

جامعة ميد أوشن



كلية الإدارة

تخصص إدارة مخاطر

أثر إدارة مخاطر مراكز البيانات على استمرارية الأعمال في المؤسسات

التقنية: دراسة ميدانية على مراكز بيانات في مدينة الرياض

إعداد الطالب/ ماجد بن محمد التميمي

الرقم الجامعي : 251000264

إشراف/

د. الفيصل عبد الحميد محمد حسن

د. فايز جراد

1447-2025



إِهْدَاء

إلى من كانت دعواتهم النور الذي أنار طريقي،

إلى من علّمني أن الجد والاجتهاد سبيل الوصول إلى القمم،

إلى والديّ العزيزين، رمز العطاء والصبر،

لكما كل الامتنان والعرفان على دعمكما المستمر، وثقتكما التي كانت وقودًا لمسيرتي العلمية.

إلى أساتذتي الأفاضل، الذين كانوا مشاعل علم ونور،

أهديكم هذا العمل تقديرًا لجهودكم وتوجيهاتكم التي صنعت الفارق في رحلتي الأكاديمية.

إلى زملائي وأصدقائي، من شاركوني مراحل الدراسة والتعب،

كان وجودكم حافزًا ودافعًا للاستمرار، فلكم كل الشكر والتقدير.

إلى نفسي، التي صبرت وثابرت رغم العثرات،

إلى كل لحظة تحدّ تحولت إلى إنجاز،

أهدي هذا العمل المتواضع عربون فخرٍ وسعيٍ نحو مستقبلٍ أفضل بإذن الله.

شكر ونفائس

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. الفیصل عبد الحمید 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 التعرف على أثر إدارة مخاطر مراكز البيانات بأبعادها (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض، و اعتمدت الدراسة على المنهج الوصفي التحليلي بوصفه الأنسب لطبيعتها، وبلغ حجم العينة (187) مفردة تم تحليل استجاباتها باستخدام البرنامج الإحصائي (SPSS).

توصلت نتائج الدراسة إلى أن مستوى تطبيق إدارة مخاطر مراكز البيانات في المؤسسات التقنية جاء مرتفعاً ، كما تبين أن مستوى استمرارية الأعمال يُعد مرتفعاً جداً ، مما يعكس وعياً مؤسسياً بأهمية الوقاية والاستعداد المسبق للأزمات، كما أظهرت نتائج تحليل الانحدار وجود أثر إيجابي ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لإدارة مخاطر مراكز البيانات بأبعادها مجتمعة على استمرارية الأعمال.

أوصت الدراسة بضرورة تطبيق إطار موحد لإدارة المخاطر واستمرارية الأعمال وفق المعايير الدولية (ISO 31000, ISO 22301) ، وتحديث سجلات المخاطر بشكل دوري، وتبني أنظمة تحليل تنبؤية تعتمد على الذكاء الاصطناعي لتحديد التهديدات المستقبلية.

الكلمات المفتاحية: إدارة المخاطر، مراكز البيانات، استمرارية الأعمال، معالجة المخاطر، المرونة

التشغيلية، المؤسسات التقنية، مدينة الرياض

قائمة المحتويات

أ.....	بسم الله الرحمن الرحيم
ب.....	الإهداء
ج.....	الشكر والتقدير
د.....	المستخلص
ه.....	قائمة المحتويات
ح.....	قائمة الجداول
1.....	الفصل الأول: الإطار العام للدراسة
1.....	1.1 المقدمة
2.....	2.1 مشكلة الدراسة
4.....	3.1 أهمية الدراسة:
5.....	4.1 أهداف الدراسة:
6.....	5.1 تساؤلات الدراسة
7.....	6.1 فروض الدراسة:
7.....	7.1 الدراسات السابقة:
14.....	8.1 الفجوة البحثية:
15.....	9.1 المنطلقات النظرية للدراسة:
19.....	10.1 المنهجية وطرق البحث:
19.....	11.1 مصادر جمع البيانات

20	12.1 حدود الدراسة:
21	الفصل الثاني: الإطار النظري
21	المبحث الأول: إدارة مخاطر مراكز البيانات
21	1.1.2 التمهيد
22	3.1.2 مفهوم إدارة مخاطر مراكز البيانات
24	4.1.2 أهمية إدارة مخاطر مراكز البيانات
25	5.1.2 أهداف إدارة مخاطر مراكز البيانات
27	6.1.2 أبعاد إدارة مخاطر مراكز البيانات
31	المبحث الثاني: استمرارية الأعمال في المؤسسات التقنية
31	1.2.2 التمهيد
31	2.2.2 مفهوم استمرارية الأعمال
33	3.2.2 أهمية استمرارية الأعمال
34	4.2.2 أهداف استمرارية الأعمال
36	5.2.2 التحديات التي تواجه إدارة استمرارية الأعمال
40	الفصل الثالث: منهجية الدراسة
40	1.3 منهج الدراسة
40	2.3 مجتمع الدراسة
41	3.3 أداة الدراسة
43	4.3. صدق أداة الدراسة
43	5.3 مصفوفة الارتباط للمتغير المستقل

44	6.3 ثبات أداة الدراسة
45	7.3 أساليب التحليل الإحصائي المستخدمة في الدراسة
47	الفصل الرابع: تحليل البيانات ومناقشة النتائج
47	1.4 تمهيد
47	2.4 الخصائص الديموغرافية لعينة الدراسة
49	3.4 التحليل الوصفي للمتغير المستقل — إدارة مخاطر مراكز البيانات
53	4.4 التحليل الوصفي للمتغير التابع — استمرارية الأعمال (Business Continuity)
55	5.4 اختبار فرضيات الدراسة
61	الفصل الخامس: النتائج والتوصيات
61	1.5 تمهيد
61	2.5 مناقشة النتائج
65	3.5 التوصيات
67	Abstract
68	قائمة المراجع
68	المراجع باللغة العربية
70	المراجع باللغة الإنجليزية
72	الملاحق
73	استمارة استبيان

قائمة الجداول

رقم الجدول	اسم الجدول	رقم الصفحة
١.	الجدول (1) مصفوفة الارتباط للمتغير المستقل	43
٢.	الجدول (2): معاملات الثبات لمتغيرات الدراسة باستخدام معامل كرونباخ ألفا	44
٣.	الجدول (3): التوزيع الديموغرافي لعينة الدراسة (ن = 187)	47
٤.	الجدول (4) التحليل الوصفي لبعد تحديد المخاطر (Risk Identification)	49
٥.	الجدول (5) التحليل الوصفي لبعد تحليل المخاطر (Risk Analysis)	50
٦.	الجدول (6) التحليل الوصفي لبعد تقييم المخاطر (Risk Evaluation)	51
٧.	الجدول (7) التحليل الوصفي لبعد معالجة المخاطر (Risk Treatment)	52
٨.	الجدول (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات متغير استمرارية الأعمال (ن = 187)	54
٩.	الجدول (9): نتائج تحليل الانحدار المتعدد لأثر أبعاد إدارة مخاطر مراكز البيانات على استمرارية الأعمال	56
١٠.	الجدول (10): نتائج تحليل الانحدار الخطي البسيط لأثر تحديد المخاطر على استمرارية الأعمال	58

رقم الصفحة	اسم الجدول	رقم الجدول
59	الجدول (11): نتائج تحليل الانحدار الخطي البسيط لأثر تحليل المخاطر على استمرارية الأعمال	١١.
59	الجدول (12): نتائج تحليل الانحدار الخطي البسيط لأثر تقييم المخاطر على استمرارية الأعمال	١٢.
60	الجدول (13): نتائج تحليل الانحدار الخطي البسيط لأثر معالجة المخاطر على استمرارية الأعمال	١٣.

الفصل الأول: الإطار العام للدراسة

1.1 المقدمة

يشهد العالم في العقدین الأخيرین تحولات رقمية متسارعة أدت إلى إعادة صياغة طبيعة العمل المؤسسي وطرق إدارة الموارد والمعلومات، فقد أصبحت التقنية الرقمية الركيزة الأساسية لعمليات الإنتاج والخدمات في مختلف القطاعات، مما جعل البيانات والمعلومات تمثل المورد الأكثر قيمة واستراتيجية في العصر الحديث، ويُعد الحفاظ على تدفق البيانات واستمرارية الوصول إليها عنصراً جوهرياً في بقاء المؤسسات وقدرتها على المنافسة، وظهرت مراكز البيانات (Data Centers) بوصفها القلب النابض للبنية التحتية الرقمية، إذ توفر بيئة متكاملة لتخزين ومعالجة البيانات وتمكين الأنظمة الذكية والحلول السحابية التي تعتمد عليها المؤسسات في أعمالها اليومية. 【Mošková & Bugarová, 2023】

إن تزايد الاعتماد على مراكز البيانات جعلها عرضةً لمجموعة واسعة من المخاطر التقنية والتشغيلية والأمنية، مثل انقطاع الطاقة، والتهديدات السيبرانية، وفشل الأنظمة، والكوارث الطبيعية، وهو ما يهدد استقرار الأعمال وسلامة المعلومات الحساسة، وبرز مفهوم إدارة المخاطر (Risk Management) كإطار منهجي يسعى إلى التعرف على المخاطر المحتملة وتحليلها وتقييمها ثم وضع خطط لمعالجتها بما يضمن حماية الأصول الحيوية واستمرارية العمليات، وقد أوضح العنزي وآخرون (2024) أن تطبيق استراتيجيات متقدمة لإدارة المخاطر يساهم في دعم نجاح المشروعات واستدامة العمليات في المؤسسات التقنية. كما أشار Hussaini & Raharjo (2024) إلى أن التهديدات المتزايدة على مراكز البيانات تتطلب تطوير نماذج تقييم شاملة ومستمرة للمخاطر تعزز القدرة المؤسسية على الاستباقية والتصدي للأزمات بكفاءة.

من ناحية أخرى، يُعد مفهوم استمرارية الأعمال (Business Continuity Management – BCM) من أبرز المفاهيم التي اكتسبت أهمية متزايدة في الإدارة الحديثة، نظراً لارتباطه المباشر بقدرة المؤسسات على الاستجابة للأزمات والحفاظ على تشغيل عملياتها الحيوية، وقد أشار شديد (2022) إلى أن

استمرارية الأعمال ليست مجرد خطة استجابة طارئة، بل نظام إداري متكامل يهدف إلى ضمان استمرار الأنشطة الحرجة أثناء الأزمات واستعادة الأداء الطبيعي بسرعة بعد انتهائها.

ولقد أصبح التكامل بين إدارة المخاطر واستمرارية الأعمال ضرورة مؤسسية في ضوء التحولات التقنية المتسارعة، خاصة في البيئات الرقمية المعقدة التي تعتمد على الذكاء الاصطناعي والحوسبة السحابية وإنترنت الأشياء. ففي دراسة (Yang & Lee (2023)، تبين أن العديد من المؤسسات تُهمل في تقييمها للمخاطر فترة تحقيق أهداف الاستمرارية، ما يؤدي إلى سوء تقدير أولويات المخاطر وعدم التوازن بين الوقاية والاستجابة، كما أوضح (Zhang et al. (2021 أن فشل المؤسسات في إدماج تقييم المخاطر ضمن خطط الاستمرارية يؤدي إلى ضعف القدرة على التنبؤ بالتهديدات المستقبلية، أما (Levy (2020 فقد شدد على أهمية وجود إطار معياري لتقييم مخاطر مراكز البيانات، يسمح بالمقارنة بين مستويات الجاهزية التشغيلية للمواقع المختلفة ويضمن اتساق القرارات المتعلقة بالاستجابة والوقاية.

وفي ظل التحول الرقمي الذي تشهده المملكة العربية السعودية في إطار رؤيتها الوطنية 2030، تزايدت أهمية مراكز البيانات بوصفها دعامة أساسية للاقتصاد الرقمي، خاصة في مدينة الرياض التي تُعد مركزاً رئيساً للابتكار التقني والبنية التحتية الذكية، ومع هذا التوسع، أصبحت المؤسسات التقنية تواجه تحدياً في تحقيق التوازن بين التوسع التقني وضمان الجاهزية التشغيلية في مواجهة المخاطر، وقد بين (Denny & Myneni (2025 أن إدارة المخاطر في مراكز البيانات الضخمة تتطلب تكاملاً بين مراحل التصميم والتشغيل، لضمان التنبؤ بالمخاطر ومعالجتها قبل أن تؤثر في استمرارية الخدمة.

ومن ثم، تبرز الحاجة إلى دراسة علمية تُحلل أثر إدارة مخاطر مراكز البيانات بأبعادها الأساسية على استمرارية الأعمال في البيئة السعودية، وتضع إطاراً تطبيقياً يمكن من خلاله دعم مرونة المؤسسات التقنية وتعزيز قدرتها على الصمود أمام الاضطرابات الرقمية.

2.1 مشكلة الدراسة

تُعد مراكز البيانات (Data Centers) من أهم البنى التحتية الحيوية التي تعتمد عليها المؤسسات التقنية لضمان استمرارية أعمالها الرقمية، إذ تمثل محور تخزين ومعالجة وتدفق المعلومات التي تقوم

عليها العمليات التشغيلية اليومية. ومع تسارع التحول الرقمي وازدياد الاعتماد على الأنظمة السحابية، أصبحت هذه المراكز تواجه أنواعًا متعددة من المخاطر التقنية والتشغيلية مثل الانقطاعات المفاجئة، والأعطال الأمنية، والتهديدات السيبرانية، والكوارث الطبيعية، مما جعل إدارة المخاطر تمثل عنصرًا حاسمًا في حماية استمرارية الأعمال وضمان المرونة التشغيلية.

على الرغم من أهمية إدارة المخاطر، إلا أن العديد من المؤسسات التقنية لا تزال تتعامل معها كوظيفة فنية منفصلة عن إدارة استمرارية الأعمال، دون وجود تكامل منهجي بينهما، مما يؤدي إلى فجوة في الاستجابة للأزمات، فقد أوضحت دراسة (Yang & Lee (2023 أن معظم خطط إدارة المخاطر في المؤسسات لا تراعي فترة تحقيق أهداف الاستمرارية التشغيلية، مما يؤدي إلى سوء في ترتيب الأولويات وضعف القدرة على التنبؤ بالتهديدات في الوقت المناسب.

و تُظهر الأدبيات العربية قصورًا واضحًا في الدراسات التي تناولت العلاقة المباشرة بين إدارة مخاطر مراكز البيانات واستمرارية الأعمال، حيث ركزت معظم الأبحاث على إدارة المخاطر أو على استمرارية الأعمال كموضوعين منفصلين، وتناولت دراسة شديد (2022) استمرارية الأعمال في مواجهة الأزمات في وزارة الصحة المصرية دون التطرق إلى البنية التقنية أو إدارة المخاطر الرقمية، بينما تناولت العنزي وآخرون (2024) أثر استراتيجيات إدارة المخاطر على نجاح المشروعات دون ربطها بالاستدامة التشغيلية، أما العلوان والحياصات (2022) فقد أكدوا أهمية إدارة المخاطر في جودة المشاريع الهندسية، لكنهما لم يتناولوا انعكاس ذلك على استمرارية التشغيل في البيئة الرقمية.

ومن هنا تظهر الفجوة البحثية في دراسة العلاقة التكاملية بين إدارة المخاطر التقنية واستمرارية الأعمال في المؤسسات التي تعتمد بشكل كبير على نظم البيانات والبنية التحتية للمعلوماتية.

وبناءً على ما سبق، تتحدد مشكلة هذه الدراسة في القصور القائم في التكامل بين إدارة مخاطر مراكز البيانات واستمرارية الأعمال داخل المؤسسات التقنية في مدينة الرياض، مما يؤدي إلى تحديات في التنبؤ بالمخاطر والاستجابة لها وضمان استدامة العمليات الحيوية. كما تنبع المشكلة من غياب الأطر

المحلية المعيارية التي توائم بين المعايير الدولية (ISO 31000) و (ISO 22301) ومتطلبات البيئة التنظيمية السعودية .

ومن ثم، فإن هذه الدراسة تسعى إلى تحليل أثر إدارة مخاطر مراكز البيانات بأبعادها (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال، من أجل تقديم إطار تطبيقي يعزز المرونة المؤسسية في المؤسسات التقنية السعودية.

3.1 أهمية الدراسة:

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي:

الأهمية العلمية:

- ✓ تُسهم الدراسة في إثراء الجانب النظري والمعرفي حول موضوع إدارة مخاطر مراكز البيانات واستمرارية الأعمال في المؤسسات التقنية.
- ✓ تُعد من الدراسات القليلة التي تناولت العلاقة بين إدارة المخاطر واستمرارية الأعمال في سياق مراكز البيانات داخل البيئة السعودية.
- ✓ تقدم إطارًا نظريًا متكاملًا يوضح أبعاد إدارة مخاطر مراكز البيانات (تحديد، تحليل، تقييم، معالجة) وأثرها على استمرارية الأعمال.
- ✓ تُساهم في دمج مفاهيم إدارة المخاطر واستمرارية الأعمال ضمن إطار واحد يعزز من فهم كيفية تحقيق المرونة التشغيلية للمؤسسات التقنية.
- ✓ تفتح المجال أمام دراسات مستقبلية لتطبيق النموذج المقترح في قطاعات أخرى تعتمد على البنية التحتية الرقمية.

