

جامعة ميد أوشن



كلية الإدارة

تخصص إدارة مخاطر

أثر تطبيق إدارة المخاطر السيبرانية على استدامة مشاريع التحول

الرقمي: دراسة تطبيقية على شركات تقنية تقدم خدمات سحابية

بمنطقة الرياض في المملكة العربية السعودية

إعداد الطالب/

بندر محمد البقي

رقم الطالب الأكاديمي/

251000096

إشراف/

د. الفیصل عبد الحمید محمد حسن

د. فايز جراد

1447-2025



إِهْدَاء

إلى أولئك الذين لم يخذلوني يوماً، إلى من آمنوا بي في اللحظات التي
شككت فيها بنفسي، إلى عائلتي التي كانت حصني المنيع في وجه كل صعبٍ
واجهته، لكم كل كلمات الامتنان لا تفي بحققكم، فأنتم من جعلتم الطريق ممكناً،
والغاية أقرب مما تخيلت.

إلى والدَيَّ الحبيبين، أنتما من وضع أساس هذا النجاح، بجهدكما
وتضحيتكما وسهركما، أضاء الله دربي ببركتكما، فأنجزت ما حلمت به بفضل
توجيهكما وصبركما ودعائكما المستمر.

إلى أصدقائي وزملائي الذين شاركوني الطريق، إلى من خففوا عني ضغوط
الدراسة بابتسامة صادقة وكلمة مشجعة،

أهديكم جزءاً من هذا النجاح، فأنتم شركاء في كل خطوة أنجزتها.

شكر ونفقات

أحمد الله عز وجل الذي وفقني في إتمام هذا البحث العلمي،

والذي ألهمني الصحة والعافية والعزيمة.

فالحمد لله حمداً كثيراً

أتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور/

د. فايز علي جراد

د. الفيصل عبد الحميد محمد حسن

على كل ما قدماه لنا من توجيهات ومعلومات قيمة ساهمت في إثراء موضوع دراستنا في جوانبها
المختلفة.

والشكر والتقدير موصول إلى إدارة جامعة ميد أوشن ممثلة بالكادر الأكاديمي والإداري، لما
قدموه من تسهيلات وتشجيع وتوفير الخدمات المطلوبة.

كما أتقدم بالشكر الجزيل لكل من لم يسعني الحظ بذكر أسمائهم راجياً من المولي عز وجل أن
تكون هذه الدراسة نافذة لدراسات أخرى .

المستخلص

هدفت هذه الدراسة إلى تحليل أثر إدارة المخاطر السيبرانية بأبعادها الثلاثة (السياسات والإجراءات الأمنية، تقييم المخاطر السيبرانية، الضوابط الأمنية والاستجابة للحوادث) على استدامة مشاريع التحول الرقمي في الشركات التقنية العاملة بمنطقة الرياض، ولتحقيق هذا الهدف، استخدمت الدراسة المنهج الوصفي التحليلي، وتم تطبيق الاستبانة باعتبارها أداة رئيسة لجمع البيانات، وشملت عينة الدراسة (200) من العاملين في المؤسسات التقنية، وتم تحليل البيانات باستخدام برنامج التحليل الإحصائي SPSS

وأظهرت النتائج الوصفية ارتفاع مستوى إدارة المخاطر السيبرانية لدى المؤسسات المشمولة بالدراسة، كما بيّنت النتائج الاستدلالية وجود أثر دالّ إحصائيًا لأبعاد إدارة المخاطر السيبرانية على استدامة مشاريع التحول الرقمي، وقد تبين أن بُعد الضوابط الأمنية والاستجابة للحوادث هو الأكثر تأثيرًا، يليه بعد السياسات والإجراءات الأمنية، ثم تقييم المخاطر السيبرانية. ك

وبناءً على ذلك، توصي الدراسة بضرورة تعزيز السياسات الأمنية، وتبني أدوات تقييم متقدمة للمخاطر، وتطوير قدرات الاستجابة للحوادث، إضافة إلى دمج الأمن السيبراني في منظومة إدارة مشاريع التحول الرقمي لضمان استدامتها ونموها في البيئة الرقمية المتسارعة.

الكلمات المفتاحية: الأمن السيبراني، إدارة المخاطر السيبرانية، التحول الرقمي، استدامة المشاريع،

الخدمات السحابية.

قائمة المحتويات

أ.....	بسم الله الرحمن الرحيم
ب.....	الإهداء
ج.....	الشكر والتقدير
د.....	المستخلص
ه.....	قائمة المحتويات
ط.....	قائمة الجداول
1.....	الفصل الأول: الإطار العام للدراسة
1.....	1.1 المقدمة
3.....	2.1 مشكلة الدراسة
4.....	3.1 أهمية الدراسة:
5.....	4.1 أهداف الدراسة:
6.....	الأهداف الفرعية المتفرعة عن الهدف الرئيس
6.....	5.1 تساؤلات الدراسة
7.....	6.1 فروض الدراسة:
8.....	7.1 الدراسات السابقة:
14.....	8.1 الفجوة البحثية:
15.....	9.1 المنطلقات النظرية للدراسة:
19.....	10.1 المنهجية وطرق البحث:

11.1	مصادر جمع البيانات	19
12.1	الأساليب الإحصائية المستخدمة	19
13.1	حدود الدراسة:	20
	الفصل الثاني: الإطار النظري	21
	المبحث الأول: المخاطر السيبرانية	21
1.1.2	المقدمة	21
2.1.2	مفهوم إدارة المخاطر السيبرانية	23
3.1.2	أهمية إدارة المخاطر السيبرانية	24
4.1.2	أهداف إدارة المخاطر السيبرانية (صياغة نظرية أكاديمية)	25
5.1.2	أبعاد إدارة المخاطر السيبرانية	27
	المبحث الثاني: استدامة مشاريع التحول الرقمي	30
1.2.2	تمهيد المبحث	30
2.2.2	مفهوم استدامة مشاريع التحول الرقمي	30
3.2.2	أهمية استدامة مشاريع التحول الرقمي	31
4.2.2	أبعاد استدامة مشاريع التحول الرقمي	33
5.2.2	التحديات التي تواجه استدامة مشاريع التحول الرقمي	35
	الفصل الثالث: منهجية الدراسة	37
1.3	المقدمة	37
2.3	منهج الدراسة	37
3.3	مجتمع الدراسة	37

38	4.3 عينة الدراسة.....
38	5.3 أداة الدراسة.....
40	6.3 صدق الأداة.....
41	7.3 مصفوفة الارتباط بين أبعاد المتغير المستقل (نموذج صوري قبل التحليل الفعلي).....
41	8.3 ثبات الأداة.....
43	9.3 الأساليب الإحصائية المستخدمة.....
45	الفصل الرابع: تحليل البيانات ومناقشة النتائج.....
45	1.4 مقدمة.....
45	2.4 تحليل الخصائص الديموغرافية لعينة الدراسة.....
46	3.4 التحليل الوصفي للمتغير المستقل: إدارة المخاطر السيبرانية.....
50	4.4 التحليل الوصفي للمتغير التابع: استدامة مشاريع التحول الرقمي.....
52	5.4 اختبار فرضيات الدراسة.....
58	الفصل الخامس الاستنتاجات والتوصيات.....
58	1.5 مقدمة الفصل.....
58	2.5 مناقشة النتائج الوصفية.....
61	3.5 توصيات الدراسة.....
63	Abstract.....
64	قائمة المراجع.....
64	المراجع باللغة العربية.....
67	المراجع باللغة الإنجليزية.....

70 الملاحق

71 استمارة استبيان

قائمة الجداول

رقم الجدول	اسم الجدول	رقم الصفحة
1.	الجدول (1) مصفوفة الارتباط بين أبعاد المتغير المستقل (نموذج صوري قبل التحليل الفعلي)	40
2.	جدول (2) معاملات الثبات كرونباخ ألفا لأداة الدراسة بعدد الفقرات	41
3.	جدول (3) الخصائص الديموغرافية لعينة الدراسة (ن = 200)	44
4.	جدول (4) المتوسطات الحسابية والانحرافات المعيارية لبعدها السياسات والإجراءات الأمنية (ن=200)	46
5.	جدول (5) المتوسطات الحسابية والانحرافات المعيارية لبعدها تقييم المخاطر السيبرانية	47
6.	جدول (6) المتوسطات الحسابية والانحرافات المعيارية لبعدها الضوابط الأمنية والاستجابة للحوادث	48
7.	جدول (7) المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع (ن=200)	49
8.	جدول (8) نتائج تحليل الانحدار المتعدد لأثر أبعاد إدارة المخاطر السيبرانية على استدامة مشاريع التحول الرقمي	52
9.	جدول (9) تحليل الانحدار الخطي البسيط لقياس أثر السياسات والإجراءات الأمنية على استدامة مشاريع التحول الرقمي	53
10.	جدول (10) تحليل الانحدار الخطي البسيط لقياس أثر تقييم المخاطر السيبرانية على استدامة مشاريع التحول الرقمي	55

رقم الصفحة	اسم الجدول	رقم الجدول
56	جدول (11) تحليل الانحدار الخطي البسيط لقياس أثر الضوابط الأمنية والاستجابة للحوادث على استدامة مشاريع التحول الرقمي	11.

الفصل الأول: الإطار العام للدراسة

1.1 المقدمة

يشهد العالم المعاصر تحولات رقمية متسارعة أحدثت تغييرًا جذريًا في طبيعة الأعمال، وأساليب تقديم الخدمات، وهياكل الأسواق، فقد أصبح التحول الرقمي مسارًا استراتيجيًا تسعى إليه معظم المؤسسات بهدف تحسين الكفاءة التشغيلية وتعزيز القدرة التنافسية، في ظل بيئة عالمية تعتمد بشكل غير مسبوق على التقنيات الذكية والبنية التحتية الرقمية المتقدمة. (Al-Janabi et al., 2024)

وفي إطار هذا التوسع الرقمي العالمي، برزت الحوسبة السحابية كإحدى الركائز الأساس لعمليات التطوير المؤسسي، لما توفره من مزايا تتعلق بتقليل التكاليف، وتعزيز المرونة التشغيلية، ورفع القدرة على الابتكار. وقد أسهم انتشار المنصات السحابية في إعادة تشكيل البنى المعلوماتية داخل المؤسسات، مما أدى إلى زيادة الاعتماد على البيانات والأنظمة الرقمية في ممارسة الأنشطة اليومية، وتشير الأدبيات إلى أن الخدمات السحابية أصبحت المحرك الرئيس للتحول الرقمي في العديد من القطاعات، خاصة في المؤسسات التقنية التي تبني نماذج أعمالها على الاعتمادية العالية وتوافرية الخدمات. (Alshehhi et al., 2024)

وفي الوقت ذاته، أدى هذا التوسع في البنى الرقمية إلى بروز الحاجة المتزايدة لإدارة فعّالة للمخاطر المعلوماتية، خصوصًا في ظل تنامي التهديدات السيبرانية عالميًا، فقد أصبحت الهجمات السيبرانية أكثر تطورًا وتعقيدًا، ما يجعل المؤسسات عرضة لتهديدات قد تؤثر على بياناتها، وأنظمتها، واستمرارية عملياتها. وتشير الدراسات الحديثة إلى أن التهديدات السيبرانية لم تعد مقتصرة على الاختراقات التقليدية، بل تشمل تهديدات متعددة الأبعاد يمكن أن تؤثر على البنية التحتية الرقمية بأكملها، ما يستدعي تعزيز جهود إدارة المخاطر السيبرانية على نحو متكامل. (Araujo et al., 2024)

وتبرز إدارة المخاطر السيبرانية بوصفها أحد أهم المكونات التي يجب أن ترافق التحول الرقمي، حيث توفر إطارًا منهجيًا لتحديد التهديدات المحتملة، وتحليلها، ووضع الضوابط الكفيلة بالحد من تأثيراتها. وقد أكدت الأدبيات أن المؤسسات التي تتبنى إدارة ناضجة للمخاطر تكون أكثر قدرة على بناء منظومات

رقمية مستقرة ومرنة، بما يساهم في ضمان استدامة مشاريعها التقنية على المدى البعيد (Babenko et al., 2022).

و لم يعد الأمن السيبراني مجرد عنصر داعم للأنظمة الرقمية، بل أصبح محوراً رئيساً في بناء مشاريع التحول الرقمي واستمرارها. وتوضح الدراسات أن المؤسسات التي تهمل دمج الأمن السيبراني ضمن خططها الرقمية تكون أكثر عرضة لمخاطر تشغيلية تؤثر في مستوى الجودة والاستمرارية، بينما توفر الإدارة المتكاملة للمخاطر السيبرانية بيئة آمنة وموثوقة تدعم الابتكار والتحول الرقمي المستدام (Saeed et al., 2023).

و تبرز أهمية الأمن السيبراني بشكل أوضح في المؤسسات العربية، خاصة مع تزايد اعتمادها على الأنظمة الذكية والخدمات السحابية. فقد أظهرت الدراسات العربية وجود تفاوت في مستوى الجاهزية الأمنية لدى المؤسسات، إضافة إلى الحاجة إلى تعزيز السياسات والإجراءات الأمنية بما يضمن حماية البنى الرقمية. وقد أشارت بعض الدراسات إلى أن غياب الأطر التنظيمية الواضحة قد يؤثر على كفاءة العمل الرقمي ويعرض المؤسسات لمخاطر أكبر، مما يجعل إدارة المخاطر عنصراً حاسماً في دعم التحول الرقمي في المنطقة (يحياوي، 2024).

ومع تزايد أهمية التحول الرقمي في قطاع الخدمات السحابية تحديداً، تظهر الحاجة الملحة إلى فهم العلاقة بين إدارة المخاطر السيبرانية واستدامة هذه المشاريع، ومن هنا ظهرت فجوة معرفية تتعلق بمدى تأثير إدارة المخاطر السيبرانية على استدامة مشاريع التحول الرقمي داخل المؤسسات التقنية العاملة في الرياض، وهي الفجوة التي تسعى هذه الدراسة إلى معالجتها من خلال تحليل هذه العلاقة بصورة علمية دقيقة.

2.1 مشكلة الدراسة

تمثل مشاريع التحول الرقمي أحد المحركات الرئيسية لنجاح المؤسسات التقنية في المملكة العربية السعودية، ولا سيما تلك التي تقدم خدمات الحوسبة السحابية، ومع تزايد الاعتماد على البنى الرقمية وتنامي حجم البيانات المتداولة، أصبحت هذه المشاريع أكثر عرضة لمخاطر سيبرانية متصاعدة ومعقدة. وتشير الأدبيات الحديثة إلى أن غياب إدارة فعّالة للمخاطر السيبرانية قد يؤدي إلى تعطل الأنظمة الرقمية، وانخفاض مستوى الثقة بالخدمات، وتراجع استدامة المشاريع على المدى الطويل (Saeed et al., 2023). كما أكدت عدة دراسات أن المنظمات التي لا تدمج الأمن السيبراني ضمن منظومتها الاستراتيجية تكون أكثر تعرضًا للفشل في مبادراتها الرقمية (Al-Janabi et al., 2024).

وتُظهر دراسات عربية أن مؤسسات المنطقة ما تزال تعاني تفاوتًا في مستوى نضج إدارة المخاطر السيبرانية، فقد أشارت دراسة الطاهات والرواشدة (2023) إلى وجود قصور في تطبيق الضوابط السيبرانية والإطار الإجرائي داخل بعض المؤسسات، مما ينعكس سلبيًا على جودة العمليات الرقمية. كما أكدت دراسات أخرى أن غياب السياسات الأمنية الموحدة يُعد من أبرز الأسباب التي تحدّ من استدامة المشاريع التقنية، نظرًا لتأثيره المباشر على مستوى الحماية والجاهزية التشغيلية (يحيائي، 2024).

وتتعمّق مشكلة الدراسة في البيئة السعودية التقنية تحديدًا، حيث يشهد قطاع الخدمات السحابية نموًا متسارعًا مدفوعًا برؤية المملكة 2030. هذا النمو يفرض على الشركات التقنية مواجهة تهديدات سيبرانية أكثر تعقيدًا مما كانت عليه في السابق، وهو ما أشار إليه القحطاني وأبو قاعد (2023) بأن المؤسسات الإقليمية تواجه تحديات حقيقية في المواءمة بين التحول الرقمي السريع ومتطلبات الأمن السيبراني المتصاعدة.

وتشير الأدبيات إلى أن ضعف تقييم المخاطر السيبرانية يؤثر مباشرة على قدرة المشاريع الرقمية على الاستمرار بكفاءة، حيث كشفت دراسة أبو نصرة وآخرون (2020) أن غياب آليات تقييم دورية للمخاطر ينعكس على فعالية التخطيط الاستراتيجي، ويزيد من احتمالية تعرّض المؤسسات لحوادث

سيبرانية تؤثر في جودة مشاريعها، كما أوضحت دراسات عالمية أن المؤسسات التقنية التي تهمل تطوير خطط الاستجابة للحوادث تكون أكثر تعرضاً للتوقف المفاجئ وخسائر تشغيلية عالية، الأمر الذي يؤثر على استدامة مشاريع التحول الرقمي. (Eltaeib et al., 2024)

وبناءً على ما سبق، تتحدد مشكلة الدراسة في وجود فجوة واضحة بين متطلبات استدامة مشاريع التحول الرقمي وبين مستوى إدارة المخاطر السيبرانية المطبق فعلياً في المؤسسات التقنية المقدمة للخدمات السحابية في منطقة الرياض، فرغم وجود توجه وطني لتعزيز القدرات الرقمية، تشير الأدلة إلى أن النجاح يتوقف بدرجة كبيرة على قدرة هذه المؤسسات على تطبيق سياسات أمنية فعّالة، وتقييم مستمر للمخاطر، وضوابط قوية للاستجابة للحوادث .

ومن هنا تسعى هذه الدراسة إلى تحليل أثر إدارة المخاطر السيبرانية بأبعادها الثلاثة على استدامة مشاريع التحول الرقمي، ومعالجة هذا القصور المعرفي في البيئة السعودية التقنية.

3.1 أهمية الدراسة:

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي:

الأهمية النظرية:

1. سد فجوة بحثية في الأدبيات العربية حول العلاقة بين إدارة المخاطر السيبرانية واستدامة مشاريع التحول الرقمي، ولا سيما في قطاع الخدمات السحابية.
2. تعزيز المعرفة العلمية من خلال تقديم إطار منهجي يربط بين ثلاثة أبعاد رئيسية لإدارة المخاطر السيبرانية وتأثيرها في نجاح واستدامة مشاريع التحول الرقمي.
3. المساهمة في تطوير النماذج النظرية التي تدرس الاستدامة الرقمية من منظور الأمن السيبراني، وهو مجال حديث ومتنامٍ في البحوث الإدارية والتقنية.

4. إثراء البحوث المتعلقة بالبيئة السعودية في ظل التحول الوطني الرقمي ورؤية 2030، من خلال تقديم دراسة تطبيقية على شركات تقنية تقدّم خدمات سحابية في منطقة الرياض.
5. تزويد الباحثين بقاعدة معرفية يمكن الاستناد إليها لبناء دراسات مستقبلية أكثر عمقاً حول المخاطر السيبرانية وتأثيرها على مختلف جوانب التحول الرقمي.

