول (4-8): نتائج تحليل الانحدار الخطي البسيط

المؤشر	القيمة
(R) معامل الارتباط	0.632
(R ²) معامل التحديد	0.399
(Beta) معامل الانحدار	0.802
قيمة الثابت	0.740
(p) مستوى الدلالة	0.001

يُفسّر النموذج (39.9%) من التباين في الاستدامة. ومعادلة الانحدار

$$\text{الاستدامة} = 0.740 + 0.802 \times (\text{إدارة المخاطر الرقمية})$$

H4 اختبار فرضية الفروق

ANOVA جدول (4-9): متوسطات مجموعات الخبرة ونتائج

مجموعة الخبرة	العدد	المتوسط	F قيمة	p مستوى	القرار
أقل من 5 سنوات	4	4.312	0.084	0.920	X H4 رفض
من 5 إلى 10 سنوات	9	4.241			
أكثر من 10 سنوات	12	4.211			

مما يُشير إلى أن ثقافة إدارة المخاطر الرقمية، ($p=0.920$) لا توجد فروق ذات دلالة إحصائية. باتت سمةً مؤسسية راسخة لا ترتبط بالخبرة الفردية.

ملخص نتائج اختبار الفرضيات 4.3.5

جدول (4-10): ملخص نتائج اختبار الفرضيات

النتيجة	الدلالة الإحصائية	قيمة الارتباط	الفرضية
مقبولة ✓	(دالة) $p=0.001$	$r=0.632$	الفرضية الرئيسية
مرفوضة ✗	(غير دالة) $p=0.074$	$r=0.363$	الأمن السيبراني: H1
مقبولة ✓	(دالة) $p=0.003$	$r=0.570$	الامتثال التشريعي: H2
مقبولة ✓	(دالة) $p=0.002$	$r=0.592$	استمرارية الأعمال: H3
مرفوضة ✗	(غير دالة) $p=0.920$	$F=0.084$	فروق الخبرة: H4

مناقشة النتائج في ضوء الأدبيات السابقة

الفرضية الرئيسية

، ($r=0.632$) أثبتت الدراسة وجود علاقة ارتباطية موجبة ودالة بين إدارة المخاطر الرقمية والاستدامة التي أكدت أن الجهات الناشطة في إدارة (Zeriouh 2024) وهو ما يتقاطع مع نتائج، ($p=0.001$) الذي ربط كفاءة إدارة (Ferrari 2023) مخاطرها تُحقق أداءً تشغيلياً أفضل، ويتسق مع استنتاج المخاطر بمستوى استدامة المؤسسات.

دلالة عملية تستحق التوقف عندها؛ فتفسير 39.9% من ($R^2=0.399$) وتحمل قيمة معامل التحديد التباين في الاستدامة بمتغير واحد فقط هو إدارة المخاطر الرقمية يُعدّ نسبة معتبرة في العلوم الإدارية والاجتماعية، حيث تتأثر الظواهر التنظيمية عادة بعوامل متعددة ومتشابكة. وهذا يعني أن ما يقارب من التباين المتبقي في مستوى الاستدامة تُفسّره عوامل أخرى لم تتناولها هذه الدراسة، كحجم 60% الميزانية المخصصة للمشروع، أو مستوى الدعم القيادي، أو طبيعة الخدمة المقدمة ذاتها. وهذا لا يُضعف من قيمة النتيجة بل يفتح الباب أمام دراسات مستقبلية تستكشف هذه العوامل الإضافية بصورة تكاملية.

(H1) فرضية الأمن السيبراني

ويُعزى ذلك إلى قراءتين. ($p=0.074$) مفاجئة بعدم بلوغها الدلالة الإحصائية H1 جاءت نتيجة إحصائية تتعلق بمحدودية العينة، وموضوعية مفادها أن الأمن السيبراني بات سمةً موحدة في الجهات مما يُقلّص التباين اللازم لإظهار الارتباط. ويُوصى بإعادة الاختبار في ECC الحكومية بفعل إلزامية عينات أوسع.