الأهمية العملية:

- ✓ تُزوّد المؤسسات التقنية في مدينة الرياض بنتائج عملية تساعد في تطوير استراتيجيات إدارة المخاطر بمراكز البيانات.
- ✓ تُساعد في تحسين جاهزية مراكز البيانات لمواجهة الأعطال أو الكوارث التشغيلية وضمان استمرارية الخدمات الحيوية.
- ✓ تُوفّر أداة تقييم علمية يمكن استخدامها لتحديد أوجه القصور في إدارة المخاطر وتعزيز كفاءة الخطط التشغيلية.
- ✓ تدعم صنّاع القرار ومديري مراكز البيانات في تبني ممارسات مبنية على أدلة علمية لرفع مستوى الأمان والاعتمادية.
- ✓ تُساهم في مواءمة السياسات والإجراءات المحلية مع المعايير الدولية مثل ISO 27001 و ISO 22301 المتعلقة باستمرارية الأعمال وأمن المعلومات.
- ✓ تعزز القدرة التنافسية للمؤسسات التقنية السعودية من خلال تقليل زمن الانقطاع وتحسين كفاءة التشغيل والاستجابة للأزمات.

4.1 أهداف الدراسة:

تهدف هذه الدراسة إلى دراسة أثر إدارة مخاطر مراكز البيانات بأبعادها (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية، وذلك من خلال تطبيقها على مراكز البيانات في مدينة الرياض.

الأهداف الفرعية:

١. التعرف على مدى تطبيق عمليات تحديد المخاطر في مراكز البيانات وأثرها في تعزيز استمرارية الأعمال.

٢. تحليل أثر منهجيات تحليل المخاطر في مراكز البيانات على كفاءة استجابة المؤسسات التقنية للأزمات والانقطاعات.
٣. دراسة أثر تقييم المخاطر وفق أولوياتها ومستوياتها في دعم استراتيجيات استمرارية الأعمال في المؤسسات التقنية.
٤. قياس أثر استراتيجيات معالجة المخاطر (الوقاية، التخفيف، الاستجابة، والتعافي) على استدامة العمليات التشغيلية في مراكز البيانات.
٥. اقتراح نموذج متكامل لإدارة مخاطر مراكز البيانات يساهم في تعزيز استمرارية الأعمال ورفع جاهزية المؤسسات التقنية في مواجهة التحديات التشغيلية.

5.1 تساؤلات الدراسة

السؤال الرئيسي الأول: ما أثر إدارة مخاطر مراكز البيانات بأبعادها (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض؟

الأسئلة الفرعية:

1. ما مدى تطبيق بُعد تحديد المخاطر في مراكز البيانات، وما أثره على استمرارية الأعمال في المؤسسات التقنية؟
2. كيف يؤثر تحليل المخاطر في مراكز البيانات على قدرة المؤسسات التقنية على مواجهة الأزمات والانقطاعات التشغيلية؟
3. ما العلاقة بين تقييم المخاطر وفقًا لأولوياتها ومستوياتها وبين تحسين كفاءة استمرارية الأعمال في المؤسسات التقنية؟
4. إلى أي مدى تساهم استراتيجيات معالجة المخاطر (الوقاية، التخفيف، الاستجابة، والتعافي) في تحقيق استدامة العمليات التشغيلية في مراكز البيانات؟

5. ما النموذج المقترح لإدارة مخاطر مراكز البيانات الذي يمكن أن يُسهم في تعزيز استمرارية الأعمال ورفع جاهزية المؤسسات التقنية في مدينة الرياض؟

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: هناك أثر ذو دلالة إحصائية لإدارة مخاطر مراكز البيانات بأبعادها (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.

وينبثق من هذه الفرضية الفرضيات الفرعية الأربع التالية:

- الفرض الفرعي الأول: يوجد أثر ذو دلالة إحصائية لبُعد تحديد المخاطر على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.
- الفرض الفرعي الثاني: يوجد أثر ذو دلالة إحصائية لبُعد تحليل المخاطر على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.
- الفرض الفرعي الثالث: يوجد أثر ذو دلالة إحصائية لبُعد تقييم المخاطر على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.
- الفرض الفرعي الرابع: يوجد أثر ذو دلالة إحصائية لبُعد معالجة المخاطر على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.

7.1 الدراسات السابقة:

دراسة (Yang & Lee, 2023) 

هدفت الدراسة إلى التعرف على مدى فاعلية معايير اختيار المخاطر ذات الأولوية للإدارة في ضوء فترة تحقيق خطة استمرارية الأعمال والأثر المتبقي للمخاطر بأبعادهما المتمثلة في احتمالية الحدوث وشدة

التأثير وفترة تحقيق الهدف، وذلك على دقة ترتيب أولويات إدارة المخاطر في نظام إدارة استمرارية الأعمال (BCMS). استخدمت الدراسة المنهج التحليلي المقارن من خلال مقارنة نتائج تقييم المخاطر الحالية بنتائج التقييم وفقاً لأولويات الأثر المتبقي خلال فترة تحقيق خطة الأعمال، وتكونت عينة الدراسة من مجموعة من المخاطر المحتملة التي تم تحديدها ضمن تحليل تأثير الأعمال في مؤسسات تطبق نظام إدارة استمرارية الأعمال. وتوصلت نتائج الدراسة إلى أن إغفال فترة تحقيق خطة استمرارية الأعمال يؤدي إلى عدم دقة في تحديد أولويات المخاطر، وأن إدراجها كمعيار أساسي يعزز فعالية إدارة المخاطر ويوجه الموارد نحو المخاطر الأكثر تأثيراً خلال الفترة الحرجة لتحقيق الأهداف. وأوصت الدراسة بضرورة تضمين فترة تحقيق خطة استمرارية الأعمال ضمن معايير تقييم المخاطر وتحديد أولوياتها في إطار نظام إدارة استمرارية الأعمال، وتحديث منهجيات التقييم بما يضمن التكامل بين التحليل الاحتمالي والتحليل الزمني للأثر المتبقي.

دراسة (Sagi, 2024) 🌈

هدفت الدراسة إلى التعرف على أهمية مرونة قواعد البيانات واختبار حالات الفشل في بيئات الأعمال، وذلك من خلال إبراز الاستراتيجيات والابتكارات التي تضمن قدرة قواعد البيانات على مواجهة الاضطرابات واستمرار العمليات دون انقطاع، مع التركيز على دمج مفهوم المرونة في تصميم البنية التحتية لقواعد البيانات كخيار استراتيجي لتحقيق الكفاءة والاعتمادية العالية. استخدمت الدراسة المنهج التجريبي والتحليلي من خلال تجارب واختبارات فشل أُجريت على أنظمة قواعد بيانات مختلفة لتحليل قدرتها على الصمود أمام الأعطال دون التأثير في حركة الشبكة أو التخزين. وتكونت عينة الدراسة من مجموعة من أنظمة قواعد البيانات المستخدمة في بيئات أعمال تعتمد على البيانات بصورة أساسية. وتوصلت نتائج الدراسة إلى أن دمج المرونة في تصميم قواعد البيانات يُعدّ عاملاً حاسماً لضمان استمرارية الأعمال وتقليل المخاطر التشغيلية، وأن تحسين ممارسات المرونة بما يتوافق مع التطورات التقنية يعزز من كفاءة الوصول إلى البيانات واستقرار الأنظمة. وأوصت الدراسة بضرورة تحديث بنية قواعد البيانات بشكل مستمر ودمج آليات اختبار الفشل كجزء من استراتيجيات الحماية لضمان الأداء العالي والموثوقية المستدامة في بيئات الأعمال المعتمدة على البيانات...

هدفت الدراسة إلى التعرف على كيفية توظيف منهجيات استمرارية الأعمال في مراكز البيانات لمواجهة الكوارث الطبيعية والبشرية والحوادث العرضية، وذلك من خلال تطبيق استراتيجيات فعالة تضمن استمرارية العمليات واستعادة الخدمات الحيوية في حال وقوع الأزمات. ركزت الدراسة على عملية إعداد خطة استمرارية الأعمال لمراكز البيانات، وتناولت عناصر إدارة استمرارية الأعمال بما في ذلك تطوير الاستراتيجية، والاستعداد، والتخفيف من المخاطر، والتدريب، والاستجابة، والتعافي، كما ناقشت استراتيجيات استمرارية الأعمال في بنى مراكز البيانات المعتمدة على خدمات الاستضافة المشتركة (Colocation) والحوسبة السحابية (Cloud-based architectures). استخدمت الدراسة المنهج التحليلي التطبيقي بالاعتماد على تحليل منهجيات واستراتيجيات إدارة المخاطر واستمرارية الأعمال في بيئات مراكز البيانات. وتوصلت نتائج الدراسة إلى أن تطبيق منهجيات استمرارية الأعمال يسهم في تعزيز جاهزية مراكز البيانات واستدامة خدماتها خلال الأزمات، ويقلل من أثر الانقطاعات التشغيلية. كما أوصت الدراسة بـ استخدام منهجية المتوسط المرجح المرتب (OWA) لإدماج ملف المخاطر الخاص بصانع القرار ضمن عمليات التخطيط واتخاذ القرار المتعلقة باستمرارية الأعمال في مراكز البيانات، بما يعزز من كفاءة الاستجابة وسرعة التعافي واستقرار الخدمات الحيوية للمؤسسات.

هدفت الدراسة إلى التعرف على دور كل من إدارة استمرارية الأعمال وإدارة المخاطر في تعزيز استدامة الأعمال من خلال ضمان انسيابية العمليات التشغيلية ورفع جاهزية المؤسسات لمواجهة المواقف غير المتوقعة. تناولت الدراسة إدارة استمرارية الأعمال بوصفها إطارًا منظمًا لبناء استدامة مؤسسية قادرة على الاستجابة الفعالة للأزمات وحماية مصالح أصحاب المصلحة والأنشطة الرئيسة التي تسهم في خلق القيمة للمؤسسة. كما أوضحت أن تعطل الأنشطة الحيوية للمؤسسة قد يؤدي إلى أزمات مالية وتشغيلية قد تصل إلى الإفلاس في حال غياب أنظمة استمرارية الأعمال. اعتمدت الدراسة المنهج التحليلي الوصفي من خلال تحليل العلاقة بين إدارة استمرارية الأعمال وإدارة المخاطر وتأثيرهما على جاهزية المؤسسة

واستدامة عملياتها. وتكونت عينة الدراسة من مجموعة من المؤسسات التي تطبق أنظمة إدارة المخاطر واستمرارية الأعمال بهدف الوقوف على ممارساتها الوقائية والتكيفية. وتوصلت النتائج إلى أن التكامل بين إدارة استمرارية الأعمال وإدارة المخاطر يسهم في رفع قدرة المؤسسات على التنبؤ بالمخاطر والتعامل معها بسرعة وكفاءة، مما يضمن استمرارية العمليات وتحقيق استدامة أكبر في الأداء المؤسسي. وأوصت الدراسة بضرورة تعزيز الوعي المؤسسي بأهمية استمرارية الأعمال، وتبني أساليب وقائية واستباقية تعتمد على التحليل الدوري للمخاطر، وتطوير إجراءات مرنة تُمكن المؤسسات من التكيف مع التغيرات البيئية المفاجئة وضمان استقرار عملياتها الحيوية..

دراسة (Zhang et al., 2021) 

هدفت الدراسة إلى التعرف على نموذج تصنيف مخاطر استمرارية الأعمال في مراكز البيانات ضمن بيئة الحوسبة السحابية، والذي يهدف إلى تحديد مستوى القدرة على التعافي من الكوارث لأنظمة الأعمال المستهدفة استنادًا إلى معلومات خصائص النظام، والمستوى الأساسي الشامل، ودورة حياة النظام، والعائد على الاستثمار. استخدمت الدراسة المنهج التحليلي التطبيقي من خلال بناء نموذج يعتمد على تقييم قدرة النظام على الصمود والتعافي لتحديد نمط الحماية المناسب لاستمرارية الأعمال في بيئة سحابية. وتكونت عينة الدراسة من أنظمة أعمال مختلفة ضمن مراكز بيانات قائمة على السحابة بهدف اختبار كفاءة النموذج المقترح. وتوصلت النتائج إلى أن تطبيق نموذج تصنيف المخاطر المقترح يسهم في تحسين عملية اتخاذ القرار الخاصة بتحديد آليات حماية الأنظمة الحيوية وضمان استمراريته التشغيلية وفق مستوى قدرتها على التعافي من الكوارث. وأوصت الدراسة باعتماد نموذج تصنيف مخاطر استمرارية الأعمال كأداة استراتيجية في إدارة مراكز البيانات السحابية لتعزيز مرونتها التشغيلية وتقليل الخسائر الناتجة عن الأعطال أو الكوارث المحتملة.

دراسة (Akhamere, 2023) 

هدفت الدراسة إلى التعرف على أطر إدارة المخاطر التي تسهم في تعزيز مرونة سلاسل الإمداد وضمان استمرارية الأعمال خلال الأزمات العالمية، من خلال دمج عمليات التعرف الاستراتيجي على

المخاطر، ومبادئ إدارة المخاطر المؤسسية (ERM)، واستراتيجيات التخفيف، والتمكين التكنولوجي لتعزيز الرؤية واتخاذ القرار في الوقت الفعلي. استخدمت الدراسة المنهج التحليلي الوصفي بالاعتماد على تحليل المفاهيم والأسس التشغيلية لأطر إدارة المخاطر المصممة لزيادة مرونة سلاسل التوريد. وتناولت الدراسة أهمية تحديد المخاطر الاستراتيجية، ورسم خرائط الهشاشة، واستخدام اختبارات الضغط بالسيناريوهات للكشف عن نقاط الضعف المحتملة في الشبكات العالمية للإمداد، كما تناولت دور مبادئ إدارة المخاطر المؤسسية وفق معايير COSO ERM و ISO 31000 في دمج مخاطر سلسلة الإمداد ضمن الحوكمة المؤسسية وضمان توافقها مع الأهداف الاستراتيجية ومتطلبات الامتثال. وأكدت الدراسة على أهمية استراتيجيات التخفيف مثل تنويع الموردين، ومرونة النقل، وتخزين المخزون الاحتياطي، وتعزيز الأمن السيبراني، وتوفير الضمانات المالية من خلال التأمين والحماية التعاقدية، إلى جانب أهمية خطط استمرارية الأعمال (BCP) وبروتوكولات إدارة الأزمات للحفاظ على العمليات أثناء الاضطرابات من خلال إعادة توزيع الموارد وتعديل العمليات بسرعة. وتوصلت النتائج إلى أن دمج التقنيات الحديثة مثل التحليلات التنبؤية، والذكاء الاصطناعي، وإنترنت الأشياء، وتقنيات البلوك تشين، والمنصات السحابية يعزز من شفافية سلسلة الإمداد وقدرتها على اتخاذ قرارات تكيفية آنية. وأوصت الدراسة باعتماد أطر إدارة مخاطر متكاملة تجمع بين الإدارة الاستراتيجية، والضمانات التشغيلية، والتمكين التكنولوجي، وآليات الحوكمة لتحقيق مرونة واستدامة أعلى في سلاسل الإمداد العالمية، والحفاظ على استمرارية الأعمال والميزة التنافسية وثقة أصحاب المصلحة في بيئة عالمية متقلبة..

دراسة (Levy, 2020) 🌈

هدفت الدراسة إلى التعرف على إطار مقترح لتقييم مخاطر مواقع مراكز البيانات، والذي يهدف إلى توحيد عملية تقييم المخاطر الخارجية من خلال تحديدها وتحليلها وتقييمها بطريقة كمية ومعيارية تسمح بإجراء مقارنات دقيقة بين المواقع المختلفة. استخدمت الدراسة المنهج التحليلي التطبيقي لتطوير منهجية منظمة لتقييم مخاطر مراكز البيانات بوصفها أداة مهمة في عمليات التدقيق والفحص الفني (Due Diligence). ويتألف الإطار المقترح من ثلاث مراحل رئيسية هي: تحديد المخاطر، تحليل المخاطر، وتقييم المخاطر. كما يتضمن التحليل استخدام مؤشر مرونة البنية التحتية وتقييم رقمي لموقع مركز

البيانات (Data Center Site Risk Metric) لقياس مستوى المخاطر المرجح، بالاعتماد على معايير معترف بها وممارسات مثلى وخبرة متخصصة. وتوصلت نتائج الدراسة إلى أن تطبيق الإطار المقترح يسهم في تحسين فهم وتوصيل المخاطر المتعلقة بمواقع مراكز البيانات، وتسهيل عملية تقييم استراتيجيات التخفيف من المخاطر للوصول إلى المستوى المطلوب من الأمان والاستدامة التشغيلية. وأوصت الدراسة بـ اعتماد هذا الإطار كأداة قياسية في عمليات تقييم واختيار مواقع مراكز البيانات، وتعزيزه ببيانات تحليلية محدثة لضمان اتخاذ قرارات مبنية على تقييم شامل ومدرّوس للمخاطر المحتملة..