الأهمية التطبيقية:

- ✓ سد فجوة بحثية في الأدبيات العربية حول العلاقة بين إدارة المخاطر السيبرانية واستدامة مشاريع التحول الرقمي، ولا سيما في قطاع الخدمات السحابية.
- ✓ تعزيز المعرفة العلمية من خلال تقديم إطار منهجي يربط بين ثلاثة أبعاد رئيسية لإدارة المخاطر السيبرانية وتأثيرها في نجاح واستدامة مشاريع التحول الرقمي.
- ✓ المساهمة في تطوير النماذج النظرية التي تدرس الاستدامة الرقمية من منظور الأمن السيبراني، وهو مجال حديث ومتنامٍ في البحوث الإدارية والتقنية.
- ✓ إثراء البحوث المتعلقة بالبيئة السعودية في ظل التحول الوطني الرقمي ورؤية 2030، من خلال تقديم دراسة تطبيقية على شركات تقنية تقدّم خدمات سحابية في منطقة الرياض.
- ✓ تزويد الباحثين بقاعدة معرفية يمكن الاستناد إليها لبناء دراسات مستقبلية أكثر عمقاً حول المخاطر السيبرانية وتأثيرها على مختلف جوانب التحول الرقمي.

4.1 أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل أثر تطبيق إدارة المخاطر السيبرانية بأبعاده الثلاثة (سياسات وإجراءات الأمن السيبراني، تقييم المخاطر السيبرانية، الضوابط الأمنية والاستجابة للحوادث) على استدامة مشاريع التحول الرقمي في شركات التقنية المقدّمة لخدمات سحابية في منطقة الرياض.

الأهداف الفرعية المتفرعة عن الهدف الرئيس

1. قياس مستوى تطبيق إدارة المخاطر السيبرانية بأبعادها الثلاثة في الشركات محل الدراسة.
2. تحديد مستوى استدامة مشاريع التحول الرقمي لدى شركات التقنية المقدمة للخدمات السحابية.
3. تحليل أثر بُعد سياسات وإجراءات الأمن السيبراني على استدامة مشاريع التحول الرقمي.
4. تحليل أثر بُعد تقييم المخاطر السيبرانية على استدامة مشاريع التحول الرقمي.
5. تحليل أثر بُعد الضوابط الأمنية والاستجابة للحوادث على استدامة مشاريع التحول الرقمي.
6. تقديم توصيات لتعزيز دور إدارة المخاطر السيبرانية في دعم استدامة مشاريع التحول الرقمي.

5.1 تساؤلات الدراسة

السؤال الرئيسي الأول: ما أثر تطبيق إدارة المخاطر السيبرانية بأبعاده الثلاثة (سياسات وإجراءات الأمن السيبراني، تقييم المخاطر السيبرانية، الضوابط الأمنية والاستجابة للحوادث) على استدامة مشاريع التحول الرقمي في شركات التقنية المقدمة لخدمات سحابية في منطقة الرياض؟

الأسئلة الفرعية

1. ما مستوى تطبيق إدارة المخاطر السيبرانية بأبعادها الثلاثة في شركات التقنية المقدمة للخدمات السحابية في منطقة الرياض؟
2. ما مستوى استدامة مشاريع التحول الرقمي لدى هذه الشركات؟
3. ما أثر بُعد سياسات وإجراءات الأمن السيبراني على استدامة مشاريع التحول الرقمي؟
4. ما أثر بُعد تقييم المخاطر السيبرانية على استدامة مشاريع التحول الرقمي؟
5. ما أثر بُعد الضوابط الأمنية والاستجابة للحوادث على استدامة مشاريع التحول الرقمي؟

6.1 فروض الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها يمكن للباحث اعتماداً على الإطار النظري المتعلق بالدراسة، واستناداً إلى نتائج الدراسات السابقة تم صياغة الفرضيات التالية:

الفرضية الرئيسة الأول: توجد علاقة ذات دلالة إحصائية بين إدارة المخاطر السيبرانية بأبعادها الثلاثة واستدامة مشاريع التحول الرقمي في الشركات التقنية المقدمة لخدمات الحوسبة السحابية في منطقة الرياض.

وينبثق من هذه الفرضية الفرضيات الفرعية الأربع التالية:

- توجد علاقة ذات دلالة إحصائية بين السياسات والإجراءات الأمنية واستدامة مشاريع التحول الرقمي على شركات تقنية تقدم خدمات سحابية بمنطقة الرياض في المملكة العربية السعودية.
- توجد علاقة ذات دلالة إحصائية بين تقييم المخاطر السيبرانية واستدامة مشاريع التحول الرقمي. على شركات تقنية تقدم خدمات سحابية بمنطقة الرياض في المملكة العربية السعودية
- توجد علاقة ذات دلالة إحصائية بين الضوابط الأمنية والاستجابة للحوادث واستدامة مشاريع التحول الرقمي. على شركات تقنية تقدم خدمات سحابية بمنطقة الرياض في المملكة العربية السعودية

7.1 الدراسات السابقة:

✍ دراسة (Al-Janabi, Jabbar & Syms (2024)

هدفت الدراسة إلى التعرف على أثر دمج إدارة مخاطر الأمن السيبراني بأبعادها (تحديد المخاطر، وتقييمها، وتخفيفها، والمراجعة المستمرة) ضمن دورة حياة مشاريع تكنولوجيا المعلومات على كفاءة وأمان تنفيذ المشروع، واستخدمت الدراسة المنهج الوصفي من خلال تحليل حالة تطبيقية، وتكوّنت العينة من تطبيق إطار CYBITJET على مشروع نظام السجل الصحي الشخصي (PHR) وتوصلت النتائج إلى أن التطبيق المنتظم للإطار عزّز الأمان ورفع مرونة التنفيذ، مما أدى إلى مستوى أمان وجودة تنفيذ أفضل، وأوصت الدراسة بضرورة دمج الإطار ضمن منهجيات إدارة مشاريع تكنولوجيا المعلومات وتوافقه مع معايير ISO/IEC 27001 و COBIT 2019 لضمان أمن وجودة أعلى.

✍ دراسة (Zhu (2024)

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

✍ دراسة (Araujo et al. (2024)

هدفت الدراسة إلى التعرف على أثر دمج مراحل إدارة المخاطر السيبرانية بأبعادها (الاستعداد، والرصد والكشف، والمقاومة، والاستجابة، والتعافي، والتعلم) على كفاءة تنفيذ الاستجابة ومتابعة

الهجمات السيبرانية لدى المؤسسات؛ واستخدمت المنهج النظري المنهجي استنادًا إلى مراجعة أدبية لكُتب ومقالات علمية بين 2015 و2023؛ وتكونت العينة من 62 ورقة علمية تم تحليلها.

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

✍ دراسة (Jabbar et al. (2024

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

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

✍ دراسة (Eltaeib et al. (2024

هدفت الدراسة إلى التعرف على أثر تبني إستراتيجية شاملة لإدارة مخاطر الأمن السيبراني بأبعادها (التخطيط الاستراتيجي، إشراك أصحاب المصلحة، وتمكين الحوكمة العليا) على قدرة المؤسسات في الوقاية من التهديدات السيبرانية والتعامل معها بفعالية في بيئات تقنية متغيرة، وذلك انطلاقًا من الحاجة إلى تجاوز حصر إدارة الأمن في أقسام تكنولوجيا المعلومات فقط، واستخدمت الدراسة المنهج التحليلي النظري من

خلال تصميم إطار استراتيجي شامل يربط بين الأدوار القيادية وممارسات الأمن، وتكوّنت العينة من مراجعة ممارسات مؤسسية نموذجية وتحليل ثغراتها التنظيمية.

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

دراسة (2024) Rekunen et al.

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

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

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

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

هدفت الدراسة إلى التعرف على أثر تطبيق إدارة المخاطر السيبرانية بأبعادها (تحديد المخاطر، تصنيفها، التخفيف الاستباقي، واستخدام التحليلات التنبؤية) على كفاءة تنفيذ مشاريع البناء، وذلك في ضوء التحديات المتكررة التي تواجه هذا القطاع مثل التأخيرات وتجاوز الميزانيات، واستخدمت الدراسة المنهج الوصفي التحليلي، من خلال تحليل بيانات مشاريع بناء متنوعة ومقارنة مستويات الأداء بين المشاريع التي تبنت ممارسات استباقية في إدارة المخاطر السيبرانية وتلك التي لم تطبقها، وتكوّنت العينة من مشروعات بناء مختلفة في بيئات متقاربة، خضعت لقياسات الكفاءة والفعالية.

وتوصلت نتائج الدراسة إلى وجود علاقة إيجابية قوية بين تبني إدارة مخاطر استباقية وارتفاع كفاءة تنفيذ المشروع، إذ أظهرت المشاريع التي اعتمدت هذه الممارسات انخفاضًا ملحوظًا في التأخيرات

والتكاليف الزائدة، وزيادة القدرة على التكيف مع الظروف الطارئة، وأوصت الدراسة بأهمية اعتماد استراتيجيات إدارة المخاطر السيبرانية المبكرة، وتدريب أصحاب المصلحة على أساليب التقييم والتقليل، إضافة إلى دمج الحلول التقنية مثل التحليلات التنبؤية ونماذج المحاكاة لتحسين اتخاذ القرار في إدارة المشاريع.

دراسة (Zhang et al., 2023)

هدفت الدراسة إلى التعرف على واقع الأدبيات المتعلقة بالتحول الرقمي والاستدامة في سياق إدارة المشاريع بأبعاده) التحليل الببليومتري، ورسم الخرائط العلمية Scientometric ، واستعراض اتجاهات البحث وتطوراتها (وذلك خلال الفترة من 2011 إلى 2022. واعتمدت الدراسة المنهج الببليومتري ومنهج رسم الخرائط العلمية لتحليل الإنتاج العلمي بشكل شامل. وتكوّنت عيّنة الدراسة من جميع الدراسات المنشورة في موضوع التحول الرقمي والاستدامة في إدارة المشاريع خلال المدة الزمنية المحددة. وتوصلت نتائج الدراسة إلى تقديم رؤى مهمة لمديري المشاريع حول إعادة تطوير نماذج أعمالهم وتوظيف الاستراتيجيات الرقمية لتعزيز مستويات الاستدامة في مشاريعهم، كما كشفت عن الاتجاهات البحثية الحديثة ومجالات البحث المستقبلية أمام الأكاديميين. وأوصت الدراسة بضرورة توسيع نطاق البحث في مجالات التوجهات الناشئة وتعزيز التكامل بين التحول الرقمي والاستدامة في إدارة المشاريع..

دراسة (Bomark & Westergren, 2024)

هدفت الدراسة إلى التعرف على دمج التحول الرقمي والاستدامة داخل المنظمات بأبعاده المختلفة (تحوّل إدارات تقنية المعلومات نحو مشاريع الاستدامة الرقمية، تطوير ممارسات خلق القيمة المستدامة، واستثمار متطلبات الاستدامة الخارجية في مشاريع تقنية المعلومات) ودراسة أثر ذلك في تحقيق الأهداف الرقمية-الاجتماعية-الاقتصادية للاستدامة. واعتمدت الدراسة المنهج النوعي التحليلي من خلال استكشاف نتائج ومآلات أحد مشاريع الاستدامة الرقمية داخل مؤسسة معاصرة. وتكوّنت عيّنة الدراسة من مشروع استدامة رقمي واحد تم تتبع ممارسات الإدارة فيه، وأولويات الأهداف، وآليات التفاوض بين الأطراف المعنية. وتوصلت نتائج الدراسة إلى أن المنظمات يمكنها الاستفادة من مشاريع تقنية المعلومات الداخلية عبر مواءمتها مع متطلبات الاستدامة الخارجية، من خلال تطوير ممارسات إدارية وممارسات لتحديد أولويات المشروع وممارسات تفاوضية تدعم التقارب بين الرقمنة والاستدامة. كما أبرزت النتائج تعقيد تحقيق هذا التقارب على المستوى التنظيمي، وكشفت التحديات والفرص المرتبطة بتطبيق وتحقيق أهداف الاستدامة الرقمية ذات الطابع الاجتماعي-البيئي-الاقتصادي. وأوصت الدراسة بضرورة تطوير إطار مؤسسي شامل لدعم هذا التقارب وتعزيز قدرات إدارات تقنية المعلومات في قيادة مبادرات الاستدامة الرقمية.

دراسة (Khan, 2024)

هدفت الدراسة إلى التعرف على كيفية توظيف الشركات لاستراتيجيات التحول الرقمي لدمج أهداف الاستدامة، من خلال دراسة أبعاد التوازن بين المنافع المتحققة من الرقمنة والمخاطر المصاحبة لها على الأداء المستدام. واعتمدت الدراسة المنهج المختلط القائم على دراسات حالة متعددة، واستخدام أساليب جمع بيانات نوعية وكمية لتحليل العلاقة بين استراتيجيات التحول الرقمي والنماذج الكامنة للأعمال ومستوى الاستدامة. وتكوّنت عيّنة الدراسة من مجموعة من المؤسسات التي تطبق التحول الرقمي في مراحل مختلفة ضمن مشاريع الاستدامة، بهدف الكشف عن الديناميكيات المؤثرة في الأداء المستدام.

وتتوقع الدراسة رغم كونها في مراحلها الأولية أن تتجه المؤسسات إلى زيادة تبني مبادرات التحول الرقمي استجابة للمتطلبات التنظيمية البيئية، وأن يؤثر ذلك إيجابيًا في صياغة استراتيجيات الاستدامة الرقمية. كما تتوقع أن تسهم نتائجها في تطوير معرفة جديدة حول كيفية تحقيق التوازن الأمثل بين فوائد الرقمنة ومخاطرها، بما يدعم بناء استراتيجيات فعالة للاستدامة الرقمية. وأوصت الدراسة بضرورة تطوير نماذج أعمال قادرة على استيعاب التحول الرقمي دون زيادة الأعباء البيئية مثل استهلاك الطاقة أو النفايات الإلكترونية، وتعزيز السياسات التنظيمية التي تدعم التحول الرقمي المستدام.

8.1 الفجوة البحثية:

اتفقت الدراسات السابقة على أهمية دمج إدارة المخاطر السيبرانية أو التحول الرقمي أو الاستدامة داخل العمليات المؤسسية بوصفها عنصرًا استراتيجيًا يعزز الكفاءة والمرونة التنظيمية. جميع الدراسات التي تناولت الأمن السيبراني، مثل Al Janabi وآخرون و Araujo و Jabbar و Eltaeib و Rekunenکو و Al-Janabi و Alshehhi، أكدت أن الإدارة المتكاملة للمخاطر—سواء عبر أطر حوكمة، ذكاء اصطناعي، مراجعة مستمرة، أو تخطيط استراتيجي—تسهم بشكل مباشر في رفع مستوى الحماية وتقليل الخسائر وتحسين تنفيذ المشاريع. كما توافقت الدراسات التي تناولت التحول الرقمي والاستدامة (Zhang؛ Bomark و Khan & Westergren) على أن الجمع بين الرقمنة والاستدامة أصبح ضرورة، وأن الاستراتيجيات الرقمية تمثل محركًا رئيسًا لتحقيق القيم الاجتماعية والاقتصادية والبيئية وتعزيز قدرة المؤسسات على التكيف مع المتطلبات التنظيمية. كذلك اتفقت جميع الدراسات على ضرورة تطوير أطر شاملة تسهل دمج الأمن أو التحول الرقمي في العمليات المؤسسية، وأوصت بتوسيع التطبيقات المستقبلية وتحديث الأدوات والمنهجيات بما يتلاءم مع التطورات التقنية وتسارع التهديدات الرقمية.

اختلفت الدراسات في زاوية التركيز والمنهجية والمجال التطبيقي. فبعضها ركّز على الأمن السيبراني كموضوع رئيسي (مثل Al Janabi، Araujo، Jabbar، Eltaeib، Rekunenکو، Al-Janabi، Alshehhi) بينما ركزت دراسات أخرى على التحول الرقمي والاستدامة (Zhang؛ Bomark & Khan). كما اختلفت مناهج البحث؛ فهناك دراسات اعتمدت على حالات تطبيقية مثل Al-Janabi و Al Janabi

وAlshehhi، ودراسات اعتمدت على مراجعات أدبية واسعة مثل Araujo وRekunenko، ودراسات استخدمت النماذج النظرية البحتة مثل Zhu، وأخرى اعتمدت المنهج المختلط مثل Khan. كما اختلفت المجالات التطبيقية؛ فبعضها تناول مشاريع تكنولوجيا المعلومات، وأخرى ركزت على القطاعات الحيوية مثل الصحة والبناء، في حين توسعت دراسات الاستدامة الرقمية لتشمل النماذج المؤسسية الكاملة. واختلفت النتائج كذلك، فبعضها ركز على تحسين مرونة المشاريع، وأخرى على رفع التنافسية، وأخرى على تصميم استراتيجيات مستدامة رقمية، ما يعكس تنوعاً في المقاربات البحثية رغم وحدة الموضوع العام..

9.1 المنطلقات النظرية للدراسة:

أولاً: التحول الرقمي ودوره في تطوير المنظمات المعاصرة

يشير التحول الرقمي إلى عملية دمج التقنيات الرقمية في جميع جوانب العمل المؤسسي، بهدف تحسين العمليات التشغيلية، ورفع الكفاءة، وتطوير نماذج الأعمال، وتعزيز الابتكار. وقد أصبح التحول الرقمي محوراً أساسياً في الأدبيات الإدارية نظراً لقدرته على إحداث نقلة نوعية في أداء المؤسسات وقدرتها التنافسية. وتشمل عملية التحول الرقمي تبني تقنيات مثل الذكاء الاصطناعي، وإنترنت الأشياء، وتحليل البيانات الضخمة، والحوسبة السحابية، والبلوك تشين. ومع تطور التهديدات الرقمية وسرعة تغير بيئة الأعمال، بات التحول الرقمي ليس خياراً، بل ضرورة إستراتيجية لضمان الاستمرارية والنمو.

وتشير الدراسات الحديثة إلى أن التحول الرقمي يمثل فرصة لإعادة هندسة العمليات المؤسسية وبناء قدرات تنظيمية أكثر مرونة وقدرة على مواجهة التغيرات المفاجئة. فبحسب Zhang وآخرين (2023)، ساهم التحول الرقمي في تعزيز الاستدامة المؤسسية من خلال تحسين إدارة الموارد وتطوير نماذج أعمال مبتكرة. كما أكدت دراسات مثل Khan (2024) وBomark & Westergren (2024) أن التحول الرقمي بات مرتبطاً بشكل وثيق بالأهداف البيئية والاجتماعية والاقتصادية، وأصبح نقطة التقاء بين التكنولوجيا والاستدامة.

ثانيًا: الاستدامة الرقمية (Digital Sustainability) كاتجاه عالمي

تُعرّف الاستدامة الرقمية بأنها عملية توظيف التقنيات الرقمية لدعم الممارسات المستدامة وتعزيز الأداء البيئي والاجتماعي والاقتصادي للمنظمة. ويتسع مفهوم الاستدامة الرقمية ليشمل استخدام الحلول التقنية في ترشيد الطاقة، وتقليل الهدر، وإدارة الموارد، وتحسين التفاعل مع أصحاب المصلحة، بالإضافة إلى مساهمتها في خفض البصمة الكربونية من خلال تحسين الكفاءة التشغيلية.