ومن زاوية تحليلية أعمق، يمكن القول إن هذه النتيجة، رغم عدم دلالتها الإحصائية، لا تعني بالضرورة أن الأمن السيبراني غير مهم لاستدامة المشاريع، بل قد تعني أنه أصبح شرطاً أساسياً ضمناً بين الجهات؛ فحين (Differentiating Factor) لا عاملاً تفاضلياً (Baseline Requirement) يمتلك جميع أفراد العينة تقريباً مستوى مرتفعاً من ممارسات الأمن السيبراني، يصعب إحصائياً أن يُفسّر هذا المتغير تبايناً في الاستدامة لأن التباين في المتغير نفسه محدود أصلاً. وهذا يختلف جوهرياً عن الامتثال التشريعي واستمرارية الأعمال، اللذين أظهرتا تبايناً أوسع في استجابات المشاركين، مما سمح لهما بإظهار علاقة دالة إحصائية مع الاستدامة.

(H2) فرضية الامتثال التشريعي

مما يُثبت أن، ($r=0.570$ ، $p=0.003$) برز الامتثال التشريعي أحد أبرز محركي الاستدامة المنظومة التشريعية الرقمية الوطنية لا تقتصر على الإلزام التنظيمي بل تُسهم فعلياً في تعزيز ديمومة المشاريع التقنية الحكومية.

وتحمل هذه النتيجة رسالة ضمنية مهمة لصانعي السياسات؛ فحين تكون التشريعات الرقمية الوطنية مصممة بعناية ومرتبطة عضوياً بواقع تشغيل المشاريع لا مجرد إجراءات شكلية، فإنها تتحول من عبء تنظيمي إلى أداة حماية فعلية تُسهم في استدامة المشروع ذاته. وهذا ما يُفسر أيضاً السبب وراء تصدر لأعلى متوسط في الدراسة كلها (4.52)؛ إذ يبدو أن العاملين في NDMO عبارة الالتزام بسياسات الميدان لا ينظرون لهذه السياسات بوصفها قيداً خارجياً بل جزءاً من منظومة الحماية الذاتية لمشاريعهم.

(H3) فرضية استمرارية الأعمال

وهو ما ينسجم مع ، ($r=0.592$ ، $p=0.002$) جاءت استمرارية الأعمال الأقوى ارتباطاً بالاستدامة ويتجلى أثر هذا البُعد بوضوح في التفاوت الملحوظ في . (ISO 2018) مبدأ المرونة التشغيلية في إجابات عبارة الاستمرارية التشغيلية (انحراف 0.93) التي كشفت أن الانقطاع التشغيلي لا يزال واقعاً في بعض الجهات.

وتُقدم هذه النتيجة تفسيراً مقنعاً لسبب كون استمرارية الأعمال أقوى الأبعاد الثلاثة ارتباطاً بالاستدامة تحديداً: فبينما يُمكن للأمن السيبراني والامتثال التشريعي أن يعملوا بصورة وقائية في الخلفية دون أن يكون تأثيرهما المباشر ملموساً يومياً للمستفيد، فإن استمرارية الأعمال هي البُعد الوحيد الذي يظهر أثره بصورة مباشرة وفورية في تجربة المستخدم النهائي للخدمة الحكومية الرقمية؛ فانقطاع الخدمة، حتى لو كان قصيراً، يُترجم فوراً إلى تجربة سلبية ملموسة، بعكس ثغرة أمنية لم تُستغل بعد أو تأخر بسيط في تحديث سياسة امتثال. وهذا الارتباط المباشر بتجربة المستفيد هو ما يمنح استمرارية الأعمال ثقلها الأكبر في تحديد مستوى الاستدامة المُدرَكة للمشروع.

(H4) فرضية الفروق وفق الخبرة

وهي نتيجة إيجابية تعكس ترسخ ثقافة إدارة، ($p=0.920$) غياب فروق دالة ANOVA أكدت نتائج المخاطر الرقمية كسمة مؤسسية عامة تتجاوز الفوارق الفردية، مما يُشير إلى نجاح مسيرة التحول الرقمي في تأسيس بيئة مؤسسية داعمة.

وتستحق هذه النتيجة تأملاً إضافياً حين نلاحظ أن المجموعة الأقل خبرة (أقل من 5 سنوات) سجّلت أعلى متوسط بين المجموعات الثلاث (4.312)، وإن كان الفرق غير دال إحصائياً. وهذا النمط، وإن لم يبلغ الدلالة، يحمل إشارة جديرة بالمتابعة في دراسات لاحقة بعينات أكبر: فقد يعكس ذلك أن الكوادر الأحدث في سوق العمل نشأت مهنيّاً في بيئة رقمية بالفعل تفترض إدارة المخاطر كجزء أصيل من العمل التقني، بينما اضطرت الكوادر الأقدم إلى اكتساب هذا الوعي تدريجياً عبر مسيرتها المهنية. وإن صحّ هذا التفسير، فإنه يحمل دلالة مطمئنة على مستقبل ثقافة إدارة المخاطر الرقمية في القطاع الحكومي مع تجدد الأجيال الوظيفية.