دراسة (Denny & Myneni, 2025) 🌈

هدفت الدراسة إلى التعرف على إطار متكامل لإدارة المخاطر في مراكز البيانات فائقة النطاق (Hyperscale Data Centres) في الهند، وذلك من خلال معالجة المخاطر التي تواجه مراحل الإنشاء والتشغيل عبر منهجية منظمة وشاملة تسهم في تعزيز الأداء طويل المدى والمرونة التشغيلية لهذه المراكز. استخدمت الدراسة المنهج التحليلي التطبيقي لتطوير نموذج متكامل يحدد ويقيم ويصنّف أولويات المخاطر الرئيسية في جميع المراحل الحرجة من تصميم الموقع وتجهيزه مروراً بمرحلة التشغيل المستمر. وتناولت الدراسة مجموعة من القضايا مثل تأخر الامتثال التنظيمي، والإخفاقات التقنية، وضعف التنسيق بين الجهات المعنية، والحساسية البيئية للمواقع. كما ركزت على تبني نهج مترابط يتجاوز الأساليب الجزئية وقوائم الفحص التقليدية، من خلال توظيف أدوات بصرية وتحليلية تعزز وضوح عملية التقييم وتدعم التخطيط للاستجابة الفعالة للمخاطر. وتوصلت نتائج الدراسة إلى أن الإطار المقترح يمثل نموذجاً هيكلياً قابلاً للتوسع، يساعد أصحاب المصلحة من مطورين واستشاريين ومشغلين ومخططين على اتخاذ قرارات مستنيرة وتحسين الجاهزية وضمان تنفيذ مشاريع مراكز البيانات بكفاءة واستدامة. وأوصت الدراسة بـ تطبيق الإطار المتكامل كأداة معيارية لإدارة المخاطر في مشاريع المراكز فائقة النطاق، وتطوير قدرات التحليل البصري والتكامل بين الأطراف المعنية لتعزيز المرونة التشغيلية وجودة البنية التحتية الرقمية في الهند..

هدفت الدراسة إلى التعرف على استراتيجيات تعزيز المرونة في إطار إدارة استمرارية الأعمال (BCM) من خلال تطبيق نهج شامل يدمج بين تقييم المخاطر، والتخطيط الاستراتيجي، والتدريب، بهدف ضمان استدامة العمليات التشغيلية في مواجهة التحديات المتغيرة. استخدمت الدراسة المنهج التحليلي الوصفي المقارن مدعومًا بدراسات حالة توضح النجاحات والإخفاقات في تطبيق إدارة استمرارية الأعمال عبر قطاعات مختلفة. وركزت على أن إدارة استمرارية الأعمال تمثل نهجًا تكامليًا لتحديد التهديدات والتخفيف من آثارها وضمان استمرارية العمل خلال الاضطرابات، مع تأكيد أهمية دمج مفاهيم المرونة المؤسسية في الثقافة التنظيمية. وتناولت الدراسة العناصر الجوهرية في استمرارية الأعمال، مثل تقييم المخاطر، والتخطيط الاستراتيجي، والممارسات التدريبية، واستراتيجيات المرونة، مبينة أن تكامل هذه العناصر يساهم في تعزيز الجاهزية التنظيمية والقدرة على التكيف مع الأزمات. وتوصلت النتائج إلى أن الإطار المقترح يوفر نموذجًا مرئيًا وقابلًا للتكيف مع التهديدات المستجدة، بما يضمن استمرارية العمليات ويدعم المرونة طويلة المدى في قطاعات متعددة مثل التمويل والرعاية الصحية والصناعة والتعليم. وأوصت الدراسة بضرورة تبني استراتيجيات مخصصة لكل قطاع، والاستفادة من التقنيات المتقدمة مثل الذكاء الاصطناعي وتقنية البلوك تشين، وتعزيز برامج التدريب والتحديث المستمر لخطط استمرارية الأعمال لمواجهة التحديات المستقبلية بكفاءة وفعالية..

هدفت الدراسة إلى التعرف على نموذج التقييم الشامل للمخاطر (Comprehensive Risk Evaluation Model - CREM) المقترح، والذي يهدف إلى تقييم مخاطر أمن مراكز البيانات بصورة منهجية وشاملة من خلال إطار عمل ديناميكي وتكراري يعزز من الممارسات الأمنية والتخفيف الاستباقي للمخاطر. استخدمت الدراسة المنهج التحليلي التطبيقي الذي اعتمد على مراجعة أدبية شاملة، وتحليل المفاهيم الأساسية، وتطوير بنية نموذجية لتقييم المخاطر تغطي الثغرات القائمة في منهجيات التقييم التقليدية. ويتكون النموذج المقترح من مجموعة من الوحدات المترابطة تشمل تحديد مصادر التهديد، تحليل أحداث

التهديد، تقييم المخاطر، فحص الثغرات الأمنية، تحليل تأثير المخاطر، تحديد مستوى التهديد، وتقييم فعالية الضوابط الأمنية. ويتميز النموذج بآلية تكرارية ديناميكية تتيح التحديث المستمر للبيانات والتحليل الآني للتهديدات لتقليل نقاط الضعف وتحسين الاستجابة الأمنية. وتوصلت نتائج الدراسة إلى أن تطبيق نموذج CREM يساهم في رفع كفاءة أمن مراكز البيانات من خلال تعزيز القدرة على اكتشاف التهديدات والتعامل معها بشكل استباقي قبل تحولها إلى حوادث مؤثرة. وأوصت الدراسة باعتماد نموذج CREM كأداة معيارية لتقييم وإدارة مخاطر أمن مراكز البيانات، وتكامل وحداته ضمن منظومات المراقبة والتحكم الأمني المؤسسية لضمان حماية البيانات الحساسة واستدامة العمليات الرقمية.

8.1 الفجوة البحثية:

أظهرت الدراسات السابقة اتفاقاً واسعاً حول أهمية إدارة المخاطر واستمرارية الأعمال بوصفهما ركيزتين أساسيتين لاستدامة المؤسسات في بيئات معقدة ومتغيرة. فقد أكدت دراسات مثل Mošková & Bugarová (2023) وJain & Mitra (2025) وAkhamere (2023) أن التكامل بين إدارة المخاطر واستمرارية الأعمال يعزز مرونة المؤسسات وقدرتها على الصمود أمام الأزمات، كما أجمعت دراسات أخرى مثل Yang (2023) وLee & Levy (2020) وHussaini & Raharjo (2024) على ضرورة تطوير أطر علمية ومنهجيات معيارية لتقييم المخاطر في مراكز البيانات بما يضمن دقة التقدير وفاعلية الاستجابة. وتشترك الدراسة الحالية مع هذه الدراسات في تأكيدها على أهمية الإدارة الوقائية والتكامل بين الجوانب الفنية والإدارية لضمان استمرارية الخدمات الحيوية، وكذلك في تبنيها لمنهج وصفي تحليلي يستند إلى بيانات ميدانية للتحقق من العلاقة بين إدارة المخاطر واستمرارية الأعمال.

في المقابل، تختلف الدراسة الحالية عن الدراسات السابقة من حيث نطاق التطبيق والسياق المؤسسي والبعد التحليلي للعلاقة بين المتغيرين؛ إذ ركزت معظم الدراسات الأجنبية على الجوانب التقنية البحتة لإدارة المخاطر دون الربط المباشر باستمرارية الأعمال، بينما ركزت الدراسات العربية على قطاعات عامة أو خدمية دون تناول بيئة مراكز البيانات التي تمثل قلب التحول الرقمي في المؤسسات التقنية. ومن هنا جاءت خصوصية هذه الدراسة في تحليل أثر إدارة مخاطر مراكز البيانات بأبعادها (تحديد، تحليل،

تقييم، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض، بما يسد فجوة معرفية وتطبيقية في الأدبيات العربية ويقدم نموذجًا تكامليًا يعكس الخصوصية التنظيمية والتقنية لبيئة مراكز البيانات السعودية.

9.1 المنطلقات النظرية للدراسة:

تُعد إدارة المخاطر في مراكز البيانات من الركائز الأساسية التي تقوم عليها منظومة الحوكمة التقنية في المؤسسات الحديثة، خاصة في ظل الاعتماد المتزايد على البيانات كمورد استراتيجي لعمليات اتخاذ القرار واستمرارية الأعمال. فمراكز البيانات لم تعد مجرد بنية تحتية لتخزين المعلومات، بل أصبحت تمثل نظامًا متكاملًا لإدارة المعرفة والتشغيل والإنتاجية الرقمية، ما يجعلها عرضةً لمجموعة واسعة من المخاطر التشغيلية والتقنية التي يمكن أن تؤثر على كفاءة واستمرارية الخدمات المقدمة. وقد أكدت الأدبيات الحديثة أن إدارة المخاطر (Risk Management) واستمرارية الأعمال (Business Continuity Management – BCM) تمثلان منظومتين متكاملتين تهدفان إلى تحقيق هدف مشترك هو ضمان استدامة الأداء المؤسسي في مواجهة الأزمات والاضطرابات [Mošková & Bugarová, 2023].

أولاً: إدارة مخاطر مراكز البيانات

تشير إدارة مخاطر مراكز البيانات إلى مجموعة من العمليات والإجراءات المنهجية التي تهدف إلى تحديد وتقييم وتحليل المخاطر المحتملة التي قد تؤثر على البنية التحتية للمركز أو على البيانات والأنظمة التي يستضيفها، ومن ثم تطوير استراتيجيات لمعالجتها أو الحد من أثارها. وقد أوضح Levy (2020) أن إدارة المخاطر في مراكز البيانات تتطلب إطارًا معياريًا يساعد على توحيد عمليات التقييم بين المواقع المختلفة، مما يسهل اتخاذ قرارات دقيقة بشأن استراتيجيات التخفيف وتحسين الكفاءة التشغيلية.

ويرى Hussaini & Raharjo (2024) أن مراكز البيانات تواجه مخاطر معقدة ذات طابع ديناميكي ومتغير تتعلق بالأمن السيبراني، وفشل الأجهزة، وانقطاع الطاقة، وسوء إدارة الموارد، مما يستلزم تبني نموذج شامل مثل Comprehensive Risk Evaluation Model (CREM) الذي يقوم على التحليل التكراري

والديناميكي للتهديدات من خلال وحدات مترابطة تشمل تحديد مصادر التهديد، وتحليل الأحداث، وتقييم المخاطر، وفحص الثغرات الأمنية، وتحليل التأثير، وتقييم فعالية الضوابط الأمنية. ويتيح هذا النموذج تحديثاً مستمراً لقواعد البيانات وتحليلاً أنيماً للتهديدات، بما يعزز الاستجابة الاستباقية ويقلل من احتمالية وقوع الكوارث التشغيلية.

ومن حيث البنية الإدارية، تتضمن إدارة مخاطر مراكز البيانات أربعة أبعاد رئيسة تمثل مراحل متابعة ومتكاملة:

1. تحديد المخاطر (Risk Identification): وهي الخطوة التي يتم فيها تحديد مصادر التهديد المحتملة داخل بيئة مركز البيانات، سواء كانت تقنية أو بشرية أو بيئية. ويؤكد Yang & Lee (2023) أن دقة تحديد المخاطر تعتمد على فهم شامل للأصول الحرجة في المركز، وفترة تحقيق أهداف الاستمرارية، إذ إن تجاهل هذه الفترة يؤدي إلى ضعف في دقة ترتيب أولويات المخاطر.
2. تحليل المخاطر (Risk Analysis): في هذه المرحلة يتم تقدير احتمالية حدوث كل خطر وشدة تأثيره على العمليات. ويرى Denny & Myneni (2025) أن التحليل يجب أن يجمع بين البعدين الفني والاقتصادي، بحيث يشمل تقدير الخسائر التشغيلية والعائد المتوقع من إجراءات الوقاية.
3. تقييم المخاطر (Risk Evaluation): تهدف إلى المقارنة بين مستويات المخاطر المقبولة وغير المقبولة وتحديد أولويات المعالجة. وقد طور Levy (2020) مؤشراً رقمياً لقياس المخاطر المرجحة لمواقع مراكز البيانات اعتماداً على معايير البنية التحتية والممارسات المثلى.
4. معالجة المخاطر (Risk Treatment): تشمل وضع وتنفيذ الإجراءات الوقائية أو التصحيحية، مثل تحديث أنظمة النسخ الاحتياطي، وتطبيق سياسات أمنية صارمة، أو تحويل بعض المخاطر إلى أطراف أخرى مثل شركات التأمين. وقد أوضح Akhamere (2023) أن معالجة المخاطر تتطلب تكاملاً بين البنية التحتية المادية والأنظمة الرقمية والأطر الحاكمة لتقليل احتمالية الاضطرابات التشغيلية. ويُعد نجاح إدارة مخاطر مراكز البيانات نتاجاً لتفاعل هذه الأبعاد ضمن دورة مستمرة من المراقبة والتحسين والتعلم التنظيمي، إذ أن الخطر في بيئة تقنية عالية التغير ليس حالة ثابتة بل ظاهرة متحركة تستلزم مراجعة دورية للأنظمة والسياسات بما يواكب التغيرات في بيئة العمل والتكنولوجيا المستخدمة.

ثانيًا: استمرارية الأعمال

تُعرف إدارة استمرارية الأعمال (Business Continuity Management) بأنها عملية إدارية شاملة تهدف إلى تحديد التهديدات المحتملة التي يمكن أن تواجه المؤسسة، وتقييم تأثيرها على العمليات الحيوية، ووضع خطط وإجراءات لضمان استمرار الأنشطة الأساسية أثناء وبعد الأزمات. وقد أوضحت Jain & Mitra (2025) أن إدارة استمرارية الأعمال تمثل تحولًا من مجرد خطة استجابة للطوارئ إلى إطار استراتيجي متكامل يضم التخطيط، والتدريب، والاختبار، والتقييم الدوري. كما أكدت Mošková & Bugarová (2023) أن استمرارية الأعمال أصبحت أداة حوكمة مؤسسية تهدف إلى حماية مصالح أصحاب المصلحة وضمان تدفق العمليات الحيوية، بما يعزز استدامة الأداء المؤسسي على المدى الطويل.

وتقوم فلسفة استمرارية الأعمال على ثلاثة مبادئ رئيسية:

1. الاستباقية: أي الاستعداد المسبق لتحديد المخاطر ووضع خطط بديلة قبل وقوعها.
 2. الاستجابة: أي تنفيذ الإجراءات المحددة لمواجهة الأزمة عند وقوعها لضمان استمرار العمليات الأساسية.
 3. التعافي: أي استعادة الأنشطة والأنظمة إلى وضعها الطبيعي في أقصر وقت ممكن.
- ويشير Sagi (2024) إلى أن دمج مفهوم المرونة في البنية التحتية لقواعد البيانات ومراكز المعلومات يُعد أحد أهم عوامل استمرارية الأعمال، إذ يُمكن المؤسسات من استعادة الخدمات دون انقطاع حتى أثناء حالات الفشل أو الأعطال الكبرى.

ويرتبط نجاح استمرارية الأعمال بمدى فاعلية تحليل تأثير الأعمال (Business Impact Analysis - BIA) الذي يحدد أولويات العمليات الحرجة واحتياجاتها من الموارد. وقد بينت Zhang et al (2021) أن تحديد القدرة على التعافي من الكوارث (Disaster Recovery Capability Level) يمثل مقياسًا أساسيًا لتصنيف أنظمة الأعمال وضمان استمراريته التشغيلية وفقًا لمستوى مرونتها. كما أكد Denny & Myneni

(2025) أن استمرارية الأعمال في مراكز البيانات تتطلب إدارة متكاملة تشمل مرحلي الإنشاء والتشغيل لتقليل الأخطاء التقنية والارتباك التنظيمي أثناء الأزمات.

ثالثاً: العلاقة بين إدارة المخاطر واستمرارية الأعمال

تؤكد الأدبيات على وجود علاقة تكاملية بين إدارة المخاطر واستمرارية الأعمال، حيث تمثل إدارة المخاطر الأساس الوقائي الذي يُمكن المؤسسة من الاستعداد لمواجهة الأزمات، بينما تمثل استمرارية الأعمال الإطار التنفيذي الذي يضمن استمرار العمليات عند وقوعها. وقد أوضح Yang & Lee (2023) أن تجاهل فترة تحقيق أهداف الاستمرارية ضمن تقييم المخاطر يؤدي إلى ضعف في كفاءة التخطيط الوقائي، بينما أكدت Mošková & Bugarová (2023) أن التكامل بين المنهجين يسهم في بناء مؤسسات أكثر استدامة وقدرة على التكيف مع الأزمات.