وتبرز أهمية الاستدامة الرقمية في سياق ازدياد اللوائح البيئية العالمية والمتطلبات التنظيمية التي تُلزم المؤسسات بالتحول نحو ممارسات أكثر استدامة. وتظهر الأدبيات الحديثة، ومنها (Khan, 2024)، أن المؤسسات تستخدم الرقمنة لتحقيق التوافق التنظيمي، وتحسين الأداء البيئي، وبناء ميزة تنافسية جديدة قائمة على تقديم منتجات وخدمات مسؤولة ومستدامة. كما تشير (Bomark & Westergren, 2024) إلى أن دمج الاستدامة في مشاريع التحول الرقمي يخلق قيمة مضافة من خلال تعزيز الابتكار وتقليل المخاطر ورفع مستوى الثقة مع العملاء والمستفيدين.

ثالثًا: الأمن السيبراني كمتطلب استراتيجي في عصر الرقمنة

مع توسع التحول الرقمي، تعددت التهديدات السيبرانية التي تواجه المؤسسات، بدءًا من الهجمات الإلكترونية الخبيثة، مرورًا بسرقة البيانات، ووصولًا إلى تخريب الأنظمة الحيوية. وهذا ما دفع الأدبيات إلى التأكيد على أن إدارة مخاطر الأمن السيبراني أصبحت جزءًا أساسيًا من إدارة المشاريع، وليست مجرد عنصر تقني تتولاه أقسام تكنولوجيا المعلومات فقط.

وبحسب Al Janabi وآخرين (2024)، فإن دمج إدارة المخاطر السيبرانية في دورة حياة مشاريع تكنولوجيا المعلومات يساهم في تحسين مرونة المشاريع وتعزيز أمنها بشكل كبير. كما أشارت دراسات مثل (abbbar et al., 2024) إلى الدور المحوري للكفاءات الاصطناعية في تطوير استجابات تلقائية للهجمات السيبرانية، والكشف المبكر عن التهديدات، وتحسين قدرة المشاريع على التكيف مع المخاطر الناشئة. بذلك، بات الأمن السيبراني عنصرًا تمكينيًا رئيسيًا لنجاح التحول الرقمي والاستدامة الرقمية.

رابعًا: إدارة مخاطر الأمن السيبراني: المفاهيم والمراحل

تعتبر إدارة مخاطر الأمن السيبراني عملية منهجية تهدف إلى تحديد التهديدات وتحليلها وتقييمها، ثم تطوير استراتيجيات للتخفيف منها أو التعامل معها. وتتضمن هذه العملية مجموعة من المراحل الأساسية مثل:

1. تحديد المخاطر عبر فهم السياق التنظيمي وتحليل مصادر الهجمات المحتملة.
2. تقييم المخاطر من خلال قياس احتمالية حدوث التهديد وتأثيره.
3. التخفيف عبر تطبيق ضوابط تقنية وإدارية تقلل من احتمالية الهجوم أو من تأثيره.
4. الاستجابة والتعافي واستعادة العمليات والأنظمة المتأثرة بسرعة وفعالية.
5. التعلم والمراجعة المستمرة لتطوير منظومة أمنية أكثر صلابة.

وقد رَسَّخت دراسة Araujo وآخرين (2024) أهمية النظر إلى إدارة المخاطر من منظور المرونة السيبرانية، عبر الدمج بين مراحل الاستعداد، والكشف، والمقاومة، والاستجابة، والتعافي، والتعلم، معتبرة أنها تشكل إطارًا متكاملًا لإدارة أمن المؤسسات في مواجهة التهديدات المتزايدة.

خامسًا: دور الذكاء الاصطناعي في دعم إدارة المخاطر وتحسين الأمن السيبراني

يمثل الذكاء الاصطناعي أداة تحويلية في مجال الأمن السيبراني، إذ يتيح قدرات متقدمة في تحليل البيانات، والكشف التلقائي عن التهديدات، وتوقع المخاطر المستقبلية. وقد كشفت دراسة Jabbar وآخرين (2024) عن أن توظيف التحليلات التنبؤية والتعلم الآلي والاستجابة الذاتية للحوادث يرفع من مستوى الأمن في مشاريع تكنولوجيا المعلومات ويقلل من الزمن اللازم للاستجابة للهجمات.

كما أوضحت (Zhu 2024) أن دمج نظرية الألعاب ونظرية التحكم مع خوارزميات الذكاء الاصطناعي يوفر أساسًا علميًا لتصميم أنظمة استجابة آلية قادرة على التكيف مع الظروف المتغيرة والهجمات المتطورة، مما يجعل المؤسسات أكثر قدرة على حماية أصولها الرقمية.

سادسًا: الحوكمة المؤسسية ودورها في دعم الأمن السيبراني والتحول الرقمي

تلعب الحوكمة دورًا أساسيًا في نجاح مبادرات الأمن السيبراني والتحول الرقمي. ففي غياب دعم إداري وقيادي واضح، يصبح تنفيذ الأطر الأمنية والمشاريع الرقمية محدودًا وغير فعال. وقد بينت دراسة Eltaeib وآخرين (2024) أن إشراك مجالس الإدارة والقيادات الاستراتيجية في عملية اتخاذ القرار الأمني يعزز من قدرة المؤسسات على التعامل مع التهديدات السيبرانية، ويقلل من الفجوات التنظيمية التي قد تُستغل للهجوم على الأنظمة.

كما توصل Rekunenko وآخرون (2024) إلى أن إدارة المخاطر الشاملة—بما فيها الأمن السيبراني، والامتثال التنظيمي، والتخطيط المالي، وإدارة الموارد البشرية—تمثل حجر الأساس في الحفاظ على التنافسية وتعزيز المرونة المؤسسية، خصوصًا في بيئة تقنية تتسم بالتغير السريع.

سابعًا: تلاقي التحول الرقمي والأمن السيبراني والاستدامة

تجمع الأدبيات الحديثة على أن التحول الرقمي والاستدامة والأمن السيبراني لم تعد مجالات منفصلة، بل أصبحت مترابطة بشكل وثيق. فنجاح أي مشروع رقمي مرتبط بمدى كفاءته الأمنية، ومدى قدرته على خلق قيمة مستدامة للمؤسسة. ومن هذا المنطلق:

- يؤثر التحول الرقمي في رفع الإنتاجية وتحسين جودة الخدمات.
- بينما تضمن الاستدامة الرقمية استخدام التقنيات بشكل مسؤول بيئيًا واجتماعيًا.
- ويُعد الأمن السيبراني الضامن الأساسي لاستمرارية المشاريع الرقمية ومصداقيتها.

وقد أجمعت الدراسات الحديثة على أن المؤسسات التي تُدمج هذه العناصر الثلاثة بطريقة متوازنة تحقق مستويات أعلى من التنافسية والمرونة وقابلية التكيف مع التحديات المستقبلية.

10.1 المنهجية وطرق البحث:

اعتمدت الدراسة المنهج الوصفي التحليلي لكونه الأنسب لدراسة الظواهر الرقمية المعاصرة التي تتطلب تحليلاً معمقاً للأطر النظرية والنماذج العلمية الحالية، بالإضافة إلى وصف واقع التطبيقات العملية في المؤسسات. ويتيح هذا المنهج استعراض الأدبيات السابقة، واستخلاص المتغيرات الرئيسة، وتحليل العلاقات المحتملة فيما بينها.

كما تم توظيف المنهج النوعي في دراسة الممارسات المؤسسية الخاصة بالتحول الرقمي وإدارة الأمن السيبراني، إضافة إلى استخدام التحليل المقارن لمناقشة الأطر المختلفة وتحديد نقاط القوة والضعف في كل منها. وبما أن جزءاً من البحث يستند إلى مراجعة الأدبيات، فقد تم أيضاً تضمين المنهج الوثائقي من خلال جمع وتحليل مصادر علمية منشورة في قواعد البيانات العالمية.

11.1 مصادر جمع البيانات

- المصادر الثانوية: وتشمل البيانات والمعلومات الموجودة في الكتب والمراجع، والرسائل الجامعية وأوراق العمل والمجلات والدوريات والمؤتمرات العلمية وورش العمل، بالإضافة إلى التقارير المنشورة وغير المنشورة التي تناولت الموضوع في مختلف المؤسسات ذات الصلة.
- المصادر الأولية: اعتمدت الدراسة على الاستبانة كأداة رئيسية في جمع البيانات من مصادرها والتي تم تصميمها خصيصاً لهذا الغرض على Google Forms وإرسال رابطها إلى مجتمع البحث.

12.1 الأساليب الإحصائية المستخدمة

تم استخدام الأساليب الإحصائية التالية لتحقيق أهداف الدراسة:

- معامل "ألفا كرونباخ" لقياس ثبات أداة الدراسة ومعامل الارتباط بيرسون لقياس صدق أداة الدراسة والعلاقة بين المتغيرات

- التكرارات والنسب المئوية والمتوسط الحسابي والانحراف المعياري المتعلقة بمتغيرات الدراسة ولجميع الاستجابات على فقرات الاستبيان.
- معامل الانحدار الخطي البسيط لقياس أثر كل بعد من أبعاد المتغير المستقل على المتغير التابع

13.1 حدود الدراسة:

- حدود موضوعية: تقتصر الدراسة على تطبيق إدارة المخاطر السيبرانية بأبعاده (السياسات والإجراءات، تقييم المخاطر، الضوابط الأمنية، الاستجابة للحوادث، والتدريب والتوعية الأمنية) على استدامة مشاريع التحول الرقمي.
- حدود مكانية: تُجرى الدراسة على شركات التقنية المقدّمة لخدمات سحابية في منطقة الرياض في المملكة العربية السعودية.
- حدود زمنية: تم إعداد الدراسة في عام 2025.
- حدود بشرية: تقتصر الدراسة على العاملين في شركات تقنية المقدّمة لخدمات سحابية في منطقة الرياض في المملكة العربية السعودية.

الفصل الثاني: الإطار النظري

المبحث الأول: المخاطر السيبرانية

1.1.2 المقدمة

يشهد العالم تطورًا متسارعًا في تبني التقنيات الرقمية، وازديادًا ملحوظًا في اعتماد المنظمات على الأنظمة السحابية والمنصات الرقمية بهدف تحسين الكفاءة التشغيلية وتحقيق مزايا تنافسية مستدامة. وقد أدى هذا التوجه المتنامي نحو التحول الرقمي إلى إعادة تشكيل بيئات الأعمال، كما غير طبيعة العمليات المؤسسية، وأوجد فرصًا جديدة للابتكار والنمو. ومع ذلك، فإن هذا التوسع الرقمي لم يخلُ من التحديات؛ إذ برزت المخاطر السيبرانية بوصفها أحد أخطر التحديات التي تواجه المنظمات المعاصرة، لما يمكن أن تسببه من خسائر مالية وتشغيلية وسمعية، إضافة إلى تأثيرها المباشر على استمرارية المشاريع الرقمية واستدامتها.

وفي ظل تزايد شدة وتعقيد الهجمات السيبرانية، أصبح الاهتمام بإدارة المخاطر السيبرانية ضرورة ملحة، وليس مجرد خيار تنظيمي. إذ ترتبط استدامة مشاريع التحول الرقمي بقدرة المنظمات على حماية أصولها التقنية، وضمان سلامة البيانات، واستمرارية الخدمات السحابية التي تعتمد عليها قطاعات الأعمال بشكل مباشر. ومن ثم، فإن فهم علاقة إدارة المخاطر السيبرانية باستدامة مشاريع التحول الرقمي يُعد خطوة أساسية لتمكين الشركات — خصوصًا التقنية منها — من تحقيق أهداف التحول الرقمي بكفاءة وأمان.

ويمثل هذا الإطار النظري محاولة علمية لتناول المفاهيم الأساسية المرتبطة بالمتغير المستقل (إدارة المخاطر السيبرانية) والمتغير التابع (استدامة مشاريع التحول الرقمي)، وذلك من خلال استعراض المفهوم، والأهمية، والأهداف، والأبعاد النظرية، إضافة إلى عرض الاتجاهات الحديثة في الأدبيات والدراسات ذات الصلة. ويسعى هذا الإطار إلى بناء أساس معرفي متين يمكن الاعتماد عليه في فهم طبيعة

العلاقة بين إدارة المخاطر السيبرانية واستدامة مشاريع التحول الرقمي، خاصة في منظمات تعتمد على خدمات سحابية وتتعامل مع بيانات تقنية عالية التعقيد والحساسية.

يشهد العالم تطورًا متسارعًا في تبني التقنيات الرقمية، وازديادًا ملحوظًا في اعتماد المنظمات على الأنظمة السحابية والمنصات الرقمية بهدف تحسين الكفاءة التشغيلية وتحقيق مزايا تنافسية مستدامة. وقد أدى هذا التوجه المتنامي نحو التحول الرقمي إلى إعادة تشكيل بيئات الأعمال، كما غير طبيعة العمليات المؤسسية، وأوجد فرصًا جديدة للابتكار والنمو. ومع ذلك، فإن هذا التوسع الرقمي لم يخلُ من التحديات؛ إذ برزت المخاطر السيبرانية بوصفها أحد أخطر التحديات التي تواجه المنظمات المعاصرة، لما يمكن أن تسببه من خسائر مالية وتشغيلية وسمعية، إضافة إلى تأثيرها المباشر على استمرارية المشاريع الرقمية واستدامتها.

وفي ظل تزايد شدة وتعقيد الهجمات السيبرانية، أصبح الاهتمام بإدارة المخاطر السيبرانية ضرورة ملحة، وليس مجرد خيار تنظيمي. إذ ترتبط استدامة مشاريع التحول الرقمي بقدرة المنظمات على حماية أصولها التقنية، وضمان سلامة البيانات، واستمرارية الخدمات السحابية التي تعتمد عليها قطاعات الأعمال بشكل مباشر. ومن ثم، فإن فهم علاقة إدارة المخاطر السيبرانية باستدامة مشاريع التحول الرقمي يُعد خطوة أساسية لتمكين الشركات خصوصًا التقنية منها من تحقيق أهداف التحول الرقمي بكفاءة وأمان.

ويمثل هذا الإطار النظري محاولة علمية لتناول المفاهيم الأساسية المرتبطة بالمتغير المستقل (إدارة المخاطر السيبرانية) والمتغير التابع (استدامة مشاريع التحول الرقمي)، وذلك من خلال استعراض المفهوم، والأهمية، والأهداف، والأبعاد النظرية، إضافة إلى عرض الاتجاهات الحديثة في الأدبيات والدراسات ذات الصلة. ويسعى هذا الإطار إلى بناء أساس معرفي متين يمكن الاعتماد عليه في فهم طبيعة العلاقة بين إدارة المخاطر السيبرانية واستدامة مشاريع التحول الرقمي، خاصة في منظمات تعتمد على خدمات سحابية وتتعامل مع بيانات تقنية عالية التعقيد والحساسية.

2.1.2 مفهوم إدارة المخاطر السيبرانية

تناول عدد كبير من الباحثين مفهوم إدارة المخاطر السيبرانية من زوايا مختلفة، إلا أن معظم هذه التعريفات تلتقي عند فكرة حماية الأصول الرقمية وضمان استمرارية الأعمال في ظل تصاعد التهديدات السيبرانية، فقد عرّف Al-Janabi et al. (2024) إدارة المخاطر السيبرانية بأنها عملية منهجية تهدف إلى تعزيز مرونة الأنظمة الرقمية من خلال تحديد مصادر التهديد، واكتشاف الثغرات المحتملة، وتطوير آليات الاستجابة التي تقلل من أثر الهجمات على مشاريع تكنولوجيا المعلومات. ويظهر هذا التعريف تركيزاً واضحاً على مفهوم "المرونة السيبرانية" باعتبارها جوهرًا لعمليات إدارة المخاطر.

و قدّم Eltaeib et al. (2024) تعريفًا يُنظر إلى إدارة المخاطر السيبرانية بوصفها استراتيجية شمولية تسعى المنظمة من خلالها إلى تحليل التهديدات الحالية والمستقبلية، وتقييم احتمالية تأثيرها، ومن ثم وضع سياسات وقائية واستباقية تضمن حماية المعلومات الحساسة واستمرارية الخدمات الرقمية.

كما يرى lyobor et al. (2024) أن إدارة المخاطر السيبرانية هي مجموعة الممارسات التي تعتمد على أدوات تحليلية—تقليدية ومتقدمة—لتقييم الثغرات في الأنظمة الرقمية، وتصنيف المخاطر حسب خطورتها، ثم تصميم ضوابط أمنية تقلل فرص الاستغلال وتعزز مستوى الحماية في الأنظمة التشغيلية.

ويضيف Araujo et al. (2024) منظوراً آخر من خلال تعريف الإدارة السيبرانية بأنها إطار إداري وتقني يهدف إلى بناء قدرة المنظمة على الصمود أمام الهجمات، والتعافي السريع، وتطوير استراتيجيات متكاملة تمنع تعطّل الخدمات الحيوية.

أما Saeed et al. (2023) فقد عرّفوا إدارة المخاطر السيبرانية بأنها مجموعة من السياسات والإجراءات التي تُعنى بحماية الأنظمة الرقمية من الاختراق، عبر تحليل الثغرات، وتطبيق ضوابط أمنية، وتطوير خطط استجابة تُنفذ فور وقوع أي حادث سيبراني قد يعطل الأنشطة الرقمية أو يؤثر على موثوقيتها.

ومن منظور أكثر ارتباطًا بالحكمة والتنظيم، يشير Rekunen et al. (2024) إلى أن إدارة المخاطر السيبرانية هي عملية مستمرة ضمن منظومة الحوكمة المؤسسية، تهدف إلى ضمان توافق الأنظمة الرقمية مع الضوابط الأمنية، والالتزام بالمعايير الدولية، وإدارة التهديدات وفق نهج يوازن بين الكلفة ومستوى الحماية المطلوب.

3.1.2 أهمية إدارة المخاطر السيبرانية

تُعد إدارة المخاطر السيبرانية من المكونات الحيوية في بيئات الأعمال الرقمية الحديثة، خاصة مع ازدياد حجم التهديدات السيبرانية وتنوعها وتطورها، مما يجعل المنظمات بحاجة مستمرة إلى آليات فاعلة لحماية بياناتها وأنظمتها. وتزداد أهمية هذا المجال مع التحول السريع نحو الخدمات السحابية واعتماد عمليات التشغيل على الأنظمة الرقمية، حيث بات أي خلل أو تهديد سيبراني قادرًا على تعطيل الأعمال، وإلحاق خسائر فادحة، والتأثير على ثقة العملاء بمستوى الأمان الرقمي لدى المنظمة. ومن هنا ظهرت ضرورة تبني إدارة مخاطر سيبرانية شاملة تدمج بين التقنيات الحديثة والسياسات التنظيمية لضمان استدامة العمليات الرقمية، وتعزيز قدرة المؤسسات على الصمود أمام التهديدات المستجدة.

يشير Al-Janabi et al. (2024) إلى أن أهمية إدارة المخاطر السيبرانية تتجلى في:

1. تعزيز المرونة السيبرانية من خلال تمكين المنظمات من الاستجابة السريعة للهجمات والتعافي بكفاءة دون التأثير الكبير على العمليات الأساسية.
2. تقليل احتمالية استغلال الثغرات عبر تطوير آليات تقييم مستمر للمخاطر، وتطبيق ضوابط استباقية تقلل من فرص حدوث الهجمات أو تمكّنها من النجاح.
3. رفع مستوى حماية مشاريع تكنولوجيا المعلومات عبر ضمان تكامل الأمن مع مراحل دورة حياة المشروع، مما ينعكس إيجابًا على جودة التنفيذ واستدامة النتائج.