الاستنتاجات الرئيسية

أولاً: على صعيد العلاقة بين المتغيرين

- ◀ ثبت إحصائياً وجود علاقة ارتباطية موجبة ودالة بين إدارة المخاطر الرقمية والاستدامة
- ◀ % ونموذج انحدار يُفسّر 39.9 (r=0.632).
- ◀ تُعدّ استمرارية الأعمال الأكثر ارتباطاً بالاستدامة، تليها الامتثال التشريعي، في حين لم
- ◀ يبلغ الأمن السيبراني حد الدلالة الإحصائية
- ◀ غياب فروق دالة وفق الخبرة يُشير إلى ترسخ ثقافة إدارة المخاطر كسمة مؤسسية

ثانياً: على صعيد الواقع الميداني

- ◀ تحقق الجهات الحكومية مستويات مرتفعة في ممارسات إدارة المخاطر الرقمية بأبعادها
- ◀ القائمة الممارسات الأعلى تطبيقاً (4.52) NDMO يتصدّر الالتزام بسياسات
- ◀ تُسجّل الاستمرارية التشغيلية أدنى مستوى في الاستدامة مع أعلى تشتت، مما يكشف عن
- ◀ تفاوت واقعي بين الجهات

التوصيات

أولاً: للجهات الحكومية

توصية 1: تعزيز البنية التحتية لاستمرارية الأعمال

◀، تخصيص ميزانيات واضحة لبناء أنظمة النسخ الاحتياطي المشفرة الموزعة جغرافياً

.نظراً لتسجيلها أدنى مستوى في محور الاستمرارية (م=4.04)

المبرر: أظهرت نتائج الدراسة أن استمرارية الأعمال هي البُعد الأقوى ارتباطاً بالاستدامة

.بينما جاءت عبارة النسخ الاحتياطي الموزع جغرافياً في آخر ترتيب عبارات هذا المحور، ($r=0.592$)

وهذا التناقض بين أهمية البُعد وضعف أحد مؤشراتته يجعل الاستثمار فيه أولوية عاجلة ذات عائد مباشر

.على استدامة المشروع

توصية 2: اعتماد جدول زمني منتظم للاختبارات

◀ اعتماد جدول زمني منتظم لتجارب المحاكاة واختبارات التعافي من الكوارث وربطها

.بمؤشرات الأداء المؤسسي

خطوات التنفيذ المقترحة: تحديد دورية ربع سنوية على الأقل لإجراء تجارب المحاكاة، وتوثيق نتائج

كل تجربة في تقرير يُرفع للإدارة العليا، وربط هذه النتائج بمؤشرات الأداء الفردية والمؤسسية بما يضمن

.استمرارية الاهتمام بهذا الجانب لا معالجته بصورة موسمية عابرة

توصية 3: الامتثال التشريعي الاستباقي

في المراحل الأولى لتصميم NDMO و DGA اشتراط تقييم مسبق للتوافق مع تشريعات

المشاريع.

في الجهات الكبرى لمتابعة (Digital Compliance Unit) إنشاء وحدة امتثال رقمي

التحديثات التشريعية.

وأن، ($r=0.570$) المبرر: أثبتت الدراسة أن الامتثال التشريعي ثاني أقوى الأبعاد ارتباطاً بالاستدامة مما يعني أن الجهات، (4.52) NDMO أعلى متوسط في الدراسة كلها كان لعبارة الالتزام بسياسات تدرك أهمية هذا البعد فعلياً؛ وما تحتاجه هو مؤسسة هذا الوعي في هيكل تنظيمي واضح بدلاً من تركه لجهود فردية متفرقة.

توصية 4: الاستثمار في الكوادر البشرية للأمن السيبراني

تعزيز برامج التدريب المستمر للكوادر التقنية على مهارات الأمن السيبراني الحديثة

بصورة أكثر رسوخاً في جميع مراحل دورة حياة تطوير DevSecOps تبني منهجية

البرمجيات.