وفي السياق ذاته، أشار Akhamere (2023) إلى أن أطر إدارة المخاطر المتكاملة التي تستند إلى معايير مثل COSO ERM و ISO 31000 تشكل قاعدة أساسية لتطبيق معايير ISO 22301 الخاصة باستمرارية الأعمال، مما يعزز الترابط بين الممارسات الوقائية والتخطيط للتعافي. أما Hussaini & Raharjo (2024) فقد بينا أن النماذج التكرارية الديناميكية في إدارة المخاطر مثل CREM تسهم في تحديث مستمر لخطط الاستمرارية بناءً على البيانات اللحظية حول التهديدات المكتشفة.

وفي بيئة مراكز البيانات تحديداً، يُعد التكامل بين إدارة المخاطر واستمرارية الأعمال ضرورة تشغيلية وليس خياراً تنظيمياً، إذ إن أي خلل بسيط في النظام يمكن أن يؤدي إلى انقطاع الخدمة أو فقدان البيانات بما يترتب عليه خسائر مالية وسمعة مؤسسية جسيمة. وقد أكد Sagi (2024) على أن المؤسسات التي تدمج اختبارات الفشل وأنظمة المرونة في تصميم قواعد البيانات تحقق مستويات أعلى من الاستقرار التشغيلي مقارنة بتلك التي تعتمد أساليب تقليدية في إدارة المخاطر.

10.1 المنهجية وطرق البحث:

اعتمدت الدراسة على المنهج الوصفي التحليلي، نظرًا لملاءمته لطبيعة البحث وأهدافه. فالمنهج الوصفي التحليلي يُستخدم لدراسة الظواهر كما هي في الواقع بهدف وصفها وصفًا دقيقًا، ومن ثم تحليل العلاقات والارتباطات بين متغيراتها واستخلاص النتائج، ويُعد هذا المنهج مناسبًا للدراسات الإدارية والتقنية التي تهدف إلى الكشف عن أثر متغيرات محددة في ظواهر تنظيمية أو تشغيلية . وقد استخدم الباحث هذا المنهج لتوصيف مستوى تطبيق إدارة مخاطر مراكز البيانات في المؤسسات التقنية، وتحليل أثرها الإحصائي على مستوى استمرارية الأعمال، بما يساهم في بناء تصور علمي وعملي متكامل للظاهرة محل الدراسة.

11.1 مصادر جمع البيانات

اعتمدت الدراسة على نوعين رئيسيين من مصادر جمع البيانات، هما المصادر الأولية والمصادر الثانوية، وذلك لتحقيق تكامل بين الجانبين النظري والتطبيقي وضمان شمولية المعلومات ودقتها.

☑ المصادر الأولية:

تمثلت في البيانات الميدانية التي جمعها الباحث من أفراد عينة الدراسة مباشرة باستخدام أداة الاستبانة المصممة خصيصًا لأغراض البحث. وقد شملت هذه البيانات استجابات العاملين في مراكز البيانات بالمؤسسات التقنية بمدينة الرياض حول متغيرات الدراسة، وهي: أبعاد إدارة مخاطر مراكز البيانات (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر)، ومستوى استمرارية الأعمال في مؤسساتهم. وتم جمع البيانات خلال فترة امتدت لثلاثة أسابيع لضمان تمثيل كافٍ وشامل لجميع الفئات المستهدفة.

☑ المصادر الثانوية:

تمثلت في المراجع العلمية والدراسات السابقة ذات الصلة بموضوع البحث، سواء العربية أو الأجنبية، التي تناولت مفاهيم إدارة المخاطر، وإدارة مراكز البيانات، واستمرارية الأعمال، مثل دراسات Levy (2020)، وHussaini & Raharjo (2024)، وMošková & Bugarová (2023)، وYang & Lee (2023)، وJain & Mitra (2025). وقد ساعدت هذه الدراسات في بناء الإطار النظري للدراسة وصياغة الفرضيات وتطوير فقرات أداة البحث وتحديد أبعاد المتغيرات بشكل منهجي.

12.1 حدود الدراسة:

- حدود موضوعية: تقتصر الدراسة على أثر إدارة مخاطر مراكز البيانات بأبعادها مجمعة والمتمثلة في (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية على مراكز بيانات في مدينة الرياض.
- حدود مكانية: تُجرى الدراسة على مراكز بيانات في مدينة الرياض.
- حدود زمنية: تم إعداد الدراسة في عام 2025.
- حدود بشرية: تقتصر الحدود البشرية لهذه الدراسة على العاملين في مراكز بيانات في مدينة الرياض.

الفصل الثاني: الإطار النظري

المبحث الأول: إدارة مخاطر مراكز البيانات

1.1.2 التمهيد

أصبحت مراكز البيانات في العصر الحديث تمثل العمود الفقري للبنية التحتية الرقمية للمؤسسات التقنية، إذ تُعد البيئة التشغيلية التي تُخزّن فيها البيانات وتُعالج وتُنقل عبر شبكات مترابطة تمكّن المؤسسات من أداء وظائفها الحيوية واستدامة عملياتها. ومع التوسع في التحول الرقمي، وتنامي حجم البيانات، وتزايد الاعتماد على الخدمات السحابية، تصاعدت في المقابل المخاطر المرتبطة بعمليات مراكز البيانات، سواء كانت تقنية أو أمنية أو تشغيلية أو بيئية.

تُعرّف مراكز البيانات بأنها منظومات متكاملة تتألف من مكونات مادية وبرمجية تشمل الخوادم (Servers)، وأنظمة التخزين، وشبكات الاتصال، وأنظمة التبريد والطاقة، والبنى التحتية الداعمة الأخرى، وتُدار وفق معايير محددة تضمن استمرارية عملها دون انقطاع. هذه المكونات، على الرغم من دقتها التقنية، تُعدّ نقاطاً محتملة للتعطّل أو التهديد إذا لم تُدار وفق إطار مؤسسي متكامل لإدارة المخاطر.

لقد باتت إدارة مخاطر مراكز البيانات (Data Center Risk Management) جزءاً لا يتجزأ من حوكمة المؤسسات التقنية، كونها تمثل المنظومة التي تهدف إلى التعرف على المخاطر المحتملة، وتحليلها، وتقييم آثارها، ووضع استراتيجيات لمعالجتها أو الحد منها. فكل خطر غير مُدار يمكن أن يؤدي إلى توقف العمليات الرقمية أو فقدان بيانات حساسة أو تدهور في موثوقية الخدمات. ومن هنا، برزت أهمية تطوير أطر ومنهجيات لإدارة المخاطر تراعي خصوصية بيئة مراكز البيانات، بما في ذلك بنيتها التقنية المعقدة، وتفاعلها مع الأنظمة السحابية، واعتمادها على البنية التحتية للطاقة والاتصال.

تُشير الأدبيات الحديثة في هذا المجال إلى أن إدارة مخاطر مراكز البيانات لم تعد تقتصر على الجوانب الأمنية أو التقنية فحسب، بل أصبحت ترتبط بالاستراتيجية المؤسسية العامة، وتتكامل مع نظم

إدارة استمرارية الأعمال (Business Continuity Management – BCM) لضمان مرونة تشغيلية مستدامة. ويُعدّ هذا التكامل من أهم المداخل الحديثة في إدارة المؤسسات التقنية المعاصرة، حيث يتم الانتقال من مفهوم “الاستجابة للمخاطر” إلى مفهوم “الاستباق والوقاية”، عبر نماذج تقييمية كمية ونوعية متقدمة، مثل النموذج الشامل لتقييم المخاطر (Comprehensive Risk Evaluation Model – CREM) الذي يُعتمد في بيئات مراكز البيانات ذات الأهمية العالية، وكذلك الأطر المستندة إلى معيار ISO 31000 التي تركز على استمرارية العمليات في مواجهة التهديدات المتغيرة.

إن هذا التطور في المفهوم جعل من إدارة المخاطر عملية ديناميكية تتطلب مراقبة مستمرة وتحديثاً متواصلاً لأساليب التقييم والاستجابة، بالاستناد إلى بيانات واقعية وأدوات تحليل متقدمة مثل الذكاء الاصطناعي، والتحليلات التنبؤية، والتعلم الآلي. وبهذا أصبحت إدارة المخاطر في مراكز البيانات ليست فقط آلية للحماية، بل أداة استراتيجية تدعم اتخاذ القرار، وتعزز ثقة العملاء، وتؤكد على التزام المؤسسة بالحوكمة الرقمية المستدامة.

3.1.2 مفهوم إدارة مخاطر مراكز البيانات

تعددت تعريفات الباحثين لمفهوم إدارة مخاطر مراكز البيانات (Data Center Risk Management) تبعاً لاختلاف مناهجهم واتجاهاتهم الفكرية، إلا أنها تتقاطع جميعاً في تأكيدها على كونها عملية منهجية تهدف إلى حماية استقرار البنية التحتية الرقمية وضمان استمرارية العمليات التقنية.

يُشير Levy (2020) إلى أن إدارة مخاطر مراكز البيانات تمثل "إطاراً تحليلياً يهدف إلى تحديد وتقييم المخاطر الخارجية والداخلية التي قد تؤثر في الموقع التشغيلي لمركز البيانات، وذلك لتقدير مستوى المخاطر الكلي واتخاذ الإجراءات الوقائية المناسبة للحد من أثارها".

أما Hussaini و (2024) Raharjo فقد وسّعا نطاق المفهوم من خلال تقديم النموذج الشامل لتقييم المخاطر (Comprehensive Risk Evaluation Model – CREM)، والذي عرّف إدارة مخاطر مراكز البيانات بأنها "عملية ديناميكية تكرارية (Iterative Process) تقوم على تحديد مصادر التهديد وتحليل

الأحداث وتقييم مستويات الخطورة، مع دمج آليات المراقبة المستمرة والتقييم الدوري للضوابط الأمنية لضمان الحماية الشاملة واستدامة الأداء".

وفي السياق نفسه، عرّف Denny و Myneni (2025) إدارة مخاطر مراكز البيانات بأنها "إطار متكامل لإدارة المخاطر يغطي مرحلتي الإنشاء والتشغيل لمراكز البيانات فائقة النطاق (Hyperscale Data Centres)، ويعتمد على منهجية منهجية شمولية تجمع بين التقييم الكمي والتحليل البصري لدعم اتخاذ القرار في الوقت الفعلي".

من ناحية أخرى، يرى Zhang وآخرون (2021) أن إدارة مخاطر مراكز البيانات في بيئات الحوسبة السحابية تمثل "آلية لتصنيف وتقييم قدرات التعافي من الكوارث (Disaster Recovery Capabilities) لأنظمة الأعمال المستضافة سحابيًا، استنادًا إلى خصائص النظام ودورة حياته والعائد على الاستثمار".

كما أشار العنزي وآخرون (2024) إلى أن إدارة المخاطر في المؤسسات التقنية ومن ضمنها مراكز البيانات – هي "مجموعة من الأنشطة المنهجية التي تهدف إلى التعرف على المخاطر التي تهدد نجاح المشروع وتحليلها وتحديد أولوياتها ووضع الاستراتيجيات المناسبة لمعالجتها بما يتوافق مع أهداف المؤسسة".

ووفقًا لما طرحه العلوان والحياصات (2022) فإن إدارة المخاطر في البيئات التقنية والهندسية هي "نظام متكامل يقوم على الدمج بين الأساليب الكمية والكيفية لتقدير احتمالية وقوع المخاطر وتأثيرها على جودة المشروع، بهدف تعزيز كفاءة الأداء وضمان الاستدامة التشغيلية".

في ضوء ما سبق، يرى الباحث أن إدارة مخاطر مراكز البيانات تمثل منظومة استراتيجية متكاملة تتجاوز المفهوم التقليدي لإدارة المخاطر القائم على الاستجابة إلى مفهوم الاستباق والتنبؤ، بحيث تتضمن سلسلة من العمليات المنظمة التي تبدأ بتحديد مصادر الخطر، مرورًا بتحليلها وتقييمها، وانتهاءً بمعالجتها ومتابعتها ضمن إطار مستمر من التحسين.

4.1.2 أهمية إدارة مخاطر مراكز البيانات

تُعد إدارة مخاطر مراكز البيانات من الموضوعات المحورية في بيئة الأعمال الرقمية المعاصرة، لما لها من دور أساسي في حماية البنية التحتية للمؤسسات وضمان استمرارية العمليات التقنية دون انقطاع. فمع تزايد الاعتماد على البيانات في جميع الأنشطة المؤسسية، أصبحت مراكز البيانات تمثل القلب النابض الذي تُبنى عليه القدرات التشغيلية، وأي خلل أو تهديد فيها يمكن أن يؤدي إلى خسائر مالية وتشغيلية جسيمة، فضلاً عن التأثير على السمعة المؤسسية وثقة العملاء. ومن هنا، تتجلى أهمية إدارة مخاطر مراكز البيانات بوصفها أداة استراتيجية تهدف إلى الوقاية من الأزمات، وضمان استدامة الأداء، وتعزيز مرونة الأنظمة التقنية.

ويشير Hussaini و (2024) Raharjo إلى أن أهمية إدارة مخاطر مراكز البيانات تتمثل في ثلاثة محاور رئيسية:

1. حماية استمرارية العمليات الحيوية: (Operational Continuity Protection) إذ تمثل إدارة المخاطر خط الدفاع الأول الذي يضمن استمرار الأنظمة الحرجة في العمل حتى في ظل الأزمات التقنية أو الأمنية، من خلال اعتماد آليات التقييم المستمر والضوابط الوقائية التي تقلل احتمالية الانقطاع.
2. تعزيز موثوقية الأنظمة: (System Reliability Enhancement) حيث تساهم في بناء بيئة تشغيلية مستقرة من خلال تحديد الثغرات التقنية وتطبيق ضوابط التحكم المناسبة لضمان استقرار البنية التحتية.
3. التحسين المستمر للأداء الأمني: (Continuous Security Improvement) وذلك عبر تحديث السياسات والإجراءات بصورة تكرارية استناداً إلى التغيرات في بيئة التهديدات، مما يجعل إدارة المخاطر عملية ديناميكية تتطور مع تطور التكنولوجيا.

ويرى Levy (2020) أن أهمية إدارة مخاطر مراكز البيانات تنبع من كونها أداة لتقييم المخاطر المكانية والبيئية التي قد تؤثر في استقرار المركز، فهي تُساهم في اختيار المواقع الآمنة وتشخيص العوامل الجغرافية والإنشائية التي قد تشكل تهديداً لاستمرارية العمل. وتكمن أهميتها في:

1. تقليل أثر العوامل البيئية والطبيعية: من خلال تحليل المخاطر المرتبطة بالموقع مثل الزلازل أو الفيضانات أو انقطاع الطاقة.
2. رفع كفاءة القرارات الاستثمارية في البنية التحتية: إذ تُستخدم نتائج تقييم المخاطر في توجيه الاستثمارات نحو المواقع والمشروعات ذات مستويات الأمان الأعلى.
3. دعم الجاهزية المؤسسية: عبر توفير بيانات كمية تساعد في بناء خطط الطوارئ والتعافي بما يتوافق مع معايير الاستدامة التشغيلية.

أما Denny و Myneni (2025) فيؤكدان أن أهمية إدارة مخاطر مراكز البيانات تكمن في قدرتها على تحقيق التكامل بين مرحلي الإنشاء والتشغيل من خلال إدارة المخاطر طوال دورة حياة المركز، وهو ما يعزز من فاعلية استراتيجيات الاستجابة للأزمات ويضمن جاهزية البنية التحتية على المدى الطويل. وتبرز الأهمية لديهم في ثلاثة أبعاد مترابطة:

1. الوقاية من الأعطال أثناء مرحلة البناء والتشغيل: عبر تطبيق أدوات تحليل المخاطر الهندسية والإجرائية.
2. تحسين التنسيق بين الأطراف المعنية: من خلال وضوح المسؤوليات وتحديد نقاط الخطر المشتركة بين فرق الإنشاء والتشغيل.
3. تعزيز الكفاءة التشغيلية والاستدامة: إذ تسهم الإدارة المتكاملة للمخاطر في تحسين جودة الخدمات الرقمية وتقليل الهدر في الموارد.

5.1.2 أهداف إدارة مخاطر مراكز البيانات

تُعد إدارة مخاطر مراكز البيانات إحدى الركائز الرئيسة لضمان كفاءة واستدامة الأنظمة التقنية في المؤسسات الحديثة، إذ تهدف إلى تحقيق توازن بين الأداء العالي والموثوقية والأمان التشغيلي. وتشير الأدبيات الحديثة إلى أن أهداف هذه الإدارة تتجاوز البعد الوقائي لتشمل التحسين المستمر والجاهزية المؤسسية والمرونة التشغيلية، ضمن إطار تكاملي يتماشى مع متطلبات الحوكمة واستمرارية الأعمال.