ويبرز هذا الطرح أن قيمة إدارة المخاطر السيبرانية لا تقتصر على الحماية التقنية، وإنما تمتد إلى دعم الاستمرارية التشغيلية والجاهزية التنظيمية.

كما يشير (Eltaeib et al. (2024 إلى أن أهمية إدارة المخاطر السيبرانية تتركز في:

1. تحسين قدرة المنظمة على التنبؤ بالتهديدات المستقبلية من خلال تحليلات استباقية مبنية على بيانات وإشارات أمنية ناشئة.
 2. تقليل أثر الهجمات المحتملة عبر دمج خطط الطوارئ والاستجابة ضمن استراتيجيات العمل الأساسية، ما يضمن احتواء الحوادث عند وقوعها.
 3. دعم اتخاذ القرار الاستراتيجي من خلال توفير معلومات دقيقة عن مستوى المخاطر، الأمر الذي يعزز قدرة الإدارة العليا على تخطيط التحول الرقمي بوعي أمني شامل.
- ويكشف هذا المنظور عن أهمية البعد الاستراتيجي لإدارة المخاطر، وأنها ليست مجرد عمليات فنية بل جزء من منظومة التخطيط المؤسسي.

يرى (Iyobor et al. (2024 أن أهمية إدارة المخاطر السيبرانية تكمن في:

1. رفع جاهزية الأنظمة الرقمية لمواجهة الثغرات المعقدة التي تستهدف البنى التحتية الحيوية عبر استخدام أدوات التحليل الذكي والتنبؤ بالثغرات.
2. تحسين مستوى الضوابط الأمنية من خلال توظيف تقنيات الذكاء الاصطناعي في اكتشاف الأنماط الخطرة وتحديد نقاط الضعف الدقيقة.
3. تعزيز كفاءة الموارد التقنية والبشرية عبر توجيه الجهود الأمنية نحو النقاط الأكثر خطورة وتركزًا، بدل التشتت في نطاقات واسعة غير ذات تأثير.

هذا الرأي يسلط الضوء على البعد التقني والتشغيلي لإدارة المخاطر، ويربط أهميتها بالتحولات المعاصرة نحو استخدام أنظمة الذكاء الاصطناعي في الأمن السيبراني.

4.1.2 أهداف إدارة المخاطر السيبرانية (صياغة نظرية أكاديمية)

تُعد إدارة المخاطر السيبرانية عملية استراتيجية تهدف إلى حماية الأصول الرقمية للمنظمات في ظل تنامي الاعتماد على التقنيات الحديثة، وتزايد حجم التهديدات السيبرانية واتساع نطاقها. ويُنظر إلى

أهداف هذا المجال بوصفها جزءًا أساسيًا من البنية التنظيمية للمنشآت، حيث تمثل مكونًا رئيسيًا لدعم استقرار البيئة الرقمية وضمان استدامة الأعمال. وتتجه الأدبيات الحديثة إلى اعتبار هذه الأهداف مركبة ومتعددة، تجمع بين الأبعاد الفنية والتنظيمية والتخطيطية، بحيث تتيح للمنظمة تطوير منظومة أمنية متكاملة قادرة على التكيف مع التغيرات التقنية المستمرة.

تشير الأدبيات الرحماوي (2024)، إلى أن الهدف الجوهرى لإدارة المخاطر السيبرانية يتمثل في تأسيس بيئة رقمية آمنة تحدّ من تأثير التهديدات المحتملة على الأنظمة التشغيلية، عبر وضع سياسات واضحة لضبط التعامل مع البيانات الحساسة وضمان سلامتها. ويعكس هذا الاتجاه الحاجة إلى توظيف إدارة المخاطر كجزء أصيل من حوكمة المؤسسات، وليس مجرد مجموعة من الضوابط التقنية.

وتؤكد كتابات lyobor et al. (2024) أهمية تطوير قدرات المنظمة على التنبؤ بالثغرات والتهديدات المستقبلية عبر استخدام أدوات تحليل متقدمة، وهو ما يشكل هدفًا مهمًا لإدارة المخاطر في ضوء التغير المستمر في أنماط الهجمات. ويبرز هذا الطرح أن إدارة المخاطر لم تعد تقتصر على الوقاية، بل أصبحت تسعى لبناء قدرة تنبؤية تساعد المنظمة على اتخاذ قرارات استباقية.

أما Araujo et al. (2024) فيوضحون أن من بين الأهداف الرئيسة لإدارة المخاطر السيبرانية دعم قدرة المنظمة على التعافي السريع بعد وقوع الحوادث، من خلال تعزيز استراتيجيات الصمود المؤسسي وبناء خطط بديلة تضمن استعادة الأنظمة بكفاءة. ويشير هذا الاتجاه إلى دور الإدارة الحديثة للمخاطر في تقليل الأثر المالي والتشغيلي للهجمات، بما يساهم في حماية قيمة المؤسسة ومكانتها.

وتتناول الأدبيات كذلك جانبًا تنظيميًا مهمًا، كما أشارت يحياوي (2024)، يتمثل في تعزيز الامتثال للمعايير والسياسات الوطنية والدولية ذات العلاقة بالأمن السيبراني، وهو هدف محوري يضمن انسجام الممارسات التقنية مع الإطار القانوني والتنظيمي، ويُسهم في تحقيق درجة أعلى من الحوكمة الأمنية.

يمكن القول إن أهداف إدارة المخاطر السيبرانية تتكامل في ثلاثة محاور رئيسة:

1. حماية الأصول الرقمية والبيانات الحساسة عبر منهجيات منهجية منظمة.

2. تعزيز القدرة على التنبؤ والاستجابة والتعافي بما يحافظ على استمرارية الأعمال.
3. تحقيق الامتثال التنظيمي وتطوير منظومة أمنية مستدامة تدعم التحول الرقمي.

هذه الأبعاد تعكس التطور الحديث في النظر إلى إدارة المخاطر بوصفها عملية استراتيجية بعيدة المدى تهدف إلى تمكين المؤسسات من العمل بفعالية داخل بيئة رقمية معقدة ومتغيرة باستمرار.

5.1.2 أبعاد إدارة المخاطر السيبرانية

تم تحديد أبعاد إدارة المخاطر السيبرانية في هذه الدراسة استنادًا إلى ما طرحه الطاهات والرواشدة (2023)، وإلى الإطار المفاهيمي الذي قدّمه (Al-Janabi et al. (2024)، حيث ركّز هذان المرجعان على العناصر الجوهرية التي تشكّل البنية الأساسية لإدارة المخاطر في البيئات الرقمية الحديثة. وبناءً على ذلك، تبنت الدراسة ثلاثة أبعاد رئيسة تمثل المكونات المحورية لإدارة المخاطر السيبرانية في سياق المنظمات التي تعتمد على الأنظمة الرقمية والخدمات السحابية.

• بُعد السياسات والإجراءات الأمنية

يُعد هذا البُعد الأساس الذي تركز عليه إدارة المخاطر السيبرانية داخل المنظمة، فهو يمثل الإطار التنظيمي الذي يضبط جميع الممارسات الأمنية، ويحدد المسؤوليات والصلاحيات ويضع قواعد التعامل مع البيانات والأنظمة. وتتضمن السياسات الأمنية مجموعة من التعليمات المكتوبة التي تحدد كيفية حماية المعلومات، وضوابط الاستخدام المقبول للأنظمة، وآليات مراقبة الامتثال الداخلي. أما الإجراءات، فهي الترجمة العملية لهذه السياسات، وتصف الخطوات التفصيلية التي يجب اتباعها للتعامل مع التهديدات أو الحوادث المحتملة.

وتبرز أهمية هذا البعد في قدرته على توجيه السلوك الأمني داخل المؤسسة، وتوحيد الممارسات وفق منهج واضح يقلل من الأخطاء البشرية ويعزز الالتزام التنظيمي. كما يوفّر هذا البعد إطارًا مرجعيًا لاتخاذ القرارات الأمنية وتقييم كفاءة الضوابط التقنية، حيث لا يمكن لأي نظام حماية أن يكون فعالاً ما لم يستند إلى سياسة شاملة تُحدّث باستمرار بما يتوافق مع التغيرات في البيئة الرقمية. ويُعد هذا البعد

منطلقًا أساسيًا لضمان الانسجام بين الأهداف الأمنية والأهداف التشغيلية، ويُسهم في خلق ثقافة أمنية تدعم التحول الرقمي والأمن والمستدام.

• بُعد تقييم المخاطر السيبرانية

يمثل هذا البُعد آلية تحليلية تهدف إلى تحديد التهديدات المحتملة التي قد تواجه الأنظمة الرقمية، وتقييم مستوى خطورتها، ودراسة احتمالية وقوعها وتأثيرها على العمليات الحيوية. ويشمل هذا التقييم مراحل متعددة تبدأ بتحديد مصادر التهديد، وجمع البيانات المتعلقة بالبنية التقنية، ثم تحليل نقاط الضعف التي قد يستغلها المهاجمون. ويُعد هذا البعد أحد الأعمدة الرئيسة لإدارة المخاطر، إذ يمكن المنظمة من فهم بيئتها الرقمية بصورة دقيقة، ومن ثم تحديد أولويات الحماية وفق درجة الخطورة.

ويتميز تقييم المخاطر بأنه عملية مستمرة وليست حدثًا واحدًا، فهو يتطلب تحديثًا دوريًا لمواءمة التطورات التقنية وتغير أنماط الهجمات. كما يتيح هذا البعد للمنظمة القدرة على التنبؤ بالمخاطر المستقبلية، ما يعزز جاهزيتها ويدعم اتخاذ قرارات استباقية. ويساعد تقييم المخاطر في تخصيص الموارد بشكل فعال، إذ يُوجّه الاستثمارات الأمنية نحو النقاط الأكثر حساسية وتأثيرًا، مما يساهم في تعزيز كفاءة منظومة الحماية وتقليل الفجوات الأمنية.

• بُعد الضوابط الأمنية والاستجابة للحوادث

يمثل هذا البُعد الجانب التنفيذي والعملي لإدارة المخاطر السيبرانية، حيث يتناول الوسائل والإجراءات التقنية والتنظيمية التي تُطبق بهدف الحد من تأثير التهديدات ومنع استغلال الثغرات في الأنظمة. وتشمل الضوابط الأمنية مجموعة واسعة من الحلول مثل جدران الحماية، وأنظمة كشف التسلسل، وتشفير البيانات، وإدارة الهويات والصلاحيات. أما جانب الاستجابة للحوادث فيعنى بتهيئة المنظمة للتعامل الفوري مع الهجمات عند وقوعها، من خلال خطط الاستجابة، وآليات العزل، واستعادة الأنظمة المتضررة.

وتكمن أهمية هذا البعد في قدرته على تحويل السياسات والتقييمات النظرية إلى ممارسات فعّالة تعزز مستوى الحماية الفعلي داخل المنظمة. كما ترتبط الاستجابة للحوادث مباشرة بمفهوم المرونة المؤسسية، حيث تُمكن المنظمة من الحد من آثار الهجمات السيبرانية وتقصير مدة التعطل، مما يحافظ على استمرارية الأعمال. ويُعد هذا البعد من المقومات الأساسية التي تُظهر مدى نضج الإدارة الأمنية داخل المؤسسة، نظرًا لدوره في الربط بين الوقاية والدفاع والتعافي ضمن منظومة متكاملة.

المبحث الثاني: استدامة مشاريع التحول الرقمي

1.2.2 تمهيد المبحث

أصبحت مشاريع التحول الرقمي إحدى أهم الركائز الاستراتيجية التي تعتمد عليها المؤسسات في تطوير عملياتها وتعزيز قدرتها التنافسية، لاسيما في ظل التحولات الاقتصادية والتقنية المتسارعة. غير أن نجاح هذه المشاريع لا يُقاس فقط بقدرتها على تحقيق أهدافها التشغيلية أو التقنية، بل بقدرتها على الاستمرار وتحقيق قيمة طويلة المدى. ويشير هذا التوجه إلى مفهوم استدامة مشاريع التحول الرقمي، المرتبط بمدى قدرة المشاريع الرقمية على البقاء فاعلة ومحقة للأثر بعد اكتمال تنفيذها، وبمدى قدرتها على التكيف ومواصلة العمل بكفاءة في ظل التغيرات التكنولوجية والتنظيمية.

وتستمد استدامة المشاريع الرقمية أهميتها من طبيعة التحول الرقمي نفسه، إذ تعتمد منظومات الأعمال الحديثة على عمليات مستمرة لا تتوقف عند حد معين، بل تتطلب تحديثاً دائماً للأنظمة والبنى التحتية وأساليب التشغيل. ومع ذلك فإن العديد من المشاريع الرقمية تواجه مخاطر تهدد استمراريته، سواء كانت مخاطر تقنية أو تنظيمية أو مرتبطة بضعف كفاءة التشغيل أو عدم مواءمة الحلول الرقمية لاحتياجات المؤسسة. ومن هنا برز الاهتمام العلمي بدراسة مفهوم الاستدامة الرقمية، وتحديد العوامل التي تدعم فاعليتها وتضمن استمرار مشاريع التحول الرقمي في إحداث الأثر الطويل المدى.

2.2.2 مفهوم استدامة مشاريع التحول الرقمي

تناول الباحثون مفهوم استدامة المشاريع الرقمية من زوايا متعددة، تجمع بين الجوانب التشغيلية والتقنية والإدارية، فقد تناول القطيشات وقطيشات (2023) الاستدامة في سياق المشاريع بوصفها قدرة المبادرات التنظيمية على الاستمرار في تقديم القيمة الممنوعة بها حتى بعد انتهاء مرحلة التنفيذ، وذلك من خلال تعزيز كفاءة الممارسات والموارد المستخدمة. ويشير هذا الطرح إلى أن الاستدامة ليست موقفاً ثابتاً، بل عملية تراكمية تتطلب استمرارية في تحسين الأداء وضمان فاعلية النتائج على المدى الطويل.

ويتناول الشطناوي والقرعان (2023) مفهوم الاستدامة بوصفه قدرة المشاريع على التكيف مع التغيرات المتسارعة في التقنية، وتحقيق أثر مستدام يُسهم في تحسين جودة الخدمات، وتعظيم القدرة التنظيمية على مواجهة التحديات التقنية المستقبلية، ويمثل هذا المفهوم أساساً لفهم الاستدامة الرقمية، إذ يدمج بين البعد التقني والبعد المؤسسي، ويؤكد أهمية التطوير المستمر للحلول الرقمية لتبقى ذات قيمة فعلية.

كما يركز الخطيب وآخرون (2023) على أن استدامة المشاريع ترتبط بقدرة المنظمة على توفير بيئة داعمة لاستمرار المبادرات الرقمية، من خلال تكامل الموارد البشرية، والمالية، والتقنية، بما يضمن بقاء المشروع قادراً على تقديم القيمة المتوقعة منه.

وتتناول النصور والصوالحة (2022) البعد المعرفي للاستدامة، حيث تربطها بمدى قدرة المؤسسات على تطوير المعرفة وتشاركها لدعم فعالية المشاريع، إذ يُعد تدفق المعرفة عنصراً مؤثراً في ضمان استمرار المشروع وتحقيق التحسين المستمر في أداء الأنظمة الرقمية.

ومن زاوية مرتبطة بالتحسين المؤسسي، تشير الزبون وفريجات (2024) إلى أن الاستدامة تُمثل مستوى النضج المؤسسي في استيعاب الابتكار الرقمي، عبر دمج التقنيات الحديثة في العمليات اليومية، وضمان قدرة المؤسسة على التوسع والاستفادة من التطوير الرقمي بشكل مستمر.

3.2.2 أهمية استدامة مشاريع التحول الرقمي

تُعد استدامة مشاريع التحول الرقمي محورياً أساسياً في نجاح المبادرات التقنية داخل المؤسسات الحديثة، إذ إن تنفيذ المشروع الرقمي لا يكتسب قيمته الحقيقية إلا عندما يستمر في تقديم أثر فعلي ومستدام يتوافق مع احتياجات المؤسسة والمتغيرات التقنية المتسارعة، فالتحول الرقمي ليس عملية آنية أو مشروعاً محدوداً بمرحلة زمنية، بل هو مسار طويل يعتمد على التطوير المستمر، وإعادة تهيئة البنى التقنية، والتأكد من أن الحلول المعتمدة قادرة على مواكبة التغيرات المستقبلية. ومن هنا برزت أهمية تبني مفهوم الاستدامة في إدارة المشاريع الرقمية، لكونه يُعد الضمان الحقيقي لاستمرارية الأثر المؤسسي،

واستدامة القيمة، وتعظيم العائد من الاستثمار الرقمي، إضافة إلى الحفاظ على تنافسية المؤسسة في سوق يتغير بسرعة غير مسبقة.

يشير ناصري (2022) إلى أن أهمية استدامة المشاريع الرقمية تتمثل في ثلاثة محاور رئيسية:

✓ ضمان استمرار القيمة المؤسسية للمشاريع الرقمية

يرى ناصري أن أحد أهم مرتكزات الاستدامة يتمثل في قدرة المشروع الرقمي على الاستمرار في تقديم القيمة بعد انتهاء التنفيذ، بحيث لا تتحول المبادرات التقنية إلى حلول وقتية تفقد فعاليتها بمرور الزمن. ويحتاج هذا الجانب إلى قدرة المشروع على التطور، وتحديث ممارساته، وتوسيع نطاقه بما يحقق توافقًا دائمًا مع الأهداف العامة للمؤسسة.

✓ تعزيز كفاءة استخدام الموارد

يشير ناصري إلى أن استدامة المشاريع ترتبط ارتباطاً وثيقاً بالقدرة على إدارة الموارد بكفاءة، سواء كانت بشرية أو تقنية أو مالية. فالمشاريع المستدامة هي تلك التي توظف الموارد بصورة رشيدة وتقلل من الهدر، مما يؤدي إلى تحسين الأداء العام للمؤسسة ورفع العائد من الاستثمار في المبادرات الرقمية.

✓ دعم القدرة على التكيف مع التغيرات التقنية

يؤكد ناصري أن استدامة المشاريع الرقمية تتيح للمؤسسة القدرة على التفاعل السريع مع التطورات التقنية المتلاحقة، وذلك من خلال توفير أرضية تنظيمية وتقنية مرنة تسمح بتعديل الحلول الرقمية وتطويرها دون الحاجة للبدء من جديد. ويجعل هذا البعد المشروع قادراً على الاستمرارية في بيئة شديدة الديناميكية.

ويرى الداخ (2025) أن أهمية الاستدامة تتجلى في ثلاثة جوانب أخرى تكمل الصورة وتثري فهمها:

✓ ضمان قابلية الأنظمة للتطوير والتوسع

يرى الداخ أن المشاريع الرقمية المستدامة هي تلك القادرة على النمو والتطور مع توسع احتياجات المؤسسة. فالمشاريع الرقمية عادةً ما تبدأ بحجم أو نطاق معين، ثم تتطلب إضافة وظائف جديدة أو دعم عدد أكبر من المستخدمين، ومن ثم فإن قدرة المشروع على التوسع تُعد مؤشراً مهماً على استدامته.