المبرر: رغم عدم دلالة العلاقة الإحصائية لبُعد الأمن السيبراني في هذه العينة، إلا أن أدنى عبارة في هذا المحور كانت متعلقة تحديداً بكفاءة الكوادر التقنية ($m=4.04$)، مما يشير إلى أن الاستثمار البشري لا يزال يحتاج تعزيزاً حتى مع النضج التقني العام لممارسات الأمن السيبراني.

التوصيات

أولاً: للجهات الحكومية

توصية 1: تعزيز البنية التحتية لاستمرارية الأعمال

تخصيص ميزانيات واضحة لبناء أنظمة النسخ الاحتياطي المشفرة الموزعة جغرافياً ◀

نظراً لتسجيلها أدنى مستوى في محور الاستمرارية (م=4.04)

المبرر: أظهرت نتائج الدراسة أن استمرارية الأعمال هي البُعد الأقوى ارتباطاً بالاستدامة

بينما جاءت عبارة النسخ الاحتياطي الموزع جغرافياً في آخر ترتيب عبارات هذا المحور، ($r=0.592$)

وهذا التناقض بين أهمية البُعد وضعف أحد مؤشراتته يجعل الاستثمار فيه أولوية عاجلة ذات عائد مباشر

على استدامة المشروع

توصية 2: اعتماد جدول زمني منتظم للاختبارات

اعتماد جدول زمني منتظم لتجارب المحاكاة واختبارات التعافي من الكوارث وربطها ◀

بمؤشرات الأداء المؤسسي

خطوات التنفيذ المقترحة: تحديد دورية ربع سنوية على الأقل لإجراء تجارب المحاكاة، وتوثيق نتائج

كل تجربة في تقرير يُرفع للإدارة العليا، وربط هذه النتائج بمؤشرات الأداء الفردية والمؤسسية بما يضمن

استمرارية الاهتمام بهذا الجانب لا معالجته بصورة موسمية عابرة

توصية 3: الامتثال التشريعي الاستباقي

◀ في المراحل الأولى لتصميم NDMO أو DGA اشتراط تقييم مسبق للتوافق مع تشريعات المشاريع.

◀ في الجهات الكبرى لمتابعة (Digital Compliance Unit) إنشاء وحدة امتثال رقمي التحديثات التشريعية.

وأن، ($r=0.570$) المبرر: أثبتت الدراسة أن الامتثال التشريعي ثاني أقوى الأبعاد ارتباطاً بالاستدامة مما يعني أن الجهات، (4.52) NDMO أعلى متوسط في الدراسة كلها كان لعبارة الالتزام بسياسات تدرك أهمية هذا البُعد فعلياً؛ وما تحتاجه هو مؤسسة هذا الوعي في هيكل تنظيمي واضح بدلاً من تركه لجهود فردية متفرقة.

توصية 4: الاستثمار في الكوادر البشرية للأمن السيبراني

◀ تعزيز برامج التدريب المستمر للكوادر التقنية على مهارات الأمن السيبراني الحديثة.

◀ بصورة أكثر رسوخاً في جميع مراحل دورة حياة تطوير DevSecOps تبني منهجية البرمجيات.

المبرر: رغم عدم دلالة العلاقة الإحصائية لُبُعد الأمن السيبراني في هذه العينة، إلا أن أدنى عبارة في هذا المحور كانت متعلقة تحديداً بكفاءة الكوادر التقنية ($m=4.04$)، مما يشير إلى أن الاستثمار البشري لا يزال يحتاج تعزيزاً حتى مع النضج التقني العام لممارسات الأمن السيبراني.

ثانياً: للباحثين والأكاديميين

إجراء دراسات بعينات أكبر (100+ مستجيب) للتحقق من نتائج هذه الدراسة لا سيما ◀

إذ يُرجَّح أن اتساع العينة قد يكشف دلالة إحصائية لم تظهر في هذه الدراسة، $H1$ فرضية

.بسبب محدودية حجم العينة

استكشاف متغيرات وسيطة كحجم الجهة ومستوى النضج الرقمي في العلاقة بين ◀

المتغيرين، بحيث يمكن فهم ما إذا كانت هذه العلاقة تختلف باختلاف حجم الجهة الحكومية أو

.قدمها في مسيرة التحول الرقمي

توظيف المناهج المختلطة (الكمي والنوعي معاً) لتعمق الفهم وتثري التفسير، خصوصاً ◀

في تفسير أسباب التفاوت الملحوظ في عبارة الاستمرارية التشغيلية التي سجلت أعلى انحراف

.معياري في الدراسة

ثانياً: للباحثين والأكاديميين

إجراء دراسات بعينات أكبر (100+ مستجيب) للتحقق من نتائج هذه الدراسة لا سيما ◀

إذ يُرجَّح أن اتساع العينة قد يكشف دلالة إحصائية لم تظهر في هذه الدراسة، $H1$ فرضية

بسبب محدودية حجم العينة.