ويُشير Hussaini و (2024) Raharjo إلى أن الهدف المركزي من إدارة مخاطر مراكز البيانات هو تأسيس منظومة ديناميكية لتقييم واستباق التهديدات التقنية والأمنية، بما يضمن استمرارية الأداء دون انقطاع. ويمكن تلخيص أهداف إدارة المخاطر لديهم في الآتي:

1. تحديد مصادر الخطر المحتملة بدقة من خلال الرصد الشامل لعوامل التهديد الداخلية والخارجية.
2. تحليل احتمالية وقوع المخاطر وتأثيرها النسبي على مكونات البنية التحتية الحيوية.
3. تصميم استراتيجيات وقائية واستباقية للحد من احتمالية التعطل أو فقدان البيانات.

أما Levy (2020) فيؤكد أن من أهم أهداف إدارة مخاطر مراكز البيانات تحقيق الاتساق بين العوامل البيئية والموقعية والتشغيلية، من أجل بناء مراكز بيانات قادرة على الصمود أمام الكوارث أو الظروف البيئية الطارئة. وتركز الأهداف وفق رؤيته في:

1. تحسين موثوقية اختيار مواقع مراكز البيانات عبر تطبيق منهجيات تقييم المخاطر الجغرافية والإنشائية.
2. تطوير خطط بديلة للطاقة والاتصال لضمان استمرار الخدمات عند انقطاع الموارد الأساسية.
3. توفير بيانات كمية تساهم في اتخاذ قرارات استثمارية مدروسة في مجال البنية التحتية الرقمية.

ويُضيف Denny و (2025) Myneni أن إدارة مخاطر مراكز البيانات تهدف إلى تحقيق التكامل بين مراحل الإنشاء والتشغيل من خلال أطر إدارة موحدة تسمح بتتبع المخاطر عبر دورة حياة المركز كاملة. وتتمثل الأهداف لديهم في:

1. تعزيز التنسيق بين الأطراف المعنية بالمشروع من مهندسين ومشغلين ومخططين.
2. تطبيق أدوات تحليلية وبصرية متقدمة لتقييم المخاطر بشكل فوري ودقيق.
3. ضمان جاهزية البنية التحتية التقنية عبر اختبارات منتظمة للسلامة والمرونة التشغيلية.

وفي السياق العربي، يشير العلوان والحياصات (2022) إلى أن من أبرز أهداف إدارة المخاطر في البيئات التقنية تحسين جودة الأداء وضمان الاستدامة التشغيلية عبر تبني منهجيات علمية دقيقة لتقدير احتمالات الخطر وتأثيراته. وتركز الإدارة لديهم على:

1. تحقيق الكفاءة في استخدام الموارد التقنية والبشرية.
2. تعزيز ثقافة الوعي بالمخاطر داخل المؤسسة.
3. تطوير آليات مراقبة مستمرة لتقييم فعالية إجراءات الحد من المخاطر.

ويرى العنزي وآخرون (2024) أن الهدف الأساسي من تطبيق استراتيجيات إدارة المخاطر هو دعم نجاح المشروعات التقنية ورفع الكفاءة المؤسسية، من خلال ضمان الاستجابة السريعة للمخاطر المحتملة وتقليل تأثيرها على سير العمل، مع التركيز على بناء بيئة تشغيلية مرنة وآمنة.

6.1.2 أبعاد إدارة مخاطر مراكز البيانات

تم تحديد أبعاد إدارة مخاطر مراكز البيانات استنادًا إلى مجموعة من الدراسات الحديثة التي تناولت إدارة المخاطر في البيئات التقنية ومراكز البيانات، ومن أبرزها دراسة Hussaini وRaharjo (2024) التي قدّمت النموذج الشامل لتقييم المخاطر (Comprehensive Risk Evaluation Model - CREM)، ودراسة Denny وMyneni (2025) التي طوّرت إطار إدارة متكامل للمخاطر في مراكز البيانات فائقة النطاق في الهند، إضافة إلى ما طرحه Levy (2020) حول تقييم المخاطر في مواقع مراكز البيانات، وكذلك ما توصلت إليه الدراسات العربية مثل العنزي وآخرون (2024) والعلوان والحياصات (2022) حول أبعاد إدارة المخاطر في المشروعات التقنية.

وانطلاقًا من هذه الأدبيات، يمكن تحديد الأبعاد الرئيسة لإدارة مخاطر مراكز البيانات في أربعة أبعاد مترابطة هي: تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر، حيث تشكل هذه الأبعاد المراحل الأساسية التي يقوم عليها النظام الإداري للمخاطر داخل بيئة مراكز البيانات.

أولاً: تحديد المخاطر (Risk Identification)

يُعد تحديد المخاطر الخطوة الأولى والأكثر أهمية في إدارة مخاطر مراكز البيانات، إذ يمثل الأساس الذي تُبنى عليه جميع المراحل اللاحقة. ويشير Hussaini وRaharjo (2024) إلى أن عملية تحديد المخاطر في مراكز البيانات تقوم على حصر جميع التهديدات المحتملة، سواء كانت داخلية مثل الأعطال التقنية وانقطاع الشبكة، أو خارجية مثل الكوارث الطبيعية والهجمات الإلكترونية.

في هذا السياق، تركز عملية تحديد المخاطر على تحليل بيئة العمل الداخلية والخارجية للمركز، بما يشمل مكونات البنية التحتية المادية (الخوادم، وحدات الطاقة، التبريد، الاتصال)، والبرمجيات (أنظمة التشغيل، إدارة الشبكة، التطبيقات)، والعوامل البشرية (المهندسون والمشغلون)، إضافة إلى العوامل البيئية والتنظيمية.

كما يُراعى في عملية التحديد أن تكون شاملة ومتكررة، بحيث تُحدّث قوائم المخاطر دوريًا وفقًا لتغيرات البيئة التقنية أو التوسع في القدرات التشغيلية للمركز. وتُعتبر هذه المرحلة ذات طابع استباقي، إذ تمكّن الإدارة من اكتشاف المخاطر قبل وقوعها، مما يتيح بناء قاعدة بيانات معرفية تُستخدم لاحقًا في التحليل والتقييم والمعالجة.

ثانيًا: تحليل المخاطر (Risk Analysis)

بعد تحديد مصادر الخطر، تأتي مرحلة تحليل المخاطر لتقدير خصائصها وقياس تأثيرها المحتمل على أداء مركز البيانات. ويشير Levy (2020) إلى أن تحليل المخاطر يتضمن دراسة العوامل المؤثرة في احتمالية وقوع الخطر وشدته، من خلال استخدام أدوات كمية ونوعية لتقدير مستويات الخطورة النسبية.

في مراكز البيانات، يشمل التحليل تقييم العلاقة بين سبب الخطر ونتيجته، مثل تأثير انقطاع التيار الكهربائي على أداء أنظمة التبريد، أو تأثير اختراق أمني على استقرار قواعد البيانات. ويُستخدم في هذه المرحلة مزيج من الأساليب التحليلية، منها تحليل الاحتمالية والتأثير-Probability (Probability-)

(Impact Analysis)، وتحليل السبب والجذر (Root Cause Analysis)، وتحليل السيناريوهات الذي يُستخدم للتنبؤ بنتائج محتملة تحت ظروف مختلفة.

وتبرز أهمية هذه المرحلة في أنها تتيح فهماً عميقاً لطبيعة المخاطر وعلاقاتها المتداخلة، مما يمكن المؤسسة من اتخاذ قرارات مبنية على بيانات دقيقة وليس على تقديرات عامة. كما يؤكد Myneni وDenny (2025) على أهمية استخدام الأدوات البصرية والتحليلية في تحليل المخاطر، مثل خرائط المخاطر ومصفوفات التهديد، لما توفره من وضوح في عرض المعلومات ودعم اتخاذ القرار في الوقت الفعلي.

ثالثاً: تقييم المخاطر (Risk Evaluation)

تمثل مرحلة تقييم المخاطر الجسر الذي يربط التحليل باتخاذ القرار، إذ تُستخدم نتائج التحليل لتحديد مستوى الخطر المقبول (Acceptable Risk Level) ومقارنته بالمعايير والسياسات المؤسسية. وفقاً لـ Hussaini وRaharjo (2024)، يهدف تقييم المخاطر إلى تصنيفها حسب أولويتها وأثرها المحتمل، بحيث يمكن ترتيبها من حيث الأهمية وضرورة التدخل. وفي مراكز البيانات، يُراعى عند التقييم تحديد المخاطر التي قد تؤدي إلى توقف الأنظمة الحرجة أو فقدان البيانات الحساسة، إذ تُعطى هذه المخاطر الأولوية القصوى في المعالجة.

تُستخدم في هذه المرحلة مصفوفات تقييم المخاطر (Risk Evaluation Matrices) التي تجمع بين احتمالية الحدوث وشدة التأثير، لتحديد الدرجة الكلية للمخاطر. (High – Medium – Low) كما يمكن استخدام مؤشرات كمية مثل معدل فقدان البيانات (Data Loss Rate) أو مدة الانقطاع (Downtime Duration) كمقاييس لتقييم التأثير الفعلي للمخاطر.

ويُشير العنزي وآخرون (2024) إلى أن تقييم المخاطر لا يقتصر على قياس الخطر نفسه، بل يمتد إلى تقييم كفاءة نظام إدارة المخاطر ومدى قدرته على الاستجابة الفورية وتقليل زمن التعطل التشغيلي. ومن ثم فإن عملية التقييم تمثل نقطة انطلاق لتطوير الخطط التصحيحية والتحسينية.

رابعًا: معالجة المخاطر (Risk Treatment)

تُعد معالجة المخاطر المرحلة التطبيقية في إدارة مخاطر مراكز البيانات، وتهدف إلى اختيار وتنفيذ الإجراءات التي تحد من احتمال وقوع الخطر أو تخفف من تأثيره في حال حدوثه.

وتُشير دراسة Denny و Myneni (2025) إلى أن معالجة المخاطر في مراكز البيانات تشمل مجموعة من الاستراتيجيات المتكاملة، منها الوقاية (Prevention) عبر تطوير أنظمة حماية متعددة الطبقات، والتقليل (Mitigation) من خلال تصميم بنية تحتية احتياطية (Redundancy)، والتحويل (Transfer) عبر التأمين أو التعاقد الخارجي، وأخيرًا القبول (Acceptance) لبعض المخاطر ذات التأثير المحدود.

وفي ضوء ISO 31000، تُعتبر معالجة المخاطر عملية متكررة تتضمن أيضًا مراقبة فعالية الإجراءات التصحيحية وتحديثها وفقًا للنتائج المتحققة. وتبرز أهمية هذه المرحلة في مراكز البيانات نظرًا لكونها تجمع بين الحلول التقنية (مثل أنظمة النسخ الاحتياطي والتعافي من الكوارث)، والحلول التنظيمية (مثل سياسات الأمن السيبراني وخطط الطوارئ)، مما يجعلها أكثر المراحل تأثيرًا في ضمان استمرارية الأعمال.

كما يشير العلوان والحياصات (2022) إلى أن فعالية المعالجة تعتمد على مدى تكاملها مع خطط العمل التشغيلية، بحيث لا تُنفذ بمعزل عن باقي الأنظمة بل تُدمج ضمن العمليات اليومية للمؤسسة، مما يحقق الاستدامة والجاهزية المستمرة.

المبحث الثاني: استمرارية الأعمال في المؤسسات التقنية

1.2.2 التمهيد

تُعد استمرارية الأعمال (Business Continuity Management – BCM) من المفاهيم الجوهرية في الإدارة الحديثة، خصوصًا في ظل التحولات الرقمية السريعة وزيادة المخاطر التقنية التي تهدد العمليات التشغيلية للمؤسسات. إذ لم تعد استمرارية الأعمال مجرد خطة طوارئ تُفعل عند الأزمات، بل أصبحت نظامًا إداريًا متكاملًا يهدف إلى ضمان استمرار الأنشطة الحيوية للمؤسسة دون انقطاع، والحفاظ على مستوى مقبول من الخدمات حتى في ظل الكوارث والأحداث غير المتوقعة.

لقد فرضت التطورات التكنولوجية المتسارعة، وانتشار الحوسبة السحابية، والاعتماد المكثف على البيانات، على المؤسسات التقنية ضرورة بناء قدرات مؤسسية مرنة قادرة على الصمود أمام التهديدات، سواء كانت سيبرانية، أو تشغيلية، أو بيئية. وفي هذا الإطار، تأتي استمرارية الأعمال كمنهج إداري استراتيجي يُدمج ضمن بنية الحوكمة المؤسسية لضمان جاهزية الموارد البشرية والتقنية والتنظيمية للتعامل مع أي انقطاع محتمل في الخدمات.

أصبحت استمرارية الأعمال ليست فقط استجابة للأزمات، بل إستراتيجية استباقية للوقاية والتحسين المستمر، تعتمد على إدارة المخاطر والتقييم الدوري للجاهزية المؤسسية، وتستند إلى معايير دولية مثل ISO 22301 التي وضعت إطارًا منهجيًا لتصميم، وتنفيذ، ومراقبة، وتحسين أنظمة إدارة الاستمرارية في جميع القطاعات.

2.2.2 مفهوم استمرارية الأعمال

تنوّعت تعريفات الباحثين لمفهوم استمرارية الأعمال باختلاف المدارس الفكرية والنماذج التطبيقية، إلا أنها تتقاطع جميعًا عند نقطة جوهرية مفادها أن استمرارية الأعمال هي عملية منهجية

تهدف إلى ضمان استدامة الأنشطة الحيوية للمؤسسة والحفاظ على قدرتها التشغيلية أثناء الأزمات وبعدها.

فقد عرّف Mošková و Bugarová (2023) استمرارية الأعمال بأنها "نظام إداري متكامل يعمل على تحديد التهديدات المحتملة وتأثيرها على المؤسسة، ويهدف إلى ضمان استمرارية الأنشطة الحيوية من خلال تطوير خطط واستراتيجيات وقائية واستجابية تُمكن المؤسسة من الصمود في مواجهة الانقطاعات المفاجئة."

بينما يرى Jain و Mitra (2025) أن استمرارية الأعمال تمثل "منهجًا شاملاً لإدارة المخاطر التشغيلية عبر الدمج بين التقييم الاستراتيجي، والتخطيط المسبق، والتدريب، والاختبارات الدورية، بما يضمن استدامة الأداء المؤسسي وتحقيق المرونة التشغيلية طويلة المدى."

أما Shdeed (2022) فيوضح أن استمرارية الأعمال هي "مجموعة من العمليات الإدارية المتكاملة التي تهدف إلى تمكين المؤسسة من مواجهة الأزمات والتحديات عبر خطط منهجية تضمن استمرارية تقديم الخدمات العامة والخاصة دون تعطيل مؤثر على أصحاب المصلحة." ومن منظور التحول الرقمي، تُعرّف صلاح (2025) استمرارية الأعمال بأنها "منظومة ديناميكية تركز على توظيف التقنيات الحديثة مثل التحول الرقمي والذكاء الاصطناعي لضمان بقاء العمليات المؤسسية فعّالة في ظل الأزمات، وتحقيق التوافق بين التكنولوجيا واستدامة الخدمات."

أما وفق المعيار الدولي ISO 22301، فتُعرّف إدارة استمرارية الأعمال بأنها "عملية مؤسسية تُعنى بتأسيس وتنفيذ وتشغيل ومراقبة وتحسين إطار لإدارة الاستمرارية، بهدف حماية المؤسسة من الأحداث المدمرة المحتملة، وضمان جاهزيتها للاستجابة بفاعلية عند حدوثها."

ومن خلال هذه التعريفات، يتضح أن استمرارية الأعمال ليست مجرد خطة طوارئ، بل إطار استراتيجي متكامل يُدمج ضمن الثقافة التنظيمية، ويشمل عناصر التحليل والتخطيط والتنفيذ والمراجعة والتحسين المستمر لضمان مرونة المؤسسة في بيئة متغيرة.

3.2.2 أهمية استمرارية الأعمال

تكتسب استمرارية الأعمال (Business Continuity Management - BCM) أهمية متزايدة في ظل البيئة التقنية المعقدة والمتغيرة التي تعمل فيها المؤسسات الحديثة، حيث أصبحت استمرارية الخدمات والأنشطة الحيوية مرهونة بمدى جاهزية المؤسسة لمواجهة الأزمات والمخاطر المفاجئة. فالأزمات – سواء كانت ناتجة عن كوارث طبيعية، أو أعطال تقنية، أو هجمات إلكترونية، أو أزمات اقتصادية – يمكن أن تعرّض المؤسسات لخسائر فادحة، ليس فقط على المستوى المالي، بل أيضًا على مستوى السمعة والثقة المؤسسية.

وتبرز أهمية إدارة استمرارية الأعمال في كونها الآلية المؤسسية التي تضمن استمرار تقديم الخدمات والعمليات الحيوية بأقل خسائر ممكنة، من خلال وضع خطط استباقية واستراتيجيات فعّالة للتعامل مع الأزمات قبل تفاقمها. كما تمثل أداة تنظيمية استراتيجية تسهم في تعزيز المرونة المؤسسية وتقوية قدرة المؤسسة على التعافي والعودة إلى التشغيل الكامل في أسرع وقت ممكن.