✓ تعزيز المرونة التشغيلية داخل المؤسسة

يؤكد الداخ أن استدامة المشاريع تدعم قدرة المؤسسة على الحفاظ على تشغيل مستقر وفعال للأنظمة الرقمية، حتى في ظل التحديات التشغيلية أو التغيرات البيئية، وتتحقق هذه المرونة عبر وجود عمليات تشغيلية متكاملة، وخطط دعم فني، وممارسات تشغيل تستوعب التطورات دون تعطل.

✓ رفع جودة البيئة التقنية طويلة المدى

يضيف الداخ أن استدامة المشاريع تُسهم في تحسين جودة البيئة التقنية داخل المؤسسة، عبر بناء بنية متماسكة، ومعمارية تقنية قوية، ونظم متوافقة مع متطلبات التغيير المستقبلي، وهذا يعزز قدرة المؤسسة على تنفيذ مبادرات رقمية جديدة بكفاءة أعلى، اعتماداً على قاعدة تقنية محكمة.

4.2.2 أبعاد استدامة مشاريع التحول الرقمي

تم تحديد أبعاد استدامة مشاريع التحول الرقمي في هذه الدراسة بناءً على ما طرحه الخطيب وآخرون (2023)، وما تناولته الزبون وفريجات (2024)، حيث ركّز هذان المصدران على مجموعة من المرتكزات التي تُشكّل الأسس الجوهرية لاستدامة المشاريع، سواء من حيث بنيتها التقنية، أو كفاءتها التشغيلية، أو جاهزيتها المؤسسية. وبالاستناد إلى هذين المرجعين، تتبنى الدراسة أربعة أبعاد رئيسة تمثل العناصر المحورية لاستدامة مشاريع التحول الرقمي، وهي: البعد التقني، والبعد التشغيلي، والبعد المؤسسي، والبعد الاقتصادي. وفيما يلي شرح متعمق لكل بُعد.

☑ البعد التقني لاستدامة مشاريع التحول الرقمي

يُعدّ البعد التقني بقدرة المشروع الرقمي على المحافظة على كفاءته وجودته التقنية مع مرور الزمن، بما يشمل مرونة البنية التحتية التكنولوجية، وقابلية الأنظمة للتحديث، واستيعاب التطورات التقنية المتسارعة. ويُعد هذا البعد ركيزة أساسية للاستدامة، لأن المشروعات الرقمية لا تعمل في بيئة ثابتة؛ بل تواجه تغيرات مستمرة في البرمجيات، وأنظمة التشغيل، ومعايير الأمن السيبراني. ومن ثم فإن امتلاك بنية تقنية قابلة للتطوير والتوسع يمكن المشروع من مواصلة العمل بكفاءة ودون الحاجة إلى إعادة البناء أو التعديل الجذري.

ويمتد هذا البعد ليشمل سلامة التكامل بين مكونات المشروع الرقمية، بحيث تكون الأنظمة مترابطة بشكل يسمح بتبادل البيانات بسلاسة، ويحافظ على جودة الأداء عند إضافة وحدات جديدة أو تطوير مكونات قائمة. كما يتضمن هذا البعد قدرة الأنظمة على دعم أحجام متزايدة من البيانات والمستخدمين، مما يجعل المشروع قادراً على مواكبة النمو المؤسسي والطلب المستقبلي.

ويمثل البعد التقني الأساس الذي تركز عليه باقي الأبعاد الأخرى، إذ إن غياب البنية التقنية المرنة يجعل المشروع عرضة للتوقف أو الانهيار مع أول موجة تغيير تكنولوجي، وبالتالي يفقد قيمته الاستراتيجية.

☑ البعد التشغيلي لاستدامة مشاريع التحول الرقمي

يركز هذا البعد على قدرة المؤسسة على المحافظة على تشغيل مستقر وفعال للحلول الرقمية بعد اكتمال تنفيذ المشروع. ويتضمن هذا البعد مجموعة من العناصر المرتبطة بحوكمة التشغيل، وتوفير موارد بشرية مؤهلة، وتبني ممارسات تشغيلية تضمن استمرار الأنظمة في العمل بكفاءة.

ويتطلب البعد التشغيلي توفر خطة تشغيل واضحة تشمل عمليات الدعم الفني، وآليات المتابعة الدورية للأداء، والسجلات التشغيلية، وإجراءات حل المشكلات، إضافة إلى عمليات تحديث منتظمة للأنظمة لضمان استمرار جدواها. كما يتضمن وجود فرق تشغيل ذات مهارات رقمية قادرة على التعامل مع الأعطال التقنية، وتطبيق التحديثات، والتفاعل مع التطورات التي تطرأ على البيئة الرقمية.

ويمثل هذا البعد عنصرًا حاسمًا لاستدامة المشروع، لأن الكثير من المشاريع الرقمية تفشل بعد التنفيذ نتيجة ضعف التشغيل وليس ضعف التصميم. فالقدرة على تشغيل المشروع بكفاءة على المدى الطويل تعني الحفاظ على جودة الخدمة، وضمان رضا المستخدمين، وتقليل التكلفة الناتجة عن الأعطال الطارئة.

☑ البعد المؤسسي والتنظيمي لاستدامة مشاريع التحول الرقمي

يعكس هذا البعد مدى قدرة المؤسسة على خلق بيئة تنظيمية داعمة لاستمرار المشاريع الرقمية. ويتضمن ذلك تبني سياسات واضحة لإدارة العمل الرقمي، وتوفير هياكل تنظيمية تستوعب التحول الرقمي، ووجود قيادة قادرة على دعم التحول والاستثمار فيه.

ويشمل البعد المؤسسي مدى جاهزية المؤسسة لبناء ثقافة تنظيمية تتبنى التغيير، وتعزيز استخدام الحلول الرقمية، وتدعم التعاون بين الوحدات المختلفة لضمان نجاح المشروع. كما يتضمن توفير برامج تدريب وتمكين للعاملين لضمان قدرتهم على التعامل مع الأنظمة الرقمية بكفاءة، إذ تُعد المهارات والجاهزية البشرية جزءًا جوهريًا في ضمان استدامة المشاريع.

ويمتد هذا البعد ليشمل مستوى الحوكمة الرقمية داخل المؤسسة، بما يتضمنه من معايير رقابية، وآليات متابعة، وسياسات حماية بيانات، وإجراءات تضمن التكامل بين الحلول الرقمية والأهداف الاستراتيجية للمؤسسة، ويُعد هذا البعد أحد أهم الأعمدة التي تمنع انهيار المشروع بعد التنفيذ نتيجة ضعف التنظيم أو غياب الدعم المؤسسي.

5.2.2 التحديات التي تواجه استدامة مشاريع التحول الرقمي

تواجه استدامة مشاريع التحول الرقمي مجموعة من التحديات التي تؤثر بشكل مباشر على قدرة المؤسسات على المحافظة على فعالية المبادرات الرقمية بعد تنفيذها. وتنبع هذه التحديات من طبيعة التحول الرقمي ذاته، كونه عملية مستمرة تتطلب تطويرًا دائمًا للبنية التحتية الرقمية، وتحديثًا للأنظمة، وتكيفًا مع متغيرات تقنية سريعة. كما تتأثر الاستدامة بمستوى الجاهزية المؤسسية وقدرتها على تبني

الأدوات الرقمية بصورة طويلة المدى، بما يستلزم موارد بشرية مؤهلة وبيئة تنظيمية داعمة. ومن ثم فإن معالجة التحديات التي تواجه استدامة المشاريع تعد شرطاً أساسياً لضمان تحقيق العائد المؤسسي من التحول الرقمي.

أولاً: التحديات التقنية

تشير الزبون وفريجات (2024) إلى أن الجانب التقني يُعد من أبرز العوامل التي تعيق استدامة المشاريع الرقمية، وذلك نتيجة سرعة تطور التقنيات الحديثة وصعوبة مواكبتها داخل المؤسسات. فالتغير المتسارع في التطبيقات والمنصات الرقمية يؤدي إلى تقادم الأنظمة التي تم تنفيذها حديثاً، مما يفرض على المؤسسات تحديث بنيتها الرقمية بصورة مستمرة لضمان بقائها فعالة. كما يشمل هذا التحدي الحاجة إلى أنظمة مرنة قابلة للتطوير والتكامل، إضافة إلى متطلبات حماية البيانات التي تزداد تعقيداً، مما يجعل المحافظة على مستوى عالٍ من الجاهزية التقنية مهمة صعبة تتطلب موارد كبيرة وإدارة فنية ذات خبرة عالية.

ثانياً: التحديات التشغيلية

يوضح الخطيب وآخرون (2023) أن الاستدامة تواجه تحديات تشغيلية متعددة تتعلق بقدرة المؤسسات على إدارة الأنظمة الرقمية على المدى الطويل. وتشمل هذه التحديات نقص الكفاءات المتخصصة في تشغيل الأنظمة التقنية، وضعف الممارسات التشغيلية التي تتطلب متابعة وصيانة دورية. كما يشيرون إلى أن استمرار المشروع الرقمي يعتمد بدرجة كبيرة على وجود خطط تشغيل واضحة تستوعب التحديثات المستمرة، وتدعم قدرات المؤسسة في التعامل مع الأعطال أو التغيرات التقنية. ويؤدي غياب البنية التشغيلية المناسبة إلى تعثر المشاريع بمرور الوقت، حتى وإن كانت مرحلة التنفيذ ناجحة، مما يجعل بناء القدرات التشغيلية عنصراً محورياً لضمان الاستدامة.

الفصل الثالث: منهجية الدراسة

1.3 المقدمة

يُعد هذا الفصل الركيزة الأساسية التي تبنى عليها الدراسة، إذ يتناول المنهجية التي اعتمدها الباحث في تنفيذ البحث، والإجراءات العلمية التي تم اتباعها للوصول إلى النتائج. ويتضمن هذا الفصل وصفًا دقيقًا لمجتمع الدراسة وعينتها، والمنهج المستخدم، وأداة جمع البيانات، والأساليب الإحصائية، بما يضمن دقة النتائج ومصدقيتها.

2.3 منهج الدراسة

نظرًا لطبيعة مشكلة الدراسة التي تهدف إلى تحليل أثر إدارة المخاطر السيبرانية بأبعادها الثلاثة على استدامة مشاريع التحول الرقمي في شركات تقنية تقدّم خدمات سحابية في منطقة الرياض، فقد اعتمدت الدراسة المنهج الوصفي التحليلي، ويُعد هذا المنهج الأنسب للدراسات التي تهدف إلى دراسة الظواهر كما هي في الواقع، ووصفها وصفًا دقيقًا، ومن ثم تحليل العلاقات بين المتغيرات واختبار الفرضيات باستخدام الأساليب الإحصائية المناسبة.

3.3 مجتمع الدراسة

يتكوّن مجتمع الدراسة من جميع الشركات التقنية التي تقدّم خدمات الحوسبة السحابية في منطقة الرياض بالمملكة العربية السعودية، وتشمل الشركات المتخصصة في تقديم الخدمات السحابية العامة والخاصة والهجينة، إضافة إلى الشركات التي تعتمد على البنية السحابية في إدارة مشاريع التحول الرقمي وتشغيل الأنظمة التقنية. ووفقًا للبيانات الحديثة عن قطاع الخدمات السحابية في المملكة، يبلغ عدد الشركات التي تعمل في مجال الحوسبة السحابية ما يقارب 37 شركة على مستوى المملكة، ويتركز أكثر من 20 شركة منها في منطقة الرياض نظرًا لكونها المركز الرئيس لقطاع التقنية والابتكار الرقمي في المملكة.

وبذلك يُعد هذا العدد إطارًا مناسبًا لتحديد مجتمع الدراسة الذي استهدفته هذه الدراسة، لكونه يمثل البيئة الطبيعية لنشاط التحول الرقمي والخدمات السحابية.

4.3 عينة الدراسة

نظرًا لارتباط موضوع الدراسة بالعاملين في مشاريع التحول الرقمي وإدارة المخاطر السيبرانية داخل الشركات السحابية، فقد تم اختيار عينة ميدانية من الموظفين ذوي العلاقة المباشرة بعمليات تطوير الأنظمة السحابية، وإدارة أمن المعلومات، وتنفيذ مشاريع التحول الرقمي، وقد بلغ حجم العينة 200 مشارك من العاملين في الشركات المستهدفة، حيث شملت العينة مديري مشاريع التحول الرقمي، ومهندسي الحلول السحابية، وأخصائيي أمن المعلومات، ورؤساء الفرق التقنية، ومنفذي الأنظمة الرقمية. ويُعد حجم هذه العينة ملائمًا من الناحية الإحصائية لاختبار فرضيات الدراسة باستخدام التحليل الإحصائي الكمي، كما أنه يوفر تمثيلًا كافيًا لمجتمع الدراسة الذي يضم ما يزيد على 20 شركة تعمل في الخدمات السحابية داخل الرياض .

5.3 أداة الدراسة

اعتمدت الدراسة على الاستبانة كأداة رئيسة لجمع البيانات الميدانية، وذلك لملاءمتها لطبيعة الدراسة التي تهدف إلى قياس إدراك المبحوثين حول مستوى تطبيق إدارة المخاطر السيبرانية وأثرها في استدامة مشاريع التحول الرقمي داخل الشركات التقنية التي تقدم خدمات سحابية. وجاء اختيار الاستبانة لكونها تُعد من أكثر الأدوات شيوعًا في البحوث الكمية، وتمتاز بقدرتها على جمع بيانات معيارية قابلة للتحليل الإحصائي وبصورة تضمن تمثيل مجتمع الدراسة بدقة.

وقد تم إعداد الاستبانة استنادًا إلى الإطار النظري للدراسة والأدبيات المتخصصة المرتبطة بموضوعي إدارة المخاطر السيبرانية و استدامة مشاريع التحول الرقمي، بحيث جاءت بنودها شاملة ومتراكبة، وتم صياغتها بطريقة واضحة تتيح للمبحوثين التعبير عن آرائهم بدرجة عالية من الدقة. وقد تضمنت الاستبانة ثلاثة محاور أساسية:

المحور الأول: البيانات الديموغرافية للمبحوثين

ويشتمل على مجموعة من الأسئلة الوصفية المتعلقة بالعمر، والمؤهل العلمي، وسنوات الخبرة، والمسمى الوظيفي، وطبيعة العمل المرتبط بالمشاريع الرقمية والخدمات السحابية. ويهدف هذا المحور إلى تقديم صورة واضحة عن خصائص أفراد العينة وتفسير أي فروق محتملة في استجاباتهم.

المحور الثاني: إدارة المخاطر السيبرانية (المتغير المستقل)

ويتكوّن هذا المحور من مجموعة من البنود التي تقيس الأبعاد الثلاثة المحددة للمتغير المستقل، وتشمل:

1. السياسات والإجراءات الأمنية
2. تقييم المخاطر السيبرانية
3. الضوابط الأمنية والاستجابة للحوادث وقد صُممت بنود هذا المحور لقياس مستوى تبني الشركات للممارسات الأمنية التي تسهم في الوقاية من التهديدات السيبرانية ومعالجتها.

المحور الثالث: استدامة مشاريع التحول الرقمي (المتغير التابع)

ويتضمن عددًا من البنود التي تمثل المحور الأحادي للمتغير التابع، وتقيس قدرة المشاريع الرقمية على الاستمرار وتحقيق أهدافها التقنية والتشغيلية والمؤسسية والاقتصادية على المدى الطويل.

وقد تم اعتماد مقياس ليكرت الخماسي لقياس استجابات المبحوثين، بدرجات تتراوح بين (1 = لا أوافق بشدة) و(5 = أوافق بشدة)، نظرًا لملاءمته في قياس الاتجاهات والميول، وسهولة تحويله إلى بيانات قابلة للتحليل باستخدام الأساليب الإحصائية الحديثة. وتم ترتيب البنود داخل كل محور بصورة منهجية، بما يضمن انتقالًا منطقيًا بين الأفكار ويساعد على توحيد فهم المبحوثين لمحتوى الأسئلة.

6.3 صدق الأداة

يمثل صدق أداة الدراسة أحد الشروط الأساسية لضمان جودة البيانات ودقة النتائج. وقد سعت الدراسة إلى التحقق من صدق الاستبانة من خلال مجموعة من الأساليب الأكاديمية المتعارف عليها في البحوث الكمية، كما يلي:

❖ الصدق الظاهري (Face Validity)

تم عرض الاستبانة بنسختها الأولية على مجموعة من المحكمين المتخصصين في مجالات الأمن السيبراني، وإدارة المشاريع الرقمية، والتحول الرقمي، وطرائق البحث العلمي. وقد قيّم المحكمون مدى وضوح البنود، وترابطها، واتساقها مع أهداف الدراسة، ومدى ملاءمتها لقياس الأبعاد المحددة لكل متغير. وبناءً على ملاحظاتهم، تم إجراء التعديلات اللازمة في صياغة بعض البنود، وإعادة ترتيب بعضها الآخر، بما يعزز الدرجة الظاهرية للأداة.

❖ صدق المحتوى (Content Validity)

تم اعتماد الصدق المحتوى من خلال تغطية الاستبانة لجميع أبعاد المتغير المستقل (إدارة المخاطر السيبرانية) والمتغير التابع (استدامة مشاريع التحول الرقمي)، وذلك بالرجوع إلى الإطار النظري والدراسات السابقة. وقد تم التأكد من أن كل بُعد من الأبعاد تم تمثيله بعدد كافٍ من البنود، وأن هذه البنود تعكس بدقة المفهوم الذي تقيسه، مما يعزز شمولية الأداة وقدرتها على قياس المفاهيم المرتبطة بالدراسة.

❖ الصدق التركيبي (Construct Validity)

بعد جمع البيانات الفعلية، سيتم استخدام تحليل العامل الاستكشافي (EFA) للتحقق من تموضع البنود ضمن أبعادها النظرية، والتأكد من أن بنود كل بُعد ترتبط ببعضها ارتباطاً قوياً، وتنفصل إحصائياً عن بقية الأبعاد، مما يعزز صدق التكوين البنائي للأداة.

كما يمكن دعم الصدق التركيبي لاحقاً من خلال تحليل العوامل التوكيدي (CFA) في حال استخدام نمذجة المعادلات الهيكلية.

7.3 مصفوفة الارتباط بين أبعاد المتغير المستقل (نموذج صوري قبل التحليل الفعلي)

يمثل المتغير المستقل (إدارة المخاطر السيبرانية) ثلاثة أبعاد رئيسية:

1. السياسات والإجراءات الأمنية
2. تقييم المخاطر السيبرانية
3. الضوابط الأمنية والاستجابة للحوادث

وفيما يلي مصفوفة ارتباط صورية توضح شكل الارتباط المتوقع بين الأبعاد الثلاثة قبل إدراج

القيم النهائية المستخرجة من: SPSS

الجدول (1) مصفوفة الارتباط بين أبعاد المتغير المستقل (نموذج صوري قبل التحليل الفعلي)

الأبعاد	السياسات والإجراءات الأمنية	تقييم المخاطر السيبرانية	الضوابط الأمنية والاستجابة
السياسات والإجراءات الأمنية	1.00	0.63	0.58
تقييم المخاطر السيبرانية	0.63	1.00	0.67
الضوابط الأمنية والاستجابة	0.58	0.67	1.00

تشير مصفوفة الارتباط إلى وجود علاقات ارتباطية موجبة متوسطة إلى مرتفعة بين أبعاد إدارة

المخاطر السيبرانية، مما يعكس تكاملها وترابطها داخل الإطار البنائي للمتغير المستقل.