استكشاف متغيرات وسيطة كحجم الجهة ومستوى النضج الرقمي في العلاقة بين ◀

المتغيرين، بحيث يمكن فهم ما إذا كانت هذه العلاقة تختلف باختلاف حجم الجهة الحكومية أو

قدمها في مسيرة التحول الرقمي.

توظيف المناهج المختلطة (الكمي والنوعي معاً) لتعمق الفهم وتثري التفسير، خصوصاً ◀

في تفسير أسباب التفاوت الملحوظ في عبارة الاستمرارية التشغيلية التي سجلت أعلى انحراف

معياري في الدراسة.

محدودية الدراسة وآفاق البحث المستقبلي

محدودية الدراسة

كأي دراسة علمية، لا تخلو هذه الدراسة من محدودية ينبغي الإقرار بها بصراحة عند تفسير نتائجها وتعميمها:

◀ محدودية حجم العينة (25 مستجيباً): وهي القيد الأكثر تأثيراً على قوة النتائج
مستوى الدلالة ($H1$) الإحصائية، وقد ظهر أثرها جلياً في عدم بلوغ فرضية الأمن السيبراني الإحصائية رغم اتجاهها الموجب. وكلما صغر حجم العينة، ازدادت الحاجة إلى فروق كبيرة نسبياً بين المتغيرات لتظهر دالة إحصائية، وهو ما لم يتوفر بالكامل في محور الأمن السيبراني. نظراً لتجانس استجابات المشاركين فيه.

◀ إذ تعتمد الاستبانة على تقييم (Self-Report) الاعتماد على أداة التقرير الذاتي
(Social) المستجيبين الشخصي لممارسات جهاتهم، وهو تقييم قد يتأثر بالتحيز الإيجابي، الذي يدفع المستجيب أحياناً لتقديم صورة أفضل من الواقع الفعلي (Desirability Bias)، خصوصاً في القضايا المرتبطة بتقييم أداء الجهة التي يعمل بها.

◀ محدودية التغطية الجغرافية والقطاعية: فرغم أن العينة شملت تنوعاً في أنواع الجهات الحكومية (وزارات وهيئات وقطاعات إمارية)، إلا أن حجمها الصغير لا يسمح بتعميم دقيق على مستوى كل قطاع فرعي بعينه، أو على مستوى المناطق الجغرافية المختلفة في المملكة.

◀ إذ تقيس الدراسة الواقع في لحظة (Cross-Sectional) الإطار الزمني المقطعي
زمنية محددة من عام 2026م، ولا تسمح طبيعتها المقطعية بتتبع التغير في مستوى إدارة

المخاطر الرقمية أو استدامة المشاريع عبر الزمن، وهو ما يتطلب تصميماً طويلاً
لا يتوفر في هذه الدراسة (Longitudinal)

آفاق البحث المستقبلي

انطلاقاً من محدودية هذه الدراسة ونتائجها، تقترح الباحثة عدداً من المسارات البحثية المستقبلية
الواعدة:

- دراسة مقارنة بين القطاعين الحكومي والخاص في مستوى إدارة المخاطر الرقمية وأثرها
على الاستدامة، لاستكشاف ما إذا كانت طبيعة القطاع (حكومي مقابل خاص) تُشكّل متغيراً
وسيطاً مؤثراً في قوة هذه العلاقة.
- دراسة طويلة تتابع مجموعة من المشاريع التقنية الحكومية عيناها عبر عدة سنوات، بما
يسمح برصد التغير الفعلي في مستوى إدارة المخاطر واستدامة المشروع بمرور الوقت، بدلاً من
الاكتفاء بلقطة زمنية واحدة كما في هذه الدراسة.
- استكشاف دور الذكاء الاصطناعي وتقنيات التعلم الآلي في تطوير منظومة إدارة
المخاطر الرقمية الحكومية، خصوصاً في مجال الكشف المبكر عن التهديدات السيبرانية والتنبؤ
باحتمالية تعثر المشاريع قبل وقوعه فعلياً.
- مقارنة نتائج هذه الدراسة مع دول مجلس التعاون الخليجي الأخرى لاستكشاف أوجه
التشابه والاختلاف في تأثير إدارة المخاطر الرقمية على استدامة المشاريع الحكومية، نظراً
للتقارب النسبي في السياقات التنظيمية والتشريعية بين هذه الدول.