ويُشير Jain و Mitra (2025) إلى أن أهمية استمرارية الأعمال تنبع من كونها عنصرًا جوهريًا في إدارة المخاطر المؤسسية والحوكمة الرقمية، إذ تسهم في ربط الاستعداد التشغيلي بالإدارة الاستراتيجية. وقد حددا ثلاثة أبعاد رئيسة لأهمية استمرارية الأعمال:

1. ضمان الاستدامة التشغيلية: حيث تعمل إدارة استمرارية الأعمال على تقليل الانقطاعات في الخدمات الحيوية وضمان استمرار الأنظمة التقنية الأساسية دون توقف. فوجود خطة فعّالة لاستمرارية الأعمال يمكن المؤسسات التقنية من المحافظة على مستوى أدائها حتى أثناء الطوارئ.
2. تعزيز المرونة المؤسسية: إذ تساعد المؤسسة على التكيف مع الأزمات المفاجئة من خلال بناء أنظمة مرنة قادرة على امتصاص الصدمات والتعامل مع التغيرات بسرعة وكفاءة.
3. تحقيق الثقة والاعتمادية: من خلال طمأنة العملاء والشركاء وأصحاب المصلحة بقدرة المؤسسة على الصمود أمام المخاطر والحفاظ على جودة خدماتها.

ويرى Mošková و (2023) Bugarová أن استمرارية الأعمال تمثل أداة لضمان استدامة المؤسسة في بيئة تتسم بعدم اليقين، مشيرين إلى أن المؤسسات التي تُطبق نظم استمرارية الأعمال تمتلك قدرة أعلى على التكيف مع التغيرات المفاجئة مقارنة بتلك التي تعمل بصورة تقليدية. وقد أوضحا أن أهمية الاستمرارية تتجسد في ثلاثة محاور مترابطة:

1. الوقاية من الانقطاع الكلي للعمليات الحيوية: عبر وضع أنظمة احتياطية واستراتيجيات وقائية تقلل من احتمالية توقف الخدمات.
2. رفع كفاءة إدارة الأزمات: من خلال تحديد واضح للأدوار والمسؤوليات داخل المؤسسة أثناء الطوارئ، مما يحد من الارتباك التنظيمي.
3. تحقيق التكامل بين الخطط التشغيلية والاستراتيجية: بحيث لا تقتصر الاستمرارية على الجانب الفني، بل تمتد لتشمل التخطيط طويل الأمد وضمان الاستدامة المؤسسية.

4.2.2 أهداف استمرارية الأعمال

تُعد إدارة استمرارية الأعمال (Business Continuity Management – BCM) من أهم النظم الإدارية التي تسعى المؤسسات التقنية إلى تبنيها ضمن استراتيجياتها التشغيلية والتنظيمية، نظرًا لدورها في ضمان استمرار الأنشطة الحيوية والخدمات الأساسية في مواجهة الأزمات والمخاطر المتنوعة. وتنبع أهدافها من فلسفة الوقاية والاستعداد المسبق، التي تؤكد أن المؤسسة القادرة على إدارة الأزمات بفعالية هي تلك التي تُخطط مسبقًا لاستمرارية أعمالها وفق أسس علمية ومنهجية متكاملة.

تؤكد Mošková و (2023) Bugarová أن الهدف المركزي من استمرارية الأعمال يتمثل في ضمان بقاء العمليات الحيوية مستمرة في مختلف الظروف، سواء أثناء الأزمات أو بعدها، من خلال بناء نظام متكامل يحدد التهديدات المحتملة ويضع آليات وقائية واستجابية للتعامل معها. وتوضحان أن هذا الهدف يتفرع إلى عدة مقاصد فرعية تشمل:

1. تقليل احتمالية التوقف الكلي للعمليات الحيوية عبر وضع خطط احتياطية فعالة.

2. تسريع عملية التعافي المؤسسي (Organizational Recovery) بعد وقوع الحوادث لضمان استعادة الخدمات في أقصر وقت ممكن.

3. تحقيق المرونة التشغيلية (Operational Resilience) التي تمكن المؤسسة من التكيف السريع مع الظروف المتغيرة.

ويُشير Jain و Mitra (2025) إلى أن استمرارية الأعمال تهدف إلى تطوير قدرة المؤسسة على مواجهة الأزمات المستقبلية من خلال التكامل بين التخطيط الاستراتيجي وإدارة المخاطر، حيث لا تقتصر على التعامل مع الحدث بعد وقوعه، بل تمتد إلى التحليل المسبق والتنبؤ بالاحتمالات. ويريان أن أهداف إدارة الاستمرارية تتضمن:

1. تطوير خطط استجابة مرنة (Adaptive Response Plans) تمكن المؤسسة من التحرك السريع عند الطوارئ.

2. تدعيم أنظمة الاتصال والتنسيق الداخلي والخارجي أثناء الأزمات.

3. تعزيز ثقافة الوقاية المؤسسية من خلال التدريب المستمر والاختبارات الدورية لخطة الاستمرارية.

أما Shdeed (2022) فيوضح أن من أبرز أهداف إدارة استمرارية الأعمال في المؤسسات العامة والخاصة هو ضمان تقديم الخدمات للمستفيدين بشكل متواصل رغم الأزمات، مؤكدًا على أن الهدف لا يقتصر على الاستمرار فقط، بل يشمل رفع كفاءة الأداء أثناء الأزمات عبر تحديد المسؤوليات بوضوح وتقليل الارتباك المؤسسي. ويُبين أن من الأهداف الرئيسة أيضًا:

1. تحقيق الكفاءة الإدارية والتشغيلية في أوقات الأزمات.

2. تقليل الآثار السلبية على سمعة المؤسسة وثقة المتعاملين.

3. تطوير آليات المراقبة المستمرة لتقييم فاعلية الخطط وتحسينها.

وتشير صلاح (2025) إلى أن من أهم أهداف إدارة استمرارية الأعمال في المؤسسات التقنية هو تعزيز التحول الرقمي المستدام، إذ إن استمرارية الخدمات الرقمية تمثل حجر الأساس في بناء الثقة والاعتمادية في بيئة الاقتصاد الرقمي. وتحدد أهداف إدارة الاستمرارية في هذا السياق في:

1. تحقيق الاستقرار الرقمي (Digital Stability) وضمان عمل الأنظمة الإلكترونية دون انقطاع.
2. تعزيز أمن البيانات (Data Security) واستعادتها بسرعة في حالات التعطل أو الاختراق.
3. تحقيق التكامل بين البنية التحتية التقنية وخطط الطوارئ المؤسسية.

5.2.2 التحديات التي تواجه إدارة استمرارية الأعمال

على الرغم من التطور الكبير الذي شهدته المؤسسات التقنية في تبني أنظمة إدارة استمرارية الأعمال (Business Continuity Management – BCM)، فإن تطبيق هذا النظام يواجه مجموعة من التحديات المعقدة والمتداخلة التي تختلف باختلاف طبيعة المؤسسة، وبنيتها التقنية، ومستوى نضجها التنظيمي.

وتنبع هذه التحديات من مزيج من العوامل البشرية، والتقنية، والتنظيمية، والبيئية التي تؤثر في قدرة المؤسسة على تحقيق الجاهزية التشغيلية والاستجابة الفعالة للأزمات. وقد تناولت الأدبيات الحديثة هذه التحديات من زوايا مختلفة، كما في أعمال Jain و Mitra (2025)، و Mošková و Bugarová (2023)، و Shdeed (2022)، و صلاح (2025)، والحسين ومتولي (2023)، وغيرها من الدراسات التي ركزت على العقبات التي تحول دون التطبيق الفعال لنظم الاستمرارية، خاصة في المؤسسات التقنية ومراكز البيانات.

❖ التحديات التنظيمية والإدارية

تُعد ضعف التكامل المؤسسي بين إدارة المخاطر واستمرارية الأعمال من أبرز التحديات التي تواجه المؤسسات التقنية. فكما يشير Jain و Mitra (2025)، فإن كثيرًا من المؤسسات تنظر إلى إدارة الاستمرارية على أنها وظيفة ثانوية مرتبطة بإدارة الطوارئ فقط، وليست جزءًا من النظام الإداري الاستراتيجي.

وهذا التصور يؤدي إلى تجزئة الجهود بين الإدارات المختلفة وعدم وضوح الأدوار والمسؤوليات في حالات الأزمات.

ومن التحديات الإدارية أيضًا غياب القيادة الداعمة التي تؤمن بأهمية الاستمرارية كأولوية استراتيجية، وهو ما يجعل الخطط الموضوعية مجرد وثائق شكلية لا تُطبّق فعليًا عند الأزمات. كما أن نقص الوعي المؤسسي لدى الموظفين يمثل حاجزًا مهمًا أمام ترسيخ ثقافة الوقاية والاستعداد، إذ يُنظر إلى خطط الاستمرارية في بعض الأحيان كعبء إداري بدلاً من اعتبارها وسيلة لتعزيز الأمان التشغيلي. وتشير الأدبيات العربية مثل الحسين ومتولي (2023) وعبدالسلام (2022) إلى أن المؤسسات العربية – ولا سيما التقنية – تعاني من قصور في التخطيط الاستراتيجي طويل الأمد، وضعف في مأسسة الاستمرارية كجزء من الحوكمة المؤسسية، مما يقلل من فعاليتها عند الأزمات الفعلية.

❖ التحديات التقنية والتشغيلية

تتمثل التحديات التقنية في تعقّد البنية التحتية المعلوماتية وتداخل الأنظمة التشغيلية في المؤسسات التقنية، وخاصة في مراكز البيانات. فكما يوضح Mošková وBuganová (2023)، فإن زيادة الاعتماد على الأنظمة الرقمية يجعل المؤسسات أكثر عرضة للأعطال التقنية والهجمات السيبرانية، مما يتطلب جاهزية تقنية متقدمة يصعب تحقيقها دون استثمارات ضخمة.

وتبرز هنا مشكلات تحديث أنظمة النسخ الاحتياطي والتعافي من الكوارث (Disaster Recovery Systems)، إذ تحتاج هذه الأنظمة إلى اختبارات دورية وصيانة مستمرة للتأكد من فعاليتها. كما أن ضعف التكامل بين الأنظمة الأساسية والأنظمة الاحتياطية قد يؤدي إلى فشل الانتقال السلس أثناء الانقطاعات المفاجئة.

وفي السياق نفسه، يشير صلاح (2025) إلى أن التحدي الأكبر في المؤسسات الرقمية هو التوازن بين التحول الرقمي والاستقرار التشغيلي؛ فالتحديث السريع للأنظمة والتقنيات قد يخلق ثغرات جديدة إذا لم تُواكبها خطط استمرارية محدثة. ومن المشكلات الأخرى أيضًا اعتماد بعض المؤسسات على حلول

تقنية مغلقة أو غير مرنة، مما يحدّ من قدرتها على التوسع أو التعديل في حالات الطوارئ، إضافة إلى نقص الكفاءات التقنية المتخصصة في مجال BCM وDRP (Disaster Recovery Planning).

❖ التحديات المالية والاقتصادية

تُعدّ الكلفة العالية لتطبيق أنظمة الاستمرارية من أبرز المعوقات التي تواجه المؤسسات، خاصة في القطاعات التقنية ذات الاحتياجات التشغيلية الكبيرة. فكما يوضح Mošková وBuganová (2023)، فإن تنفيذ نظام متكامل لإدارة الاستمرارية يتطلب استثمارات مالية في البنية التحتية، وتحديث الأنظمة الاحتياطية، وتدريب الكوادر البشرية.

وفي كثير من المؤسسات، لا تُعتبر هذه النفقات ذات أولوية مقارنة بالعمليات التشغيلية اليومية، مما يؤدي إلى ضعف الاستعداد الفعلي عند وقوع الأزمات. كما أن تخصيص الموارد المالية بشكل غير متوازن بين الإدارات المختلفة قد يخلق فجوات في تطبيق الإجراءات الوقائية.

أما في المؤسسات الصغيرة والمتوسطة، فإن محدودية الموارد المالية تجعلها تعتمد على حلول تقليدية أو يدوية لإدارة الأزمات، دون وجود نظام إلكتروني متكامل لمتابعة الأداء وضمان التعافي الفعلي. وتؤكد الدراسات الحديثة أن المؤسسات التي لا تستثمر في خطط استمرارية فعالة تكون أكثر عرضة للخسائر طويلة الأمد مقارنة بتلك التي تُخصص ميزانية واضحة للجاهزية التشغيلية.

❖ التحديات البشرية والثقافية

تُعدّ العوامل البشرية من أكثر الجوانب تأثيراً في نجاح أو فشل إدارة استمرارية الأعمال. إذ يشير Shdeed (2022) إلى أن ضعف الثقافة المؤسسية تجاه الاستمرارية يشكل عائقاً كبيراً أمام تنفيذ الخطط بفاعلية.

فالعديد من الموظفين لا يُدركون أهمية التدريب على خطط الطوارئ أو الممارسة الدورية للسيناريوهات المحتملة، مما يؤدي إلى بطء الاستجابة أثناء الأزمات الفعلية. كما أن مقاومة التغيير تمثل

تحديًا متكررًا، حيث يميل بعض العاملين إلى اتباع الروتين المعتاد دون الالتزام بالإجراءات الجديدة التي تفرضها خطط الاستمرارية.

إلى جانب ذلك، فإن نقص التواصل الفعال بين المستويات الإدارية المختلفة يؤدي إلى تضارب في القرارات عند وقوع الأزمة، مما يعرقل سرعة التعافي. ويُضاف إلى هذه التحديات أيضًا ضعف التحفيز المؤسسي، إذ لا توجد دائمًا مكافآت أو حوافز تشجع الموظفين على المشاركة بفاعلية في برامج التدريب على إدارة الأزمات والاستمرارية.

❖ التحديات البيئية والتشريعية

تشير الأدبيات الحديثة إلى أن البيئة التنظيمية والقانونية تشكل بدورها تحديًا مهمًا أمام تطبيق استمرارية الأعمال، خاصة في المؤسسات التي تعمل ضمن قطاعات عالية التنظيم مثل الاتصالات والخدمات التقنية.

فقد أشار Al-Nimri و Al-Shawabkeh (2023) إلى أن غياب الأطر التشريعية الملزمة أو ضعف الرقابة الحكومية على خطط الاستمرارية يؤدي إلى تفاوت في تطبيق المعايير بين المؤسسات. كما أن التغيرات البيئية مثل الكوارث الطبيعية (الفيضانات، الحرائق، الزلازل) تمثل تحديًا خارجيًا يصعب السيطرة عليه، وتتطلب استعدادًا خاصًا في مراكز البيانات التي تُعتبر من أكثر البنى الحساسة تأثرًا بالعوامل المناخية. ومن التحديات أيضًا صعوبة التوافق مع المعايير الدولية (مثل ISO 22301 و ISO 27031) بسبب متطلبات الامتثال المعقدة والاختبارات الدورية المكلفة.

الفصل الثالث: منهجية الدراسة

1.3 منهج الدراسة

نظراً لطبيعة موضوع الدراسة وأهدافها التي تسعى إلى التعرف على أثر إدارة مخاطر مراكز البيانات بأبعادها المختلفة على استمرارية الأعمال في المؤسسات التقنية، فقد استخدم الباحث المنهج الوصفي التحليلي (Descriptive Analytical Method) ، وهو المنهج الأنسب للدراسات الإدارية التي تهدف إلى تحليل الظواهر الواقعية كما هي، ووصف خصائصها، وتفسير العلاقات بين متغيراتها. ويقوم هذا المنهج على جمع البيانات من الميدان، وتحليلها إحصائياً لاستخلاص النتائج التي تعبر عن طبيعة العلاقة بين المتغير المستقل (إدارة مخاطر مراكز البيانات) والمتغير التابع (استمرارية الأعمال). كما تم استخدام الأساليب الإحصائية الوصفية والاستدلالية في تحليل البيانات بهدف اختبار الفروض والتأكد من مدى دلالتها الإحصائية.

2.3 مجتمع الدراسة

يتكوّن مجتمع الدراسة من جميع المؤسسات التقنية التي تمتلك أو تدير مراكز بيانات في مدينة الرياض، وتشمل الجهات الحكومية وشبه الحكومية، والشركات الخاصة العاملة في مجالات الاتصالات، وتقنية المعلومات، والحوسبة السحابية، والبنية التحتية الرقمية. وتُعد الرياض المركز الرئيس لمراكز البيانات في المملكة، إذ تضم ما يقارب (28) مركز بيانات من أصل 45 مركزاً على مستوى المملكة، وفقاً لتقارير الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا، 2024) ووزارة الاتصالات وتقنية المعلومات. ويتضمن هذا المجتمع فئات متعددة من الكوادر الفنية والإدارية، مثل مديري المخاطر، ومهندسي البنية التحتية، وخبراء الأمن السيبراني، ومسؤولي استمرارية الأعمال، ومشرفي التشغيل والدعم الفني. ويُقدّر العدد الكلي للعاملين في هذه المجالات داخل مراكز البيانات في الرياض بحوالي (850) موظفاً من مختلف المستويات التنظيمية. ويتميّز هذا المجتمع بخصائصه التقنية العالية واعتماده الكبير على أنظمة

التشغيل الرقمية المتقدمة، مما يجعله بيئة مثالية لاختبار العلاقة بين إدارة مخاطر مراكز البيانات واستمرارية الأعمال في المؤسسات التقنية.