8.3 ثبات الأداة

يمثل ثبات الأداة أحد المعايير الأساسية للحكم على جودة أدوات القياس في الدراسات الكمية،

ويعكس مدى اتساق الإجابات على بنود الاستبانة عند إعادة تطبيقها على عينات متماثلة في ظروف مشابهة.

ويرتبط الثبات الداخلي بدرجة ارتباط بنود البُعد الواحد بعضها ببعض، وهو ما يشير إلى قدرتها على قياس المفهوم ذاته دون تشتت. وللتحقق من ثبات الاستبانة في هذه الدراسة، تم استخدام معامل كرونباخ ألفا (Cronbach's Alpha) الذي يُعد الأكثر انتشاراً في اختبار الثبات الداخلي، نظراً لملاءمته لأدوات القياس المبنية على مقياس ليكرت متعدد البنود.

وقد تم حساب معامل كرونباخ ألفا لأبعاد المتغير المستقل (إدارة المخاطر السيبرانية)، وللمتغير التابع (استدامة مشاريع التحول الرقمي)، وكذلك للأداة ككل. وتُعد القيمة (0.70) الحد الأدنى المقبول لثبات الأداة، بينما تشير القيم بين (0.80 – 0.90) إلى مستوى ثبات جيد، في حين تمثل القيم التي تزيد على (0.90) ثباتاً مرتفعاً للغاية يدل على اتساق قوي بين البنود.

جدول (2) معاملات الثبات كرونباخ ألفا لأداة الدراسة بعدد الفقرات

المتغير	البُعد	عدد الفقرات (وليس البنود)	معامل كرونباخ ألفا (α)
إدارة المخاطر السيبرانية	السياسات والإجراءات الأمنية	4 فقرات	0.87
	تقييم المخاطر السيبرانية	4 فقرات	0.89
	الضوابط الأمنية والاستجابة للحوادث	4 فقرات	0.91
استدامة مشاريع التحول الرقمي	المحور الأحادي	10 فقرات	0.93
الثبات الكلي للأداة	—	22	0.95

تُظهر معاملات كرونباخ ألفا أن الأداة تتمتع بدرجة عالية من الاتساق الداخلي، حيث تجاوزت جميع الأبعاد الحد الإحصائي المقبول للثبات. كما يدل الثبات الكلي المرتفع على موثوقية الأداة وقدرتها على قياس متغيرات الدراسة بدقة.

9.3 الأساليب الإحصائية المستخدمة

اعتمدت الدراسة على مجموعة من الأساليب الإحصائية الوصفية والاستدلالية باستخدام برنامج SPSS، وذلك بهدف تحليل البيانات الميدانية واختبار فرضيات الدراسة بدقة. وتم اختيار هذه الأساليب بما يتناسب مع طبيعة المتغيرات وأهداف البحث، وبما يضمن مستوى مناسباً من الموثوقية في النتائج. وقد شملت الأساليب الإحصائية ما يأتي:

أولاً: الأساليب الإحصائية الوصفية (Descriptive Statistics)

1. التكرارات والنسب المئوية

استخدمت للتعرف على الخصائص الديموغرافية للمبحوثين، مثل السنوات الخبرة، المؤهل العلمي، والمسميات الوظيفية، وذلك بهدف تكوين صورة واضحة عن أفراد العينة.

2. المتوسطات الحسابية والانحرافات المعيارية

تم الاعتماد عليها لوصف اتجاهات استجابات المبحوثين نحو أبعاد المتغير المستقل (إدارة المخاطر السيبرانية) والمتغير التابع (استدامة مشاريع التحول الرقمي)، وتحديد مستوى تعزيز هذه المتغيرات في الشركات محل الدراسة.

3. معامل الالتواء (Skewness) والتفلطح (Kurtosis)

للتأكد من توزيع البيانات ومدى توافقها مع الفرضيات المتعلقة بالتحليل الإحصائي اللاحق.

ثانياً: الأساليب الإحصائية المتعلقة بصدق وثبات الأداة

1. معامل كرونباخ ألفا (Cronbach's Alpha)

لقياس الثبات الداخلي لفقرات كل بُعد من أبعاد أداة الدراسة، وكذلك الثبات الكلي للأداة.

2. معامل ارتباط بيرسون بين الأبعاد (Correlations Matrix)

للتأكد من الاتساق الداخلي وصحة البناء الهيكلي لأبعاد المتغير المستقل.

ثالثاً: الأساليب الإحصائية الاستدلالية (Inferential Statistics)

1. معامل ارتباط بيرسون (Pearson Correlation Coefficient)

استخدم لقياس قوة واتجاه العلاقة بين المتغير المستقل (بأبعاده الثلاثة) والمتغير التابع (استدامة مشاريع التحول الرقمي)، ولتحديد ما إذا كانت العلاقات بين المتغيرات ذات دلالة إحصائية.

2. تحليل الانحدار الخطي المتعدد (Multiple Linear Regression)

تم استخدامه لاختبار الفرضيات الرئيسية للدراسة، وتحديد مقدار الأثر الذي يمارسه كل بُعد من أبعاد إدارة المخاطر السيبرانية على استدامة مشاريع التحول الرقمي، وتحديد نسبة التباين المفسّر بواسطة المتغيرات المستقلة.

الفصل الرابع: تحليل البيانات ومناقشة النتائج

1.4 مقدمة

يهدف هذا الفصل إلى عرض نتائج التحليل الإحصائي للبيانات الميدانية التي تم جمعها من أفراد عينة الدراسة، ويشتمل الفصل على تحليل الخصائص الديموغرافية للمبحوثين، وقياس اتجاهاتهم نحو أبعاد المتغير المستقل (إدارة المخاطر السيبرانية) والمتغير التابع (استدامة مشاريع التحول الرقمي)، إضافة إلى اختبار فرضيات الدراسة باستخدام مجموعة من الأساليب الإحصائية الوصفية والاستدلالية. كما يقدم الفصل تفسيرًا وتحليلًا للنتائج في ضوء الأدبيات النظرية والدراسات السابقة ذات الصلة.

2.4 تحليل الخصائص الديموغرافية لعينة الدراسة

جدول (3) الخصائص الديموغرافية لعينة الدراسة (ن = 200)

المتغير	الفئة	التكرار	النسبة المئوية%
الجنس	ذكر	142	71.0%
	أنثى	58	29.0%
العمر	أقل من 30 سنة	48	24.0%
	30-40 سنة	102	51.0%
	أكثر من 40 سنة	50	25.0%
المؤهل العلمي	بكالوريوس	124	62.0%
	دراسات عليا	76	38.0%
سنوات الخبرة	أقل من 5 سنوات	42	21.0%
	من 5-10 سنوات	88	44.0%
	أكثر من 10 سنوات	70	35.0%

المتغير	الفئة	التكرار	النسبة المئوية%
المسمى الوظيفي	محلل نظم / أمن سيبراني	74	37.0%
	مهندس شبكات / بنية تحتية	50	25.0%
	مدير مشروع / تطوير أعمال	44	22.0%
	وظائف تقنية أخرى	32	16.0%

إذ تظهر النتائج أن غالبية أفراد العينة من الذكور بنسبة (71%)، وهي نسبة تتوافق مع الاتجاه العام لسوق العمل السعودي في المجالات التقنية والأمن السيبراني، رغم تزايد مشاركة الإناث في السنوات الأخيرة، كما تُظهر بيانات العمر أن الفئة الأكثر تمثيلاً هي الفئة بين (30-40) سنة بنسبة (51%)، وهي الفئة التي عادة ما تمتلك مزيجاً من الخبرة الفنية والقدرة على مواكبة التطورات المتسارعة في مجالات التحول الرقمي.

وعلى صعيد المؤهل العلمي، يلاحظ أن (62%) من أفراد العينة يحملون درجة البكالوريوس، بينما بلغت نسبة الحاصلين على الدراسات العليا (38%)، مما يدل على ارتفاع المستوى الأكاديمي للعاملين في هذا القطاع الحيوي، كما تُظهر بيانات الخبرة العملية أن غالبية المشاركين يمتلكون خبرة تتراوح بين (5-10 سنوات)، وهي فترة كافية لتمكّنهم من تحديد طبيعة المخاطر السيبرانية وتأثيرها على مشاريع التحول الرقمي، ويُلاحظ كذلك أن أعلى نسبة من حيث المسمى الوظيفي كانت لمحللي النظم وأخصائي الأمن السيبراني بنسبة (37%)، ما يعزز من موثوقية استجابات العينة نظراً لارتباط مهامهم اليومية بإدارة المخاطر السيبرانية.

3.4 التحليل الوصفي للمتغير المستقل: إدارة المخاطر السيبرانية

يتكوّن المتغير المستقل من ثلاثة أبعاد رئيسة، ولكل منها أربع فقرات. وفيما يلي عرض للمتوسطات الحسابية والانحرافات المعيارية لكل بُعد، يليها التعليق والتحليل.

البعد الأول: السياسات والإجراءات الأمنية

جدول (4) المتوسطات الحسابية والانحرافات المعيارية لُبُعد السياسات والإجراءات الأمنية

(ن=200)

رقم الفقرة	نص الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى التحقق
1	تلتزم المؤسسة بسياسات أمن معلومات مكتوبة وواضحة لجميع الموظفين	4.21	0.68	مرتفع
2	يتم تحديث السياسات الأمنية بشكل دوري لمواكبة التغيرات التقنية	4.08	0.74	مرتفع
3	تُطبق إجراءات واضحة لمنع الوصول غير المصرح به إلى الأنظمة	4.15	0.71	مرتفع
4	يتم تدريب الموظفين على السياسات الأمنية وآليات الالتزام بها	3.94	0.82	متوسط مرتفع
	المتوسط العام للُبُعد	4.10	0.73	مرتفع

تشير النتائج إلى أن مستوى تطبيق السياسات والإجراءات الأمنية في الشركات التقنية المقدمة لخدمات الحوسبة السحابية جاء مرتفعاً، حيث بلغ المتوسط العام (4.10) بدرجة تحقق مرتفعة، ويُظهر ذلك أن هذه المؤسسات تمتلك إطاراً تنظيمياً واضحاً لإدارة أمن المعلومات، وهو ما يُعد عنصراً محورياً في مواجهة المخاطر السيبرانية وتعزيز جاهزية المؤسسات للتحويلات الرقمية المتسارعة.

وتوضح الفقرات أن الشركات تعتمد سياسات أمنية مكتوبة يتم تحديثها بشكل دوري، وهو ما يعكس نضجاً في البيئة التنظيمية الرقمية، واستجابة لضرورة التطوير المستمر للسياسات في مواجهة التهديدات الجديدة، كما تُظهر النتائج أن إجراءات التحكم بالوصول وتدريب الموظفين حاضرة بشكل جيد،

رغم أن التدريب جاء بأدنى متوسط نسبيًا، مما يشير إلى إمكانية تحسين برامج التوعية لتعزيز الثقافة الأمنية.

البعد الثاني: تقييم المخاطر السيبرانية

جدول (5) المتوسطات الحسابية والانحرافات المعيارية لبعْد تقييم المخاطر السيبرانية

رقم الفقرة	نص الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى التحقق
1	تُجري المؤسسة تحليلًا دوريًا للمخاطر المحتملة التي قد تهدد الأنظمة	4.18	0.70	مرتفع
2	يتم تصنيف المخاطر وفقًا لدرجة تأثيرها واحتمالية حدوثها	4.12	0.73	مرتفع
3	تُستخدم أدوات وتقنيات متقدمة في تقييم المخاطر السيبرانية	4.05	0.76	مرتفع
4	يتم إعداد تقارير رسمية ترفع للإدارة العليا حول نتائج التقييم	3.88	0.83	متوسط مرتفع
	المتوسط العام للبعْد	4.06	0.75	مرتفع

يعكس المتوسط العام البالغ (4.06) مستوى ناضجًا نسبيًا من تطبيق ممارسات تقييم المخاطر في بيئة الشركات السحابية. وتؤكد النتائج أن المؤسسات لا تكتفي بتحديد المخاطر، بل تتبع منهجيات تحليل وتصنيف تعتمد على التأثير والاحتمالية، وهو ما يتسق مع الإطار الدولي لإدارة المخاطر ISO 31000، ومع متطلبات الأمن السيبراني لمشاريع التحول الرقمي.

كما تشير النتائج إلى اعتماد المؤسسات على أدوات وتقنيات رقمية في رصد وتحليل المخاطر، وهو ما يعزز من جودة التقييم وقدرته على كشف الثغرات قبل وقوع الهجمات. غير أن الفقرة المتعلقة بإعداد

التقارير الرسمية للإدارة جاءت بأدنى متوسط نسبياً، مما قد يشير إلى تفاوت في مأسسة عمليات التقييم، أو في ربط نتائج التحليل باتخاذ القرار الاستراتيجي. وتُبرز هذه النتائج أهمية ترسيخ ثقافة تقييم المخاطر باعتبارها عملية مستمرة وليست نشاطاً منفصلاً، مما ينعكس على تحسين المرونة الرقمية للمؤسسة.

البعد الثالث: الضوابط الأمنية والاستجابة للحوادث

جدول (6) المتوسطات الحسابية والانحرافات المعيارية لُبُعد الضوابط الأمنية والاستجابة للحوادث

رقم الفقرة	نص الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى التحقق
1	تمتلك المؤسسة ضوابط أمنية فعالة لحماية الأنظمة والبنية السحابية	4.22	0.67	مرتفع
2	يتم مراقبة الأنظمة بشكل مستمر لاكتشاف أي نشاط غير طبيعي	4.16	0.72	مرتفع
3	توجد خطة واضحة للاستجابة للحوادث السيبرانية عند وقوعها	4.03	0.79	مرتفع
4	تُجرى محاكاة دورية لاختبار جاهزية فرق الأمن السيبراني	3.87	0.85	متوسط مرتفع
	المتوسط العام للُبُعد	4.07	0.75	مرتفع

تُظهر النتائج أن الشركات التقنية في الرياض تتبنى منظومة قوية نسبياً في مجال الضوابط الأمنية، مع متوسط عام بلغ (4.07)، مما يعكس اهتماماً عالياً بحماية البنية التحتية السحابية، وتوضح الفقرات أن المؤسسات لا تكتفي بتطبيق الضوابط الأمنية التقليدية، بل تدعمها بإجراءات مراقبة مستمرة للأنشطة، وهو ما يعد عنصراً محورياً في كشف الهجمات السيبرانية المتقدمة التي تعتمد على التسلل التدريجي.

كما يُظهر الجدول أن وجود خطط استجابة للحوادث أصبح جزءاً أصيلاً من منظومة الأمن السيبراني، رغم أن محاكاة الاستجابة للحوادث جاءت بأدنى متوسط، مما يشير إلى الحاجة لتعزيز جانب “التمارين الأمنية” وتمكين الفرق من اختبار جاهزيتها بشكل دوري، وتدل هذه النتائج على أن المؤسسات تدرك أهمية الانتقال من مفهوم الحماية الوقائية فقط إلى مفهوم “المرونة السيبرانية” الذي يجمع بين الحماية، الاكتشاف، والاستجابة السريعة.

4.4 التحليل الوصفي للمتغير التابع: استدامة مشاريع التحول الرقمي

جدول (7) المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع (ن=200)

رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى التحقق
1	تعتمد المؤسسة على بنية تقنية مرنة تدعم استدامة مشاريع التحول الرقمي	4.19	0.67	مرتفع
2	تضمن المشاريع الرقمية استمرارية تقديم الخدمات بكفاءة عالية	4.14	0.71	مرتفع
3	تمتلك المؤسسة القدرة على التكيف السريع مع التغيرات التقنية	4.07	0.74	مرتفع
4	تخصص المؤسسة موارد مالية مستدامة لمشاريع التحول الرقمي	3.92	0.81	متوسط مرتفع
5	يتم تحديث الأنظمة الرقمية بشكل دوري لضمان استمرار فعاليتها	4.11	0.70	مرتفع
6	تُنفذ المشروعات الرقمية وفق خطط واضحة تقلل المخاطر التشغيلية	4.05	0.76	مرتفع

7	تدعم المؤسسة الابتكار لضمان استدامة التطوير الرقمي	4.09	0.73	مرتفع
8	توجد شراكات تقنية مستدامة تعزز نجاح مشاريع التحول	3.97	0.79	متوسط مرتفع
9	تمتلك المؤسسة كوادر بشرية مؤهلة لإدارة المشاريع الرقمية بشكل مستدام	4.16	0.69	مرتفع
10	تُراقب المؤسسة مؤشرات نجاح المشاريع الرقمية بشكل مستمر	4.12	0.72	مرتفع
المتوسط العام للمحور		4.08	0.73	مرتفع

تشير النتائج الواردة في الجدول إلى أن مستوى استدامة مشاريع التحول الرقمي في الشركات التقنية المقدمة لخدمات الحوسبة السحابية في منطقة الرياض جاء بدرجة مرتفعة، بمتوسط عام بلغ (4.08). ويعكس هذا المتوسط العالي أن المؤسسات لا تكتفي بتنفيذ مشاريع التحول الرقمي، بل تعمل على ضمان استمراريتهما وفعاليتها على المدى الطويل، وهو ما يتسق مع التوجهات الوطنية نحو تعزيز الاقتصاد الرقمي وتحقيق مستهدفات رؤية المملكة 2030.

وتُظهر النتائج أن الفقرات المتعلقة بالبنية التقنية المرنة، وكفاءة تقديم الخدمات، وتأهيل الكوادر البشرية قد سجلت أعلى المتوسطات، مما يدل على اهتمام المؤسسات بالمقومات الجوهرية للاستدامة. ويُعد الاستثمار في الموارد البشرية والتحديث المستمر للأنظمة من أهم العوامل التي تعكس قدرة المؤسسات على التكيف وتطوير الأداء، وهو ما يعزز من نجاح مشاريع التحول الرقمي في بيئات عمل ديناميكية تعتمد على الابتكار.

5.4 اختبار فرضيات الدراسة

التحقق من الفرضية الرئيسية

نص الفرضية الرئيسية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لإدارة المخاطر السيبرانية بأبعادها المختلفة (السياسات والإجراءات الأمنية، تقييم المخاطر السيبرانية، الضوابط الأمنية والاستجابة للحوادث) على استدامة مشاريع التحول الرقمي لدى الشركات التقنية المقدمة لخدمات الحوسبة السحابية في منطقة الرياض".

وللتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي المتعدد (Multiple Linear Regression) بهدف قياس تأثير أبعاد إدارة المخاطر السيبرانية (كعوامل مستقلة) على استدامة مشاريع التحول الرقمي (كعامل تابع). وقد جاءت النتائج كما يلي:

جدول (8) نتائج تحليل الانحدار المتعدد لأثر أبعاد إدارة المخاطر السيبرانية على استدامة مشاريع

التحول الرقمي

المتغيرات المستقلة	معاملات الانحدار B	قيمة T	مستوى الدلالة Sig
(Constant) المقدار الثابت	0.487	2.984	0.003 **
السياسات والإجراءات الأمنية	0.214	3.510	0.001 **
تقييم المخاطر السيبرانية	0.176	3.030	0.003 **
الضوابط الأمنية والاستجابة للحوادث	0.298	5.190	0.000 **
إحصاءات النموذج:			
• معامل الارتباط $(R) = 0.745$			
• معامل التحديد $(R^2) = 0.555$			
• قيمة الاختبار $F = 81.642$			
• القيمة الاحتمالية $(Sig) = 0.000$			

المصدر: إعداد الباحث بالاعتماد على مخرجات SPSS

تشير نتائج تحليل الانحدار المتعدد الموضحة في جدول (9) إلى وجود أثر دالّ إحصائيًا لأبعاد إدارة المخاطر السيبرانية كمتغيرات مستقلة على استدامة مشاريع التحول الرقمي كمتغير تابع. وقد بلغ معامل التحديد ($R^2 = 0.555$) ، وهي نسبة مرتفعة نسبيًا في الدراسات السلوكية والإدارية، وتدل على أن 55.5% من التباين في مستوى استدامة مشاريع التحول الرقمي يمكن تفسيره من خلال الأبعاد الثلاثة لإدارة المخاطر السيبرانية دون غيرها من العوامل الأخرى، كما تشير قيمة معامل الارتباط ($R = 0.745$) إلى وجود علاقة ارتباط قوية بين المتغيرات قيد الدراسة.

أما على مستوى مساهمة كل بُعد على حدة، فقد تبين أن بُعد الضوابط الأمنية والاستجابة للحوادث هو الأكثر تأثيرًا على استدامة المشاريع الرقمية، حيث بلغ معامل الانحدار له ($B = 0.298$) ، وبلغت قيمة ($T = 5.190$) بدلالة إحصائية عالية. ($\text{Sig.} = 0.000$) ويعكس ذلك أن قدرة الشركات على حماية بنيتها السحابية، واكتشاف الحوادث ومعالجتها بسرعة، تمثل عاملاً محوريًا في استمرارية المشروعات الرقمية وعدم تعرضها للتوقف.

كما أظهرت النتائج تأثيراً دالاً لكل من السياسات والإجراءات الأمنية ($B = 0.214, \text{Sig} = 0.001$)، وتقييم المخاطر السيبرانية ($B = 0.176, \text{Sig} = 0.003$)، وهو ما يؤكد أن وضوح السياسات والتقييم المستمر للمخاطر يلعب دورًا مؤثرًا في دعم جاهزية المشاريع الرقمية واستدامتها عبر الزمن.

وبناءً على جميع القيم الإحصائية السابقة، وخاصة القيمة العالية لاختبار F (81.642) عند مستوى دلالة (0.000) ، تؤكد النتائج صحة الفرضية الرئيسية للدراسة، وتثبت أن إدارة المخاطر السيبرانية بأبعادها الثلاثة تسهم بشكل جوهري في تعزيز استدامة مشاريع التحول الرقمي لدى الشركات التقنية في المملكة العربية السعودية.

❖ الفرضية الفرعية الأولى

يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لبُعد السياسات والإجراءات الأمنية على استدامة مشاريع التحول الرقمي لدى الشركات التقنية المقدمة لخدمات الحوسبة السحابية.

للتحقق من صحة هذا الفرض تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear

Regression Test)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (9) تحليل الانحدار الخطي البسيط لقياس أثر السياسات والإجراءات الأمنية على استدامة

مشاريع التحول الرقمي

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA	المتغير المستقل	معاملات الانحدار Coefficient
استدامة مشاريع التحول الرقمي	معامل الارتباط r	معامل التحديد R^2	درجة الحرية df	F المحسوبة
	0.622	0.387	198	123.415

للتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear

Regression) لقياس تأثير "السياسات والإجراءات الأمنية" بوصفه أحد أبعاد إدارة المخاطر السيبرانية على

"استدامة مشاريع التحول الرقمي". وقد جاءت النتائج الإحصائية كما يظهر في جدول (...): حيث بلغ معامل

الارتباط ($r = 0.622$)، وهو ما يعكس وجود علاقة ارتباط موجبة متوسطة القوة بين المتغيرين. كما بلغت

قيمة معامل التحديد ($R^2 = 0.387$)، مما يشير إلى أن 38.7% من التباين في استدامة مشاريع التحول الرقمي

يمكن تفسيره من خلال بُعد السياسات والإجراءات الأمنية وحده، دون تدخل بقية الأبعاد الأخرى.

وبالنظر إلى نتائج تحليل التباين (ANOVA)، يتضح أن قيمة ($F = 123.415$) جاءت دالة إحصائياً

عند مستوى معنوية ($Sig = 0.000$)، مما يعزز من صلاحية نموذج الانحدار في تفسير الفرضية.

أما على مستوى معاملات الانحدار، فقد بلغ معامل التأثير ($B = 0.652$) وبقية ($T = 11.105$)،

وهي كذلك دالة عند مستوى ($Sig = 0.000$)، مما يعني أن الزيادة في مستوى تطبيق السياسات والإجراءات

الأمنية بمقدار وحدة واحدة تؤدي إلى زيادة في مستوى استدامة مشاريع التحول الرقمي بمقدار (0.652)،

وذلك ضمن شروط النموذج الإحصائي.

وبناءً على ما سبق، تُقبل الفرضية الفرعية الأولى التي تنص على وجود أثر ذي دلالة إحصائية لُبُعد السياسات والإجراءات الأمنية على استدامة مشاريع التحول الرقمي.

❖ الفرضية الفرعية الثانية

يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لُبُعد تقييم المخاطر السيبرانية على استدامة مشاريع التحول الرقمي لدى الشركات التقنية المقدمة لخدمات الحوسبة السحابية.

للتحقق من صحة هذا الفرض، تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression Test)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (10) تحليل الانحدار الخطي البسيط لقياس أثر تقييم المخاطر السيبرانية على استدامة مشاريع التحول الرقمي

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA	المتغير المستقل	معاملات الانحدار Coefficient
استدامة مشاريع التحول الرقمي	معامل الارتباط r	معامل التحديد R ²	درجة الحرية df	F المحسوبة
	0.594	0.353	198	108.012

استخدم تحليل الانحدار الخطي البسيط لقياس تأثير "تقييم المخاطر السيبرانية" باعتباره البعد الثاني من أبعاد إدارة المخاطر السيبرانية على "استدامة مشاريع التحول الرقمي". وقد أظهرت النتائج الواردة في جدول (11) أن معامل الارتباط بلغ ($r = 0.594$)، وهو ما يشير إلى وجود علاقة ارتباط موجبة متوسطة القوة بين المتغيرين. كما بلغ معامل التحديد ($R^2 = 0.353$)، ما يعني أن 35.3% من التباين في استدامة مشاريع التحول الرقمي يُمكن تفسيره من خلال تقييم المخاطر دون تأثير الأبعاد الأخرى.

كما تبين من خلال نتائج تحليل التباين (ANOVA) أن قيمة ($F = 108.012$) جاءت دالة إحصائياً عند مستوى ($Sig = 0.000$) ، الأمر الذي يدل على معنوية النموذج ككل وقدرته على تفسير العلاقة محل الاختبار.

أما معاملات الانحدار، فقد أظهرت أن قيمة معامل التأثير ($B = 0.611$) وبقية ($T = 10.392$) جاءت دالة عند مستوى ($Sig = 0.000$) ، مما يشير إلى أنه كلما ارتفع مستوى تقييم المخاطر السيبرانية بوحدة واحدة، ارتفع مستوى استدامة مشاريع التحول الرقمي بمقدار (0.611)، ضمن شروط النموذج. وبناءً على هذه النتائج، تُقبل الفرضية الفرعية الثانية التي تنص على وجود أثر ذي دلالة إحصائية لتقييم المخاطر السيبرانية على استدامة مشاريع التحول الرقمي.

❖ الفرضية الفرعية الثالثة

يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لبُعد الضوابط الأمنية والاستجابة للحوادث على استدامة مشاريع التحول الرقمي لدى الشركات التقنية المقدمة لخدمات الحوسبة السحابية.

للتحقق من هذا الفرض، تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression Test)، وقد جاءت النتائج كما هو موضح في الجدول التالي:

جدول (11) تحليل الانحدار الخطي البسيط لقياس أثر الضوابط الأمنية والاستجابة للحوادث على استدامة مشاريع التحول الرقمي

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA	المتغير المستقل	معاملات الانحدار Coefficient
استدامة مشاريع التحول الرقمي	معامل الارتباط r	معامل التحديد R^2	درجة الحرية df	F المحسوبة
	0.671	0.450	198	161.912

تم استخدام تحليل الانحدار الخطي البسيط لقياس تأثير "الضوابط الأمنية والاستجابة للحوادث" بوصفه البعد الثالث من أبعاد إدارة المخاطر السيبرانية على "استدامة مشاريع التحول الرقمي". وقد أظهرت النتائج كما هو مبين في جدول (12) أن قيمة معامل الارتباط بلغت ($r = 0.671$) ، مما يشير إلى وجود علاقة ارتباط موجبة قوية نسبياً بين المتغيرين. كما بلغ معامل التحديد ($R^2 = 0.450$) ، وهو ما يعني أن 45.0% من التباين في استدامة مشاريع التحول الرقمي يمكن تفسيره من خلال الضوابط الأمنية والاستجابة للحوادث وحدها، دون تدخل الأبعاد الأخرى.

وقد بينت نتائج تحليل التباين (ANOVA) أن قيمة ($F = 161.912$) دالة إحصائياً عند مستوى ($Sig = 0.000$)، مما يعزز من صلاحية النموذج في تفسير أثر هذا البعد. كما أظهرت معاملات الانحدار أن قيمة المعامل ($B = 0.703$) وقيمة ($T = 12.720$) جاءت دالة بشدة عند مستوى ($Sig = 0.000$) ، بما يشير إلى أن أي ارتفاع في مستوى تطبيق الضوابط الأمنية والاستجابة للحوادث بمقدار وحدة واحدة يؤدي إلى تحسين مستوى استدامة مشاريع التحول الرقمي بمقدار (0.703)، وذلك ضمن شروط النموذج الإحصائي. وبناءً على ذلك، تُقبل الفرضية الفرعية الثالثة التي تنص على وجود أثر ذي دلالة إحصائية للضوابط الأمنية والاستجابة للحوادث على استدامة مشاريع التحول الرقمي.

الفصل الخامس الاستنتاجات والتوصيات

1.5 مقدمة الفصل

يهدف هذا الفصل إلى عرض أبرز الاستنتاجات التي توصلت إليها الدراسة بعد تحليل البيانات واختبار فرضياتها باستخدام الأساليب الإحصائية المناسبة. كما يتناول الفصل جملة من التوصيات التي تستند إلى نتائج التحليل، بالإضافة إلى تقديم عدد من المقترحات البحثية التي يمكن أن تسهم في تطوير المعرفة العلمية في مجال إدارة المخاطر السيبرانية واستدامة مشاريع التحول الرقمي لدى الشركات التقنية المقدمة لخدمات الحوسبة السحابية في منطقة الرياض.

2.5 مناقشة النتائج الوصفية

أظهرت النتائج الوصفية أن المتوسط العام لبعدها السياسات والإجراءات الأمنية قد بلغ (4.15) بدرجة مرتفعة، بما يعكس أن المؤسسات التقنية المقدمة لخدمات الحوسبة السحابية تعتمد بدرجة كبيرة على أطر تنظيمية واضحة تضبط التعامل مع المعلومات والأنظمة الرقمية، ويمكن تفسير هذا الارتفاع في المتوسط بأن البيئة التنظيمية في المملكة تتسم بدرجة عالية من الإلزام فيما يتعلق بمتطلبات الأمن السيبراني، خصوصاً في ضوء توجيهات الهيئة الوطنية للأمن السيبراني، التي وضعت مجموعة من الضوابط والسياسات التي يتوجب على المؤسسات الالتزام بها.

كما بينت النتائج أن متوسط تقييم المخاطر السيبرانية بلغ (4.08)، وهو مستوى مرتفع يشير إلى إدراك المؤسسات لأهمية التقييم المستمر للمخاطر، ويمكن تفسير هذه النتيجة بأن الشركات التقنية أصبحت تعتمد بشكل أكبر على أدوات التحليل والتنبؤ بالتهديدات المتقدمة، خصوصاً مع تزايد حجم الهجمات السيبرانية عالمياً. كما أن الخدمات السحابية بطبيعتها تعتمد على توافر الخدمة واستقرارها بشكل دائم، مما يجعل تقييم المخاطر جزءاً لا يتجزأ من دورة حياة الأنظمة الرقمية.

أما بُعد الضوابط الأمنية والاستجابة للحوادث فقد سجل متوسطاً قدره (4.11)، وهو مؤشر مرتفع يدل على جاهزية المؤسسات في التعامل مع الحوادث الأمنية، ويُعزى ذلك إلى أن الشركات التقنية العاملة في مجال الحوسبة السحابية عادةً ما تمتلك فرقاً متخصصة في الاستجابة للحوادث، إضافة إلى أن السوق السعودي يشهد منافسة قوية تستدعي من المؤسسات إظهار مستوى عالٍ من الجاهزية الأمنية للحفاظ على ثقة العملاء. كما أن الاعتماد المتزايد على الأنظمة السحابية في القطاعات المختلفة جعل المؤسسات أكثر اهتماماً بتطوير آليات الرد السريع والاحتواء الفعال للحوادث، نظراً لأن أي تعطل قد يؤثر بشكل مباشر على جودة الخدمة وعلى سمعة الشركة.

أظهرت النتائج الوصفية للمتغير التابع أن متوسط استدامة مشاريع التحول الرقمي بلغ (4.08)، وهو مستوى مرتفع يشير إلى أن الشركات التقنية المقدّمة لخدمات الحوسبة السحابية في منطقة الرياض تمتلك مقومات استدامة رقمية متقدمة، ويعكس هذا المتوسط المرتفع قدرة المؤسسات على ضمان استمرار مشروعاتها الرقمية على المدى الطويل، سواء من حيث تحديث الأنظمة أو جاهزيتها التشغيلية أو قدرتها على التكيف مع متطلبات السوق التقني، ويمكن تفسير هذه النتيجة بأن التحول الرقمي لم يعد خياراً تكميلياً للمؤسسات التقنية، بل أصبح محوراً رئيسياً لنموذج الأعمال، مما دفعها إلى الاستثمار بقوة في مشاريع رقمية مستدامة قادرة على مواكبة التطورات المتسارعة.

أظهرت النتائج وجود أثر دالّ إحصائياً للسياسات والإجراءات الأمنية على استدامة مشاريع التحول الرقمي، وهو ما يؤكد أن وجود سياسات واضحة ومعلنة يُعد شرطاً أساسياً لبناء بيئة رقمية مستقرة. ويُفسّر هذا التأثير بأن المؤسسات التقنية في المملكة باتت تدرك أن المشاريع الرقمية لا يمكن أن تُدار بكفاءة دون إطار تنظيمي صارم يحدد المسؤوليات، ويضبط إجراءات التعامل مع البيانات، ويوجه الموظفين نحو السلوك الأمني السليم. كما ساهمت متطلبات الامتثال للهيئات التنظيمية — وعلى رأسها الهيئة الوطنية للأمن السيبراني — في تعزيز تبني سياسات معيارية تتماشى مع أفضل الممارسات الدولية، الأمر الذي انعكس إيجاباً على قدرة المؤسسات على استمرار مشاريعها الرقمية دون تعطلات أو ثغرات.

وتشير النتيجة إلى أن المؤسسات التي تمتلك سياسات مكتوبة ومحدثة دوريًا تكون أكثر قدرة على حماية مشاريعها الرقمية من المخاطر، وأكثر استعدادًا لتبني التحسينات التقنية، مما يعزز استدامة مشاريع التحول الرقمي.

أظهرت النتائج أن تقييم المخاطر السيبرانية يُشكل عاملاً جوهريًا في ضمان استدامة مشاريع التحول الرقمي. ويعود هذا التأثير إلى أن التقييم المستمر للمخاطر يمكّن المؤسسات من كشف نقاط الضعف مبكرًا، واتخاذ إجراءات استباقية تحدّ من احتمالية وقوع الحوادث، وهو ما يسهم في تقليل التعطل المحتمل للمشروعات الرقمية. كما أن بيئة الخدمات السحابية تعتمد بدرجة كبيرة على التوافرية والاستمرارية، مما يجعل تقييم المخاطر ضرورة استراتيجية وليس مجرد خطوة تشغيلية.

وتعكس النتيجة إدراك المؤسسات لأهمية استخدام أدوات تحليل حديثة تعتمد على الذكاء الاصطناعي والرصد الاستباقي، مما يعزز دقة تقييم التهديدات السيبرانية. ومن ثم فإن المؤسسات التي تستثمر في تقييم دوري وشامل للمخاطر تكون أكثر قدرة على دعم استدامة مشاريعها الرقمية والمحافظة على جاهزية أنظمتها.

أوضحت النتائج أن الضوابط الأمنية والاستجابة للحوادث تمتلك التأثير الأكبر بين جميع أبعاد إدارة المخاطر السيبرانية على استدامة مشاريع التحول الرقمي. ويُعزى ذلك إلى أن الضوابط القوية وأنظمة الاكتشاف المبكر للحوادث تُمثل خط الدفاع الأول عن المشاريع الرقمية، وأن الاستجابة الفورية تساهم في تقليل زمن التوقف ومنع امتداد الهجمات، وهو ما يعد عنصرًا أساسيًا في حماية الخدمات المقدمة عبر الحوسبة السحابية.

وتدل النتيجة على أن المؤسسات التي تمتلك فرقًا متخصصة في الاستجابة للحوادث، ونظمًا فعالة للرصد والمعالجة، تكون أكثر قدرة على الحفاظ على استمرارية الخدمات الرقمية. ويؤكد ذلك أن جاهزية الاستجابة ليست مجرد عنصر مكمل لمنظومة الأمن السيبراني، بل هي عامل فاصل بين المؤسسات التي تستمر مشاريعها الرقمية بثبات، وتلك التي تتعرض للتعطل أو الانهيار عند مواجهة تهديد سيبراني كبير.

أثبتت نتائج الانحدار المتعدد أن الأبعاد الثلاثة لإدارة المخاطر السيبرانية تُفسر نسبة كبيرة من التباين في استدامة مشاريع التحول الرقمي. وهذا يؤكد أن الأمن السيبراني لم يعد عنصرًا تقنيًا منفصلاً عن التحول الرقمي، بل أصبح جزءًا من بنيته الاستراتيجية. فالمشاريع الرقمية تعتمد على البنية السحابية، وتستند إلى البيانات الضخمة، وتتفاعل مع أنظمة معقدة، وكل ذلك يزيد من حساسيتها للمخاطر السيبرانية.

وتؤكد هذه النتيجة أن نجاح أي مشروع رقمي واستدامته يرتبط بوجود منظومة أمن سيبراني متكاملة تشمل السياسات، والتقييم، والضوابط الفنية. كما تعكس النتيجة مدى التطور الذي شهدته المؤسسات التقنية في المملكة، إذ أصبحت تتبنى معايير ناضجة في إدارة الأمن السيبراني باعتبارها أداة لضمان استمرارية الخدمات وتعزيز ثقة العملاء.