◀ لهذه الدراسة ذاتها بعد فترة زمنية مناسبة (Replication Study) إجراء دراسة تكرارية
(كثلاث إلى خمس سنوات)، لقياس مدى تطور مستوى نضج إدارة المخاطر الرقمية في الجهات
الحكومية السعودية مع مرور الوقت وتقدم مسيرة التحول الرقمي.

4.8 خاتمة

بدأت هذه الرحلة البحثية بسؤال يبدو بسيطاً: هل تؤثر إدارة المخاطر الرقمية فعلاً على استدامة المشاريع التقنية الحكومية؟ بعد كل هذا التحليل، الإجابة لم تعد افتراضاً بل حقيقة مدعومة بالأرقام: نعم، وبأثر لا يُستهان به.

لكن ما استوقف الباحثة أكثر من وجود العلاقة نفسها هو تفاوت قوتها بين الأبعاد الثلاثة. استمرارية الأعمال والامتثال التشريعي ظهرا كمحركين حقيقيين للاستدامة، بينما تراجع دور الأمن السيبراني الإحصائي رغم أهميته الظاهرة. هذا التفاوت رسالة عملية لصانع القرار: الاستثمار في الأمن السيبراني وحده لا يكفي؛ المرونة التشغيلية والامتثال الاستباقي يستحقان الاهتمام نفسه، إن لم يكن أكثر.

في النهاية، مشاريع رؤية 2030 لن يُحكم على نجاحها بلحظة الإطلاق، بل بقدرتها على الاستمرار سنوات بعد ذلك. وإدارة المخاطر الرقمية، كما أثبتت هذه الدراسة، ليست عبئاً إدارياً إضافياً، بل هي أقرب إلى بوليصة تأمين حقيقية على مستقبل هذه المشاريع.

المراجع

المراجع الأجنبية

Ferrari, F. (2023). Digitalization and Sustainability: How Digital Transformation Affects Organizational Resilience. Journal of Digital Business, 12(3), 45–67.

ISO. (2018). ISO 31000:2018 — Risk Management Guidelines. International Organization for Standardization. Geneva, Switzerland.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology. U.S. Department of Commerce.

PMI. (2021). A Guide to the Project Management Body of Knowledge (PMBOK Guide) — 7th Edition. Project Management Institute. Pennsylvania, USA.

Zerrouh, H. (2024). Risk Management in Government Digital Transformation Projects: A Systematic Review. International Journal of Public Administration and Digital Governance, 8(1), 112–134.

الوثائق والتشريعات الوطنية

- ◀ ECC- الهيئة الوطنية للأمن السيبراني (2018). الضوابط الأساسية للأمن السيبراني المملكة العربية السعودية. (2018:1).
- ◀ إطار حوكمة التقنية والبيانات في الجهات الحكومية. (DGA) هيئة الحكومة الرقمية المملكة العربية السعودية.
- ◀ سياسات حوكمة وحماية البيانات الوطنية. (NDMO) مكتب إدارة البيانات الوطنية المملكة العربية السعودية.

الملاحق

الملحق (1):

الاستبانة

أثر إدارة المخاطر الرقمية على استدامة المشاريع التقنية في القطاع الحكومي

،عزيزي المشارك / عزيزتي المشاركة

،السلام عليكم ورحمة الله وبركاته

تقوم الباحثة بإجراء دراسة علمية لنيل درجة الماجستير بعنوان: (أثر إدارة المخاطر الرقمية على استدامة المشاريع التقنية في القطاع الحكومي السعودي). تهدف هذه الدراسة إلى استكشاف واقع ممارسات إدارة المخاطر الرقمية ودورها في تعزيز استدامة المشاريع التقنية الحكومية بما يتوافق مع مستهدفات رؤية المملكة 2030

الاعتبارات الأخلاقية والسرية

- ▶ الطوعية: شاركتكم طوعية بالكامل، ولكم الحق في الانسحاب في أي وقت
- ▶ السرية التامة: كافة الإجابات ستُعامل بسرية مطلقة ولن تُستخدم إلا لأغراض البحث العلمي.
- ▶ حجب الهوية: لا يتطلب الاستبيان ذكر الاسم أو البريد الإلكتروني أو أي تفاصيل تقنية
- حساسية