اعتمد الباحث المنهج العشوائي الطبقي في اختيار العينة لضمان تمثيل جميع أنواع المؤسسات ضمن مجتمع الدراسة، حيث تم تقسيمه إلى ثلاث طبقات رئيسية هي: القطاع الحكومي، والقطاع شبه الحكومي، والقطاع الخاص. وتم تحديد حجم العينة بـ (210) فردًا من أصل (850) يمثلون المجتمع الكلي، بنسبة تمثيل بلغت نحو 24.7%، وهي نسبة مناسبة إحصائيًا لتحقيق أهداف الدراسة. وجرى توزيع أدوات البحث (الاستبانة) إلكترونياً وميدانياً خلال الفترة من مارس إلى مايو 2025، واستُرد منها (187) استبانة صالحة للتحليل الإحصائي بنسبة استجابة مرتفعة بلغت 89%.

3.3 أداة الدراسة

اعتمدت هذه الدراسة على الاستبانة (Questionnaire) باعتبارها الأداة الرئيسة لجمع البيانات الميدانية من أفراد العينة، لما تتميز به من قدرة على قياس الاتجاهات وتحديد العلاقات بين المتغيرات محل الدراسة بطريقة كمية منظمة، وقد صُممت الاستبانة بعناية استنادًا إلى الإطارين النظري والمنهجي للدراسة، وإلى مجموعة من الدراسات السابقة ذات الصلة بإدارة المخاطر واستمرارية الأعمال في البيئات التقنية ومراكز البيانات، دراسات (Mošková & Buganová, 2023; Jain & Mitra, 2025; Levy, 2020; الشهراني وآخرون، 2024; العنزي وآخرون، 2024)، مع مراعاة خصوصية البيئة السعودية وواقع مراكز البيانات في مدينة الرياض.

تألفت الاستبانة من قسمين رئيسيين:

- القسم الأول: خُصص لجمع البيانات العامة عن المبحوثين، مثل الجنس، والمؤهل العلمي، وسنوات الخبرة، والمسعى الوظيفي، والقطاع الذي يعمل فيه، وحجم مركز البيانات.
- القسم الثاني: خُصص لقياس متغيرات الدراسة الرئيسة، وتم بناؤه على النحو الآتي:

المتغير المستقل: إدارة مخاطر مراكز البيانات

يتكوّن المتغير المستقل (إدارة مخاطر مراكز البيانات) من أربعة أبعاد رئيسة تمثل المراحل المنهجية

المتعارف عليها وفق معايير ISO 31000 و NIST SP 800-30، وهي على النحو الآتي:

١. تحديد المخاطر (Risk Identification) يقيس مدى قدرة المؤسسة على التعرف على مصادر المخاطر

المحتملة داخل مراكز البيانات، سواء كانت تقنية أو تشغيلية أو بشرية أو بيئية، ووضع آليات منهجية

لتوثيقها ومتابعتها.

٢. تحليل المخاطر (Risk Analysis) يركّز على دراسة احتمالية وقوع المخاطر وتأثيرها على العمليات

الحיוية، ومدى استخدام أدوات التحليل الكمي والنوعي لتقدير مستوى الخطورة والعلاقات بين

مسبباتها ونتائجها.

٣. تقييم المخاطر (Risk Evaluation) يتناول عملية ترتيب المخاطر وتحديد أولوياتها وفق معايير

الاحتمالية والتأثير، وقياس مدى قدرة المؤسسة على تحديد درجة تحمل المخاطر واتخاذ القرارات

المناسبة لمعالجتها.

٤. معالجة المخاطر (Risk Treatment) يقيس كفاءة المؤسسة في التعامل مع المخاطر ذات الأولوية من

خلال استراتيجيات التخفيف أو التحويل أو القبول أو التجنّب، إضافة إلى تنفيذ خطط الاستجابة

والتحسين المستمر.

وبذلك بلغ مجموع فقرات هذا المتغير (20) فقرة موزعة بالتساوي على أبعاده الخمسة.

المتغير التابع: استمرارية الأعمال (Business Continuity Management)

ويُعد هذا المتغير أحادي المحور لكونه يقيس درجة تطبيق المؤسسة لمبادئ وإجراءات استمرارية

الأعمال بصورة شاملة، دون تفرّيع داخلي للأبعاد، وقد تضمن هذا المحور (10) فقرات تقيس مستوى

التخطيط المسبق، والجاهزية المؤسسية، والاستجابة الفورية، والتعافي بعد الأزمات، والاستدامة

التشغيلية في المؤسسات التقنية ومراكز البيانات

4.3. صدق أداة الدراسة

تحقق الباحث من صدق أداة الدراسة (Validity) للتأكد من مدى قدرتها على قياس ما وضعت لقياسه، وذلك من خلال طريقتين أساسيتين:

1. صدق المحتوى: (Content Validity)

تم عرض الاستبانة على عدد من المحكمين الأكاديميين والمختصين في مجالات إدارة المخاطر واستمرارية الأعمال وتقنية المعلومات من الجامعات السعودية، للتأكد من وضوح العبارات، ودقتها، وشمولها لمجالات المتغيرات. وبعد إجراء التعديلات المقترحة من لجنة التحكيم، أقرت صلاحية الأداة لجمع البيانات الميدانية.

2. الصدق الإحصائي: (Construct Validity)

تم التحقق منه من خلال تحليل معاملات الارتباط البيني بين أبعاد المتغير المستقل (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر)، حيث يُفترض أن تكون معاملات الارتباط دالة إحصائيًا وموجبة ومتوسطة إلى مرتفعة، بما يدل على وجود علاقة ارتباطية قوية بين الأبعاد لقياس المفهوم ذاته دون تكرار أو تداخل مفرط.

5.3 مصفوفة الارتباط للمتغير المستقل

يُوضَّح الجدول الآتي معاملات الارتباط (Pearson Correlation Coefficients) بين أبعاد متغير إدارة مخاطر مراكز البيانات استنادًا إلى بيانات الدراسة الميدانية (ن = 187):

الجدول (1) مصفوفة الارتباط للمتغير المستقل

الأبعاد	تحديد المخاطر	تحليل المخاطر	تقييم المخاطر	معالجة المخاطر
تحديد المخاطر	1	0.74**	0.69**	0.65**
تحليل المخاطر	0.74**	1	0.78**	0.71**
تقييم المخاطر	0.69**	0.78**	1	0.76**
معالجة المخاطر	0.65**	0.71**	0.76**	1

($p < 0.01$)

تشير القيم الواردة في الجدول إلى أن جميع معاملات الارتباط موجبة ودالة إحصائيًا عند مستوى دلالة (0.01)، مما يدل على وجود علاقة ارتباط قوية بين الأبعاد الأربعة لمفهوم إدارة مخاطر مراكز البيانات.

وتتراوح معاملات الارتباط بين (0.65 و 0.78)، وهي تقع ضمن الحدود المقبولة إحصائيًا وفقًا للمعايير العلمية (0.40 – 0.80)، ما يعني أن الأبعاد مترابطة فيما بينها دون تطابق تام أو تكرار في القياس.

6.3 ثبات أداة الدراسة

تم التحقق من ثبات أداة الدراسة (Reliability) للتأكد من اتساقها الداخلي واستقرار نتائجها عبر استخدام معامل كرونباخ ألفا (Cronbach's Alpha)، وهو من أكثر الأساليب شيوعًا في البحوث الإدارية لقياس مدى تجانس فقرات الأداة في قياس المتغير نفسه. وقد تم احتساب معاملات الثبات لكل بُعد من أبعاد المتغير المستقل إدارة مخاطر مراكز البيانات، إضافة إلى المتغير التابع استمرارية الأعمال، وذلك باستخدام بيانات العينة البالغة (187) استبانة.

الجدول (2): معاملات الثبات لمتغيرات الدراسة باستخدام معامل كرونباخ ألفا

المتغير / البُعد	عدد الفقرات	معامل كرونباخ ألفا (α)
أولاً: إدارة مخاطر مراكز البيانات	16	0.93
تحديد المخاطر	4	0.88
تحليل المخاطر	4	0.90
تقييم المخاطر	4	0.87
معالجة المخاطر	4	0.89
ثانياً: استمرارية الأعمال (أحادي المحور)	10	0.92
المجموع الكلي للأداة	26	0.94

تشير القيم الواردة في الجدول إلى أن جميع معاملات كرونباخ ألفا تجاوزت الحد الأدنى المقبول إحصائياً (0.70) ، بل وجاءت ضمن نطاق مرتفع يتراوح بين (0.87 – 0.94)، مما يدل على مستوى عالٍ من الاتساق الداخلي بين فقرات الأداة.

7.3 أساليب التحليل الإحصائي المستخدمة في الدراسة

تم استخدام مجموعة من الأساليب الإحصائية الوصفية والاستدلالية لتحليل البيانات التي تم جمعها من الاستبيانات، وذلك باستخدام البرنامج الإحصائي (SPSS – Statistical Package for the Social Sciences) إصدار 25، نظراً لما يتميز به من دقة في التحليل وسهولة في تفسير النتائج. وقد هدفت هذه الأساليب إلى وصف خصائص العينة، وقياس صدق وثبات الأداة، واختبار فرضيات الدراسة، وذلك على النحو الآتي:

1. الأساليب الإحصائية الوصفية: (Descriptive Statistics)

أُستخدمت الأساليب الوصفية بهدف تحليل البيانات التعريفية للمشاركين وتحديد اتجاهاتهم نحو متغيرات الدراسة، وشملت ما يلي:

- التكرارات والنسب المئوية: لوصف الخصائص الديموغرافية للعينة (النوع، المؤهل، سنوات الخبرة، المسمى الوظيفي، القطاع).
- المتوسطات الحسابية والانحرافات المعيارية: لقياس مستوى إدراك المبحوثين لأبعاد متغير إدارة مخاطر مراكز البيانات ومستوى استمرارية الأعمال في مؤسساتهم.
- معاملات الالتواء والتفلطح: للتحقق من مدى توزيع البيانات واختبار افتراضات التحليل الإحصائي (Normality).

2. الأساليب الإحصائية الاستدلالية: (Inferential Statistics)

- أُستخدمت الأساليب الاستدلالية لاختبار فروض الدراسة الرئيسية والفرعية، وبيان قوة واتجاه العلاقة بين المتغيرات، وتحديد أثر المتغير المستقل على التابع، وتمثلت فيما يلي:
- معامل الارتباط لبيرسون (Pearson Correlation Coefficient): لقياس قوة واتجاه العلاقة بين أبعاد إدارة مخاطر مراكز البيانات ومتغير استمرارية الأعمال.
 - تحليل الانحدار الخطي البسيط والمتعدد (Simple & Multiple Linear Regression): لقياس أثر أبعاد إدارة مخاطر مراكز البيانات (تحديد، تحليل، تقييم، معالجة المخاطر) على استمرارية الأعمال، وتحديد البعد الأكثر تأثيراً.
 - اختبار (T-test) وتحليل التباين الأحادي (One-Way ANOVA): لقياس الفروق بين متوسطات استجابات أفراد العينة تبعاً للمتغيرات الديموغرافية مثل الخبرة، المؤهل العلمي، والقطاع.
 - معامل الثبات (Cronbach's Alpha): للتحقق من تجانس فقرات الأداة واستقرار القياس الداخلي.
 - تحليل معامل التحديد (R^2) وإحصائية (F): لتفسير نسبة التباين في المتغير التابع الناتج عن المتغير المستقل، واختبار دلالة النموذج الإحصائي.

الفصل الرابع: تحليل البيانات ومناقشة النتائج

1.4 تمهيد

يهدف هذا الفصل إلى عرض نتائج تحليل البيانات التي تم جمعها من أفراد عينة الدراسة والبالغ عددهم (187) فردًا من العاملين في مراكز البيانات بمدينة الرياض، وذلك بغرض اختبار فرضيات الدراسة والتحقق من مدى صحة العلاقات بين متغيراتها.

2.4 الخصائص الديموغرافية لعينة الدراسة

يُعرض في الجدول (3) التوزيع الوصفي لعينة الدراسة وفق المتغيرات الديموغرافية الأساسية (الجنس، المؤهل العلمي، سنوات الخبرة، المسمى الوظيفي، القطاع).

الجدول (3): التوزيع الديموغرافي لعينة الدراسة (ن = 187)

المتغير	الفئة	التكرار	النسبة المئوية (%)
الجنس	ذكر	146	78.1
	أنثى	41	21.9
المؤهل العلمي	دبلوم تقني	22	11.8
	بكالوريوس	105	56.1
	دراسات عليا	60	32.1
سنوات الخبرة	أقل من 5 سنوات	28	15.0
	من 5 إلى 10 سنوات	71	38.0
	أكثر من 10 سنوات	88	47.0
المسمى الوظيفي	مدير أنظمة وبنية تحتية	52	27.8

المتغير	الفئة	التكرار	النسبة المئوية (%)
	مسؤول أمن معلومات	47	25.1
	مدير مخاطر واستمرارية أعمال	41	21.9
	مشرف تشغيل ودعم فني	47	25.1
القطاع	حكومي	75	40.1
	شبه حكومي (اتصالات وتقنية)	69	36.9
	خاص	43	23.0

تُظهر النتائج أن نسبة الذكور بلغت (78.1%) مقابل (21.9%) من الإناث. ويُعزى ذلك إلى الطبيعة الفنية والتقنية المتخصصة لعمل مراكز البيانات، التي تتطلب مهارات في البنية التحتية والأمن السيبراني وإدارة الشبكات، وهي مجالات يغلب عليها الطابع الذكوري في سوق العمل السعودي.

أظهرت النتائج أن أكثر من نصف العينة (56.1%) يحملون مؤهل البكالوريوس، و(32.1%) دراسات عليا، و(11.8%) فقط دبلوم تقني، ويعكس هذا التوزيع ارتفاع المستوى التعليمي للعاملين في مراكز البيانات، وهو أمر متوقع في بيئة تقنية تعتمد على الكفاءات المتخصصة في مجالات هندسة الحاسبات، وإدارة المخاطر، وأمن المعلومات.

يتضح أن معظم أفراد العينة يمتلكون خبرة طويلة؛ إذ بلغت نسبة من تزيد خبرتهم عن عشر سنوات (47%)، تليها فئة خمس إلى عشر سنوات (38%)، ثم أقل من خمس سنوات (15%). ويُظهر ذلك أن العاملين في مراكز البيانات يتمتعون بخبرة مهنية تراكمية تؤهلهم للتعامل مع الأنظمة المعقدة والمخاطر التشغيلية.

يتوزع أفراد العينة على أربعة مسميات وظيفية رئيسة، وجميعها ذات ارتباط مباشر بموضوع الدراسة، حيث يشكل مديرو الأنظمة والبنية التحتية النسبة الأكبر (27.8%)، يليهم مسؤولو أمن المعلومات (25.1%)، ومشرفو التشغيل والدعم الفني (25.1%)، ثم مدراء المخاطر واستمرارية الأعمال

(21.9%)، هذا التوزيع المتوازن يعكس تمثيل جميع المستويات الإدارية والفنية ذات الصلة بعمليات إدارة المخاطر واستمرارية الأعمال، مما يمنح الدراسة عمقاً تحليلياً وتنوعاً في وجهات النظر.

توزع المشاركون بين ثلاثة قطاعات رئيسية، حيث شكّل القطاع الحكومي النسبة الأكبر (40.1%)، يليه شبه الحكومي (36.9%)، ثم القطاع الخاص (23%)، ويُفسّر هذا بأن مدينة الرياض تحتضن أكبر عدد من مراكز البيانات الحكومية والوطنية التابعة للجهات السيادية مثل الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) ومركز المعلومات الوطني.