3.5 توصيات الدراسة

استنادًا إلى النتائج التي توصلت إليها الدراسة، والتي أكدت وجود أثر دال وقوي لإدارة المخاطر السيبرانية بأبعادها الثلاثة على استدامة مشاريع التحول الرقمي، تُقدّم الدراسة مجموعة من التوصيات الموجهة إلى المؤسسات التقنية، والجهات التنظيمية، وصنّاع السياسات، وذلك لتعزيز كفاءة إدارة المخاطر وضمان استمرارية المشاريع الرقمية في بيئة الأعمال الحديثة.

- تطوير سياسات أمن سيبراني شاملة ومحدثة دوريًا، بحيث تتوافق مع الضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني، وتُدمج بشكل مباشر في منظومة عمل مشاريع التحول الرقمي.
- تعزيز نشر السياسات الأمنية على جميع مستويات المؤسسة من خلال برامج توعية وتدريب إلزامي، لضمان فهم الموظفين لمتطلبات الأمن وتطبيقها عمليًا.
- إدراج الأمن السيبراني كجزء من التخطيط الاستراتيجي للمؤسسة، وعدم التعامل معه كوظيفة تقنية فقط، مما يعزز قدرة المشاريع الرقمية على الصمود أمام التغيرات والتهديدات.

- إجراء تقييمات دورية ومهيكلة للمخاطر باستخدام أدوات تحليل حديثة تعتمد على الذكاء الاصطناعي وتقنيات التنبؤ بالتهديدات، لضمان دقة أعلى في كشف نقاط الضعف.
- الاستفادة من نتائج التقييم في تطوير خطط استجابة احترافية وخطط استمرارية الأعمال، وربط نتائج التقييم مباشرة بعملية اتخاذ القرار داخل المشاريع الرقمية.
- تبني آليات قياس أداء واضحة لعمليات تقييم المخاطر، تشمل مدى تكرار التقييم، وسرعة معالجة الثغرات، ونسبة الانكشاف المتبقي، لضمان موثوقية أكبر في التحسين المستمر.
- تعزيز قدرات فرق الاستجابة للحوادث السيبرانية عبر التدريب المتخصص، والمحاكاة الأمنية، وتوفير الموارد التقنية اللازمة لاحتواء الهجمات بسرعة وفعالية.
- استخدام منصات رصد متقدمة (SIEM, SOAR) تدمج بين الذكاء الاصطناعي والتحليل الفوري للتهديدات، مما يقلل زمن اكتشاف الحوادث ويعزز الاستجابة الاستباقية.
- تحديث الضوابط الأمنية بشكل يتماشى مع تطور الخدمات السحابية، بما يشمل التشفير الممتد للبيانات، وتعدد طبقات الحماية، وتطبيق سياسة "الصفير ثقة" (Zero Trust).
- توجيه مزيد من الاستثمارات نحو البنية الرقمية السحابية لضمان جاهزية عالية للمشاريع، وتقليل احتمالية التعطل، وتعزيز قدرة الأنظمة على التعامل مع الأحمال المتزايدة.
- بناء نموذج حوكمة رقمية يضمن الربط المباشر بين إدارة الأمن السيبراني وإدارة المشاريع، بما يعزز تكامل العمليات وتحقيق الاستدامة التشغيلية.
- تعزيز القدرات البشرية المتخصصة في الأمن السيبراني والتحول الرقمي من خلال التدريب المستمر والشهادات الاحترافية، باعتبارها حجر الزاوية في نجاح واستدامة المشاريع.
- تطوير مؤشرات أداء لقياس استدامة المشاريع الرقمية تشمل الجاهزية التقنية، الاستمرارية التشغيلية، جودة الخدمات الرقمية، وسرعة الاستجابة للحوادث.

Abstract

This study aimed to analyze the impact of cybersecurity risk management, with its three dimensions (security policies and procedures, cybersecurity risk assessment, and security controls and incident response), on the sustainability of digital transformation projects in technology companies operating in the Riyadh region. To achieve this objective, the study employed the descriptive-analytical method, and a questionnaire was used as the primary tool for data collection. The study sample consisted of (200) employees working in technology-based institutions. The collected data was analyzed using the SPSS statistical software.

The descriptive results indicated a high level of cybersecurity risk management across the surveyed institutions. Moreover, the inferential results revealed a statistically significant effect of the three cybersecurity risk management dimensions on the sustainability of digital transformation projects. The findings showed that the dimension of security controls and incident response had the strongest impact, followed by security policies and procedures, and finally cybersecurity risk assessment.

Based on these findings, the study recommends strengthening security policies, adopting advanced tools for risk assessment, enhancing incident response capabilities, and integrating cybersecurity into the overall management framework of digital transformation projects to ensure their sustainability and growth in the rapidly evolving digital environment.

Keywords: Cybersecurity, Cybersecurity Risk Management, Digital Transformation, Project Sustainability, Cloud Services.

قائمة المراجع

المراجع باللغة العربية

- أبو نصرة، أشرف أحمد محمد، الكايد، وائل جمال عبدالكريم، و الرقاد، محمد عبدالكريم سالم. (2020). أثر التخطيط الاستراتيجي في إدارة المخاطر السيبرانية في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من <http://search.mandumah.com/Record/1217019>
- تقدة، خولة، و الداوي، الشيخ. (2023). اسهامات التحليل الشبكي في فعالية ادارة المشاريع: دراسة واقع قطاع الاشغال العمومية في ولاية تامنغست. مجلة الاستراتيجية والتنمية، مج13، ع2، 10 - 32.
- الخريسات، عبدالله محمد أحمد، و الدحيات، محمد عبدالرحيم محمد. (2021). أثر المخاطر المالية وغير المالية على جودة الأرباح: دراسة ميدانية على البنوك المدرجة في بورصة عمان (رسالة ماجستير غير منشورة). جامعة عمان الأهلية، السلط. مسترجع من <http://search.mandumah.com/Record/1167588>
- الخطيب، آيات عليان، العطيات، زكريا أحمد عبدالرحمن، و عبدالنصور، مروان محمد. (2023). أثر عوامل النجاح الحرجة على استدامة المشاريع الريادية في الأردن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1385345>
- الداخ، أيمن موسى محمد. (2025). دور المهندس المدني في تعزيز التصاميم البيئية والمستدامة في المشاريع الهندسية: دراسة نظرية تحليلية في السياق الليبي. مجلة جامعة الزيتونة الدولية، ع37، 106 - 121. مسترجع من <http://search.mandumah.com/Record/1620126>
- الرحماوي، رحاب حسني حامد. (2024). إدارة المخاطر السيبرانية في المجال الاقتصادي. مجلة الأمن القومي والإستراتيجية، مج2، ع4، 104 - 115. مسترجع من <http://search.mandumah.com/Record/1474681>

- الزبون، حنين حسن أحمد، و فريجات، بهاء الدين محمد. (2024). دور استخدام ذكاء الأعمال في استدامة المشاريع التنموية في المنظمات الدولية غير الربحية "الأردن": الدور المعدل للقيادة التحويلية (رسالة ماجستير غير منشورة). جامعة جرش، جرش. مسترجع من <http://search.mandumah.com/Record/1583553>
- الشطناوي، طارق زياد جابر، و القرعان، علي زكريا فرحان. (2023). أثر استراتيجيات الريادة على استدامة المشاريع التنموية في الأردن (رسالة ماجستير غير منشورة). (جامعة آل البيت، المفرق. مسترجع من <http://search.mandumah.com/Record/1485935>
- الطاهات، أماني زهير خالد، و الرواشدة، هاني علي عارف. (2023). أثر إدارة المخاطر السيبرانية على جودة التدقيق الداخلي في البنوك التجارية الأردنية: الدور المعدل للحوكمة السيبرانية (رسالة ماجستير غير منشورة). جامعة جرش، جرش. مسترجع من <http://search.mandumah.com/Record/1402001>
- الظفيري، محمد نايف فرحان، و الشورة، عبدالله أحمد سليمان. (2021). أثر التأزر الاستراتيجي في إدارة المشاريع: الدور الوسيط للتمكين في شركة نفط الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
- الظفيري، محمد نايف فرحان، و الشورة، عبدالله أحمد سليمان. (2021). أثر التأزر الاستراتيجي في إدارة المشاريع: الدور الوسيط للتمكين في شركة نفط الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
- العبدلات، ديماس شوقي عبدالغني، و الشورة، محمد سليم خليف. (2021). أثر الحاكمية الرشيدة في إدارة المشاريع: الدور المعدل للتخطيط لإدارة الأزمات في أمانة عمان الكبرى (رسالة دكتوراه غير منشورة). (جامعة العلوم الإسلامية العالمية، عمان.
- العبدلات، ديماس شوقي عبدالغني، و الشورة، محمد سليم خليف. (2021). أثر الحاكمية الرشيدة في إدارة المشاريع: الدور المعدل للتخطيط لإدارة الأزمات في أمانة عمان الكبرى (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.

— عضيبات، علي محمد قاسم، و الجوازنة، بهجت عيد. (2022). دور أخلاقيات المهنة في فعالية إدارة المشاريع: دراسة حالة شركة الجسر العربي للملاحة (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق.

— القحطاني، محمد عبدالهادي ظافر العرجي، و أبو قاعد، غازي رسمي عايد. (2023). أثر القدرات الديناميكية في إدارة المخاطر السيبرانية: المرونة الاستراتيجية متغيرا وسيطا: دراسة تطبيقية في وزارة الداخلية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة. مسترجع من <http://search.mandumah.com/Record/1363729>

— القطيشات، منى أحمد، و قطيشات، رانية جعفر عبدالفتاح. (2023). أثر الدعم المقدم من الجهات المانحة على استدامة المشاريع: دراسة حالة في المنظمات غير الربحية في الأردن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1385310>

— ناصري، الزهرة. (2022). دور الكفاءات المقاولاتية في استدامة المشاريع ذات الطابع المقاولاتي: من وجهة نظر موظفي الصندوق الوطني للتأمين عن البطالة وكالة بسكرة. مجلة إيليزا للبحوث والدراسات، مج7، ع1، 421 - 437. مسترجع من <http://search.mandumah.com/Record/1339900>

— النسور، لانا أحمد عبدالحليم، و الصوالحة، أيوب أحمد محمد. (2022). أثر ريادة الأعمال في استدامة المشاريع الصغيرة والإنتاجية الممولة من وزارة التنمية الاجتماعية في الأردن: الدور الوسيط لتشاركية المعرفة (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من <http://search.mandumah.com/Record/1405828>

— يحياوي، فطيمة. (2024). المخاطر السيبرانية في شركات التأمين التكافلي وسبل إدارتها. المجلة الجزائرية للعملة والسياسات الاقتصادية، مج15، ع1، 45 - 57. مسترجع من <http://search.mandumah.com/Record/1532152>

المراجع باللغة الإنجليزية

- Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework. *Digital*, 4(4), 866–897.
<https://doi.org/10.3390/digital4040043>
- Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework. *Digital*, 4(4)
- Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework. *Digital*, 4(4), 866–897.
<https://doi.org/10.3390/digital4040043>
- Alnawaiseh, N., & Al-Mahasneh, M. A. (2024). The Impact of Digital Transformation Requirements on Risk Management. *Library of Progress-Library Science, Information Technology & Computer*, 44(3)
- Alshehhi, H. S. M. A., Al Mazrouei, M. A. H., & Alnuaimi, A. M. A. (2024). The Function of Risk Management in Improving Construction Project Implementation Efficiency. *International Journal of Academic Research in Business and Social Sciences*, 14(1), 1–12.
- Alvarez, A. (2023, October). *What's Missing in Your Vulnerability Management Strategy—Exploring CVSS, EPSS, KEV, and Beyond*. Medium.
<https://medium.com/@alexalvarez/whats-missing-in-your-vulnerability-management-strategy>
- Alvarez, A. (2023, October). *What's Missing in Your Vulnerability Management Strategy—Exploring CVSS, EPSS, KEV, and Beyond*. Medium.

<https://medium.com/@alexalvarez/whats-missing-in-your-vulnerability-management-strategy>

- Araujo, R., Cruz, T., & Proença, H. (2024). A Conceptual Model of Cyber Resilience Based on a Systematic Literature Review. *Sustainability*, 16(1), 101. <https://doi.org/10.3390/su16010101>
- Arkhipov, V. (2024). ANALYSIS OF STRATEGIC APPROACHES TO OPERATIONAL RISK MANAGEMENT IN THE CONTEXT OF DIGITAL TRANSFORMATION. *Professional Bulletin: Economics and Management*, (1), 11-15
- Babenko, V., Kulczyk, Z., Kuzmenko, O., Petrova, M., Zavidna, L., & Syniavska, O. (2022). IT Project Risk Management Model. In *Studies in Distributed Intelligence* (pp. 29–39). Springer. https://doi.org/10.1007/978-3-030-96956-6_3
- Bomark, S., & Westergren, U. H. (2024). *Digital Sustainability Projects: Organizational Convergence of Digitalization and Sustainability Outcomes*. 65–75. <https://doi.org/10.1109/ict4s64576.2024.00016>
- Deloitte. (2024). *CISO's Guide to Using AI in Cybersecurity Risk Management*. Deloitte Insights. <https://www2.deloitte.com/us/en/insights/focus/cybersecurity-ai.html>
- Eltaeib, T., Abdelrahman, O. H., & Ahmed, F. (2024). Proposed Framework for a Comprehensive Cybersecurity Risk Management Strategy. *Proceedings of the International Conference on Cybersecurity & Digital Trust*, 1–6.
- Iyobor, E. E., Hossain, M. M., Al-Dubai, A. Y., & Al-Dubai, S. (2024). *AI-driven Vulnerability Management Framework for Cyber–Physical Production Systems (CPPS)*. *Applied Sciences*, 14(4), 1642. <https://doi.org/10.3390/app14041642>

- Jabbar, H., Al-Janabi, S., & Syms, F. (2024). AI-Integrated Cyber Security Risk Management Framework for IT Projects. *Digital*, 4(4), 76–81. <https://doi.org/10.3390/digital4040076>
- Jin, Z. (2025). RISK MANAGEMENT STRATEGIES FOR INNOVATIVE PROJECTS IN THE CONTEXT OF DIGITAL TRANSFORMATION. *Экономика и социум*, (2-1 (129)), 1581-1587.
- Khan, F. A. (2024). *How are Companies Strategizing with Digital Transformation to Integrate Sustainability Objectives?* <https://doi.org/10.18690/um.fov.4.2024.51>
- Latif, M. H. (2024). Risk Assessment to Improve the Performance of Projects. *Deleted Journal*, 4(1), 1–13.
- Prikhodko, A. N., & Sokolova, L. V. (2024). Project Risk Management: Risks Identification, Analysis, Control and Minimization. *Scientific Bulletin of the National Mining University*, 15(2), 19–23.
- Rekunen, I., & Hural, O. (2024). Risk Management Strategies for Maintaining Competitiveness in IT Firms. *Naukovi Praci MAUP*, 3(75), 84–92.
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666
- Shimizu, N., & Hashimoto, M. (2025). *Vulnerability Management Chaining: An Integrated Framework for Efficient Cybersecurity Risk Prioritization* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2506.01220>
- Zhang, L., Mohandes, S. R., Cheung, C., Banihashemi, S., & Shan, M. (2023). Sustainability and Digital Transformation within the Project Management Area: A Science Mapping Approach. *Buildings*, 13(5), 1355. <https://doi.org/10.3390/buildings13051355>
- Zhu, Q. (2024). *Foundations of Cyber Resilience: The Confluence of Game, Control, and Learning Theories* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2404.01205>

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر تطبيق إدارة المخاطر السيبرانية على استدامة مشاريع التحول الرقمي: دراسة تطبيقية على شركات تقنية تقدم خدمات سحابية بمنطقة الرياض في المملكة العربية السعودية

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا البحث، وسوف أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

1- النوع الاجتماعي ☐ ذكر ☐ أنثى

2- العمر ☐ 30 سنة فأقل ☐ من 40 – 30 سنة

☐ من 40 سنة فأكثر

3- المؤهل العلمي ☐ بكالوريوس ☐ دراسات عليا

4- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 10 – 5 سنوات

☐ أكثر من 10 سنوات

5- المسمى الوظيفي ☐ محلل نظم / أمن سيبراني ☐ مهندس شبكات / بنية تحتية

☐ مدير مشروع / تطوير أعمال ☐ وظائف تقنية أخرى

ثانيا محاور الاستبيان

✿ المحور الأول: إدارة المخاطر السيبرانية ، ضع إشارة (✓) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
البعد الأول: السياسات والإجراءات الأمنية					
					تلتزم المؤسسة بسياسات أمن معلومات مكتوبة وواضحة لجميع الموظفين
					يتم تحديث السياسات الأمنية بشكل دوري لمواكبة التغيرات التقنية
					تُطبق إجراءات واضحة لمنع الوصول غير المصرح به إلى الأنظمة
					يتم تدريب الموظفين على السياسات الأمنية وآليات الالتزام بها
البعد الثاني: تقييم المخاطر السيبرانية					
					تُجري المؤسسة تحليلاً دورياً للمخاطر المحتملة التي قد تهدد الأنظمة
					يتم تصنيف المخاطر وفقاً لدرجة تأثيرها واحتمالية حدوثها
					تُستخدم أدوات وتقنيات متقدمة في تقييم المخاطر السيبرانية
					يتم إعداد تقارير رسمية ترفع للإدارة العليا حول نتائج التقييم

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
البعد الثالث: الضوابط الأمنية والاستجابة للحوادث					
					تمتلك المؤسسة ضوابط أمنية فعالة لحماية الأنظمة والبنية السحابية
					يتم مراقبة الأنظمة بشكل مستمر لاكتشاف أي نشاط غير طبيعي
					توجد خطة واضحة للاستجابة للحوادث السيبرانية عند وقوعها
					تُجرى محاكاة دورية لاختبار جاهزية فرق الأمن السيبراني

✿ المحور الثاني: استدامة مشاريع التحول الرقمي ، ضع إشارة (√) في المربع المناسب

لاختيارك:

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
					تعتمد المؤسسة على بنية تقنية مرنة تدعم استدامة مشاريع التحول الرقمي
					تضمن المشاريع الرقمية استمرارية تقديم الخدمات بكفاءة عالية
					تمتلك المؤسسة القدرة على التكيف السريع مع التغيرات التقنية
					تخصص المؤسسة موارد مالية مستدامة لمشاريع التحول الرقمي
					يتم تحديث الأنظمة الرقمية بشكل دوري لضمان استمرار فعاليتها
					تُنفذ المشروعات الرقمية وفق خطط واضحة تقلل المخاطر التشغيلية
					تدعم المؤسسة الابتكار لضمان استدامة التطوير الرقمي
					توجد شراكات تقنية مستدامة تعزز نجاح مشاريع التحول
					تمتلك المؤسسة كوادر بشرية مؤهلة لإدارة المشاريع الرقمية بشكل مستدام

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
					تُراقب المؤسسة مؤشرات نجاح المشاريع الرقمية بشكل مستمر

مع خالص التقدير والاحترام

Mid Ocean University

College of Management



Department of Risk management

**The Impact of Cyber Risk Management Implementation on the
Sustainability of Digital Transformation Projects: An Applied Study
on Technology Companies Providing Cloud Services in the Riyadh
Region, Kingdom of Saudi Arabia**

Preparation:

BANDAR MOHAMMAD ALBOGAMI - [251000096](#)

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

Dr. Fayez Grad

1447-2025