القسم الأول: البيانات العامة والديموغرافية

السؤال (1): طبيعة الجهة الحكومية

- ◀ وزارة
- ◀ هيئة عامة / مؤسسة حكومية
- ◀ قطاع إماري / قطاع بلدي وحكومة محلية

السؤال (2): المسمى الوظيفي العام

- ◀ مدير
- ◀ مدير إدارة / رئيس قسم
- ◀ مهندس أنظمة

السؤال (3): عدد سنوات الخبرة في المجال التقني / الإداري

- ◀ أقل من 5 سنوات
- ◀ من 5 إلى 10 سنوات
- ◀ أكثر من 10 سنوات

القسم الثاني: محاور الدراسة

خيارات الإجابة لجميع العبارات: [موافق بشدة — موافق — محايد — غير موافق — غير موافق بشدة]

المحور الأول: إدارة مخاطر الأمن السيبراني

1. تحرص الجهة على دمج متطلبات الأمن السيبراني كجزء أساسي طوال دورة حياة بناء (DevSecOps) وتطوير الأنظمة الرقمية.
2. توجد ممارسات دورية ومنتظمة لفحص الثغرات البرمجية وحماية قنوات نقل البيانات في المنصات الحكومية.
3. يساهم تطبيق الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن في تقليل حوادث شلل الخدمات الرقمية (ECC) السيبراني.
4. تمتلك الكوادر التقنية في الجهة وعياً كافياً بالمهارات السيبرانية اللازمة لإدارة التهديدات الرقمية المستجدة.

المحور الثاني: إدارة مخاطر الامتثال التشريعي

مواءمة المشاريع التقنية مع أطر (RFPs) تشترط الجهة في كراسات الشروط والمواصفات (DGA) وتشريعات هيئة الحكومة الرقمية.

6. يلتزم قطاع تقنية المعلومات في الجهة بسياسات حوكمة وحماية البيانات الوطنية

الصادرة⁶ (NDMO) عن مكتب إدارة البيانات الوطنية

يساعد الالتزام بالتشريعات الرقمية المسبقة في تجنب المشاريع التقنية خطر التوقف أو 7. التعديل الجذري المكلف بعد إطلاقها.

توجد آلية واضحة ومستمرة في الجهة لمتابعة وتحديث السياسات والأنظمة التقنية بما 8. يتوافق مع التوجهات السيادية للمملكة.

المحور الثالث: إدارة مخاطر استمرارية الأعمال

9. تمتلك الجهة خططاً إجرائية معتمدة وجاهزة للتعافي من الكوارث التقنية والأعطال (Disaster Recovery) الجسيمة.
10. تقوم الجهة بإجراء تجارب محاكاة وفروض دورية لاختبار مدى مرونة الأنظمة والمنصات الحكومية في مواجهة الاختراقات المفاجئة.
11. تعتمد الجهة على أنظمة نسخ احتياطي مشفرة وموزعة جغرافياً على سحابات حكومية معتمدة لضمان عدم فقدان البيانات.
12. تتوفر خطط بديلة لتفويض الصلاحيات وتوزيع المهام التقنية بوضوح بين فرق العمل أثناء الأزمات الرقمية الطارئة.

المحور الرابع: استدامة المشاريع التقنية الحكومية (المتغير التابع)

13. تتجسّد المشاريع التقنية في الجهة في تقديم خدماتها الرقمية للمستخدمين على مدار الساعة دون انقطاع تشغيلي غير مخطط له.
14. تساهم آليات الحوكمة الرقمية الحالية في تحقيق الكفاءة المالية وضبط الإنفاق.
15. تمتلك المنصات التقنية بالجهة مرونة كافية تتيح لها التوسع والربط الآمن والاندماج مع الأنظمة الوطنية الأخرى كالنفاذ الوطني الموحد.
16. يعكس النضج الإداري في التعامل مع المخاطر الرقمية المفهوم الحقيقي لديمومة المشاريع التقنية بما يتوافق مع رؤية المملكة 2030.

شاكرة ومقدرة لكم وقتكم ودعمكم للمسيرة البحثية الوطنية

الباحثة: ثناء إسحاق حلواني | إشراف: د. الفیصل عبد الحمید