3.4 التحليل الوصفي للمتغير المستقل — إدارة مخاطر مراكز البيانات

يهدف هذا الجزء إلى تحليل استجابات أفراد العينة تجاه فقرات المتغير المستقل إدارة مخاطر مراكز البيانات، وذلك من خلال حساب المتوسطات الحسابية والانحرافات المعيارية لكل فقرة لتحديد مستوى التطبيق الفعلي داخل مراكز البيانات بمدينة الرياض. وقد تم قياس المتغير عبر أربعة أبعاد رئيسية هي: تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر، بواقع أربع فقرات لكل بُعد، باستخدام مقياس ليكرت الخماسي = 1 أعارض بشدة، 5 = أوافق بشدة

البُعد الأول: تحديد المخاطر (Risk Identification)

الجدول (4) التحليل الوصفي لبعد تحديد المخاطر (Risk Identification)

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	تعتمد المؤسسة على نظام موحد لتحديد مصادر الخطر داخل مركز البيانات.	4.25	0.61	مرتفع
2	يتم تحديث سجل المخاطر بشكل دوري وفقاً للتغيرات التشغيلية.	4.18	0.67	مرتفع

مرتفع	0.58	4.23	تشارك الإدارات الفنية والإدارية في عملية التعرف على المخاطر.	3
مرتفع	0.55	4.30	يتم توثيق حوادث الانقطاع السابقة وتحليلها لاستخلاص الدروس المستفادة.	4
مرتفع	0.60	4.24	المتوسط العام للبُعد	

يُظهر الجدول أن المتوسط العام لبُعد تحديد المخاطر بلغ (4.24) بانحراف معياري (0.60)، وهو ما يشير إلى مستوى مرتفع من تطبيق ممارسات تحديد المخاطر في مراكز البيانات. وتُعد الفقرة المتعلقة بتوثيق الحوادث السابقة وتحليلها الأعلى تقييماً (4.30)، مما يدل على اهتمام المؤسسات بتعلم الدروس التشغيلية لتفادي تكرار الأعطال. كما تُظهر النتائج وجود ثقافة مؤسسية تشاركية في التعرف على مصادر الخطر، وهو مؤشر على نضج منظومة إدارة المخاطر واتساع نطاقها التنظيمي داخل مراكز البيانات.

البُعد الثاني: تحليل المخاطر (Risk Analysis)

الجدول (5) التحليل الوصفي لبعد تحليل المخاطر (Risk Analysis)

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	يتم تحليل المخاطر وفقاً لاحتمالية حدوثها وتأثيرها على العمليات الحيوية.	4.19	0.63	مرتفع
2	تستخدم المؤسسة أدوات كمية مثل مصفوفة الاحتمالية والتأثير لتقدير مستوى الخطر.	4.12	0.68	مرتفع
3	تتم مراجعة نتائج تحليل المخاطر بانتظام لتحديث خطط الطوارئ.	4.15	0.62	مرتفع

مرتفع	0.59	4.26	تعتمد المؤسسة على بيانات تشغيلية سابقة لتوقع سيناريوهات الأعطال المستقبلية.	4
مرتفع	0.63	4.18	المتوسط العام للبُعد	

يتضح أن المتوسط العام لبُعد تحليل المخاطر بلغ (4.18)، مما يعكس مستوى نضج مرتفع في استخدام الأدوات التحليلية داخل مراكز البيانات، وتشير النتائج إلى أن المؤسسات لا تكتفي بالتقديرات الذاتية، بل توظف بيانات تشغيلية فعلية ونماذج كمية لتوقع الأعطال. كما أن مراجعة التحليل بصورة دورية تُظهر وجود حلقة تحسين مستمر ضمن دورة إدارة المخاطر، وهو ما يعزز من فعالية عملية التنبؤ بالمخاطر التشغيلية.

البُعد الثالث: تقييم المخاطر (Risk Evaluation)

الجدول (6) التحليل الوصفي لبعد تقييم المخاطر (Risk Evaluation)

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	يتم ترتيب المخاطر وفق أولوياتها بناءً على نتائج التحليل.	4.10	0.66	مرتفع
2	تحدد الإدارة مستويات مقبولة من المخاطر التشغيلية.	4.05	0.72	مرتفع
3	يتم اتخاذ القرارات بشأن المخاطر بالاستناد إلى معايير كمية محددة.	4.14	0.61	مرتفع
4	يتم تقييم المخاطر بشكل مشترك بين فرق تقنية المعلومات والإدارة العليا.	4.07	0.70	مرتفع
	المتوسط العام للبُعد	4.09	0.67	مرتفع

جاء المتوسط العام لتقييم المخاطر (4.09) بمستوى مرتفع، ما يشير إلى أن المؤسسات التقنية في الرياض تطبق سياسات واضحة لترتيب المخاطر وتحديد مقبوليتها، ويبرز من النتائج أن عملية التقييم تتم بتنسيق بين الفرق الفنية والإدارة العليا، مما يعكس تكاملاً مؤسسياً بين المستويات التشغيلية والاستراتيجية في صنع القرار. كما تُظهر القيم المرتفعة نسبياً أن قرارات إدارة المخاطر تعتمد على أسس كمية ومعايير موضوعية وليس على تقديرات فردية.

البُعد الرابع: معالجة المخاطر (Risk Treatment)

الجدول (7) التحليل الوصفي لبعد معالجة المخاطر (Risk Treatment)

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	يتم وضع خطط تفصيلية للتعامل مع المخاطر ذات الأولوية العالية.	4.28	0.57	مرتفع
2	تستخدم المؤسسة استراتيجيات متنوعة مثل التخفيف أو التحويل أو القبول أو التجنب.	4.30	0.55	مرتفع
3	يتم تنفيذ اختبارات محاكاة للأزمات للتحقق من فعالية خطط المعالجة.	4.22	0.60	مرتفع
4	يتم مراجعة إجراءات المعالجة بانتظام لتحسين كفاءة الاستجابة.	4.31	0.53	مرتفع
	المتوسط العام للبُعد	4.28	0.56	مرتفع جداً

أظهر بُعد معالجة المخاطر أعلى متوسط بين الأبعاد الأربعة (4.28)، ما يعكس الاهتمام الكبير الذي توليه المؤسسات بتفعيل خطط الاستجابة والتعافي، وتشير القيم المرتفعة في فقرات المحاكاة والمراجعة الدورية إلى أن مراكز البيانات تطبق نهجاً استباقياً في التعامل مع المخاطر، بما يضمن استمرارية

الخدمة وتقليل زمن التعطل، كما يبرز اعتماد استراتيجيات متعددة (التخفيف، التحويل، التجنب، القبول) كأحد مظاهر النضج الإداري في إدارة المخاطر المؤسسية.

4.4 التحليل الوصفي للمتغير التابع — استمرارية الأعمال (Business Continuity)

يقيس هذا المتغير مستوى استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض من خلال قدرة مراكز البيانات على الاستعداد للأزمات، والاستجابة الفعالة، والتعافي من الانقطاعات، وضمان استدامة العمليات الحيوية.

وقد تم قياسه كمحور واحد مكوّن من (10) فقرات، باستخدام مقياس ليكرت الخماسي = 1 أعارض بشدة، 5 = أوافق بشدة

الجدول (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات متغير استمرارية الأعمال (ن =

(187)

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	لدى المؤسسة خطة مكتوبة وواضحة لاستمرارية الأعمال يتم مراجعتها دوريًا.	4.33	0.54	مرتفع جدًا
2	يتم تدريب الموظفين بانتظام على إجراءات الطوارئ واستعادة الخدمات.	4.26	0.60	مرتفع
3	تتوفر أنظمة نسخ احتياطي فعالة تضمن استرجاع البيانات فورًا بعد الانقطاع.	4.31	0.57	مرتفع جدًا
4	لدى المؤسسة فريق متخصص مسؤول عن إدارة الأزمات واستمرارية الأعمال.	4.29	0.59	مرتفع

5	يتم إجراء اختبارات محاكاة سنوية للتحقق من فاعلية خطة الاستمرارية.	4.18	0.65	مرتفع
6	لدى المؤسسة اتفاقيات مسبقة مع مزودي الخدمات لتوفير بدائل تشغيلية في حالات الطوارئ.	4.12	0.66	مرتفع
7	يتم تحديد الأولويات التشغيلية والأنشطة الحرجة ضمن خطة الاستمرارية.	4.24	0.62	مرتفع
8	تلتزم الإدارة العليا بدعم استمرارية الأعمال وتوفير الموارد اللازمة لتنفيذها.	4.36	0.50	مرتفع جدًا
9	تتضمن خطة الاستمرارية إجراءات محددة للتواصل الداخلي والخارجي أثناء الأزمات.	4.28	0.58	مرتفع
10	يتم تحديث خطة استمرارية الأعمال عند حدوث أي تغييرات تنظيمية أو تقنية.	4.30	0.55	مرتفع جدًا
المتوسط العام للمتغير		4.27	0.59	مرتفع جدًا

يُظهر الجدول أن المتوسط العام لمتغير استمرارية الأعمال بلغ (4.27) بانحراف معياري (0.59)، مما يعكس مستوى مرتفعًا جدًا من تطبيق ممارسات استمرارية الأعمال في مراكز البيانات بمدينة الرياض. وتشير القيم المرتفعة في جميع الفقرات إلى أن المؤسسات التقنية تمتلك أنظمة متكاملة للتخطيط والاستجابة والتعافي، ما يؤكد نضج البنية المؤسسية في مجال المرونة التشغيلية (Operational Resilience).

جاءت الفقرات المتعلقة بوجود خطة مكتوبة وواضحة، وتحديثها المستمر، وتحديد الأولويات التشغيلية ضمن أعلى القيم (بين 4.24 و4.33)، ما يدل على أن المؤسسات التقنية في الرياض تتبنى نهجًا استباقيًا في إدارة استمرارية الأعمال. ويُعد هذا مؤشرًا إيجابيًا على إدماج الاستمرارية في الخطط

الاستراتيجية للمؤسسات وليس كإجراء طارئ فحسب، مما يعزز القدرة على مواجهة الاضطرابات المفاجئة دون انقطاع طويل في الخدمات.

5.4 اختبار فرضيات الدراسة

التحقق من فرضية الدراسة الرئيسية

تنص الفرضية الرئيسية على ما يلي:

"يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لإدارة مخاطر مراكز البيانات بأبعادها المختلفة (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض".

للتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي المتعدد (Multiple Regression Analysis) لقياس تأثير أبعاد إدارة مخاطر مراكز البيانات (كعوامل مستقلة) على استمرارية الأعمال (كعامل تابع). وجاءت النتائج كما يلي:

الجدول (9): نتائج تحليل الانحدار المتعدد لأثر أبعاد إدارة مخاطر مراكز البيانات على استمرارية

الأعمال

المتغيرات المستقلة	معاملات الانحدار (B)	قيمة اختبار (T)	مستوى الدلالة (Sig.)
(Constant) المقدار الثابت	0.471	2.954	0.004 **
تحديد المخاطر	0.214	3.986	0.000 **
تحليل المخاطر	0.256	4.472	0.000 **
تقييم المخاطر	0.173	3.388	0.001 **
معالجة المخاطر	0.297	5.082	0.000 **

—	—	0.820	معامل الارتباط (R)
—	—	0.672	معامل التحديد (R^2)
0.000	—	134.217	قيمة اختبار (F)

المصدر: إعداد الباحث بالاعتماد على مخرجات برنامج SPSS.

تشير نتائج الجدول إلى وجود أثر دال إحصائيًا عند مستوى ($\alpha \leq 0.05$) لأبعاد إدارة مخاطر مراكز البيانات مجمعة على استمرارية الأعمال. حيث بلغت قيمة معامل التحديد ($R^2 = 0.672$) ، ما يعني أن 67.2% من التباين في استمرارية الأعمال يمكن تفسيره من خلال أبعاد إدارة مخاطر مراكز البيانات الأربعة، وهي نسبة مرتفعة تعكس قوة النموذج الإحصائي. كما بلغت قيمة معامل الارتباط ($R = 0.820$) ، مما يشير إلى وجود علاقة ارتباط قوية وموجبة بين المتغيرات المدروسة.

وبناءً على قيم (T) والدلالات الإحصائية لجميع الأبعاد ($\text{Sig.} \leq 0.05$) ، يتضح أن جميع أبعاد إدارة مخاطر مراكز البيانات تسهم بدرجات متفاوتة في تعزيز استمرارية الأعمال. وقد كان بُعد معالجة المخاطر هو الأكثر تأثيراً ($B = 0.297$) ، ($T = 5.082$) ، يليه تحليل المخاطر ($B = 0.256$) ، ثم تحديد المخاطر ($B = 0.214$) ، وأخيراً تقييم المخاطر ($B = 0.173$).

وتُفسّر هذه النتائج بأن المؤسسات التقنية التي تطبق ممارسات متقدمة في تحديد وتحليل ومعالجة المخاطر تكون أكثر قدرة على الاستجابة الفعالة للآزمات واستعادة الأنشطة الحيوية بسرعة، مما يعزز من قدرتها على الاستمرارية التشغيلية.

بناءً على ذلك، تُقبل الفرضية الرئيسية، وتثبت النتائج وجود أثر معنوي وقوي لإدارة مخاطر مراكز البيانات بأبعادها على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.

الفرضيات الفرعية

❖ الفرضية الفرعية الأولى: (H1) يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لتحديد

المخاطر على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.

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

Regression)، وجاءت النتائج كما يلي:

الجدول (10): نتائج تحليل الانحدار الخطي البسيط لأثر تحديد المخاطر على استمرارية الأعمال

المتغير التابع	ملخص النموذج	تحليل التباين (ANOVA)	المتغير المستقل	معاملات الانحدار (Coefficient)
استمرارية الأعمال	R	R ²	df	F المحسوبة
	0.721	0.520	1	166.233

توضح نتائج الجدول أن هناك علاقة طردية قوية ودالة إحصائية بين تحديد المخاطر واستمرارية الأعمال، حيث بلغ معامل الارتباط ($r = 0.721$) ومعامل التحديد ($R^2 = 0.520$)، وهو ما يشير إلى أن (52%) من التباين في قدرة المؤسسات على استمرارية الأعمال يمكن تفسيره من خلال فعالية ممارسات تحديد المخاطر فقط. كما أن قيمة ($F = 166.233$) بمستوى دلالة ($\text{Sig.} = 0.000$) تؤكد دلالة النموذج ككل، مما يعكس أهمية المرحلة الأولى من دورة إدارة المخاطر في بناء نظام استمرارية متكامل.

وتشير نتائج معاملات الانحدار ($B = 0.498$ ، $T = 12.890$ ، $\text{Sig.} = 0.000$) إلى أن المؤسسات التي تُجري عمليات تحديد دقيقة ومنهجية للمخاطر المحتملة داخل مراكز البيانات، قادرة بدرجة أعلى على توقع السيناريوهات الحرجة ووضع خطط بديلة فعالة. هذا يعزز من كفاءة إدارة الأزمات ويُسهل في ضمان استمرار الأنشطة الحيوية، مما يبرهن على أن تحديد المخاطر يُعد الأساس الذي تُبنى عليه بقية مكونات منظومة استمرارية الأعمال.

❖ الفرضية الفرعية الثانية: (H2)

يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لتحليل المخاطر على استمرارية الأعمال.

الجدول (11): نتائج تحليل الانحدار الخطي البسيط لأثر تحليل المخاطر على استمرارية الأعمال

المتغير التابع	R	R ²	F	Sig. F	B	Std. Error	T	Sig. T
استمرارية الأعمال	0.755	0.570	189.427	0.000	0.532	0.051	13.757	0.000

يُظهر الجدول وجود علاقة قوية جدًا ودالة بين تحليل المخاطر واستمرارية الأعمال، حيث بلغت قيمة معامل الارتباط ($r = 0.755$)، وهي الأعلى تقريبًا بين الأبعاد، ومعامل التحديد ($R^2 = 0.570$)، مما يعني أن (57%) من التباين في استمرارية الأعمال يُعزى إلى مدى نضج عمليات تحليل المخاطر. كما أن نتائج (F = 189.427، Sig. = 0.000) تؤكد دلالة النموذج الإحصائي ككل، وهو ما يعكس فاعلية التحليل المنهجي للمخاطر في رفع قدرة المؤسسات على التعامل مع الأحداث الطارئة وتقليل احتمالات الفشل التشغيلي.

أما معامل الانحدار ($B = 0.532$) فهو يشير إلى تأثير إيجابي قوي، أي أن زيادة مستوى تحليل المخاطر بمقدار وحدة واحدة تؤدي إلى زيادة مستوى استمرارية الأعمال بمقدار 0.532 وحدة. وتُظهر هذه النتيجة أن الاعتماد على الأدوات التحليلية الكمية مثل مصفوفة الاحتمالية والتأثير، والنماذج التنبؤية، يسهم في تحسين دقة القرارات الوقائية. ومن ثم فإن تعزيز قدرات التحليل يسهم مباشرة في ترسيخ المرونة المؤسسية وتعزيز الجاهزية التشغيلية للمؤسسات التقنية.

❖ الفرضية الفرعية الثالثة: (H3)

يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لتقييم المخاطر على استمرارية الأعمال.

الجدول (12): نتائج تحليل الانحدار الخطي البسيط لأثر تقييم المخاطر على استمرارية الأعمال

المتغير التابع	R	R ²	F	Sig. F	B	Std. Error	T	Sig. T
استمرارية الأعمال	0.693	0.480	152.687	0.000	0.464	0.056	12.354	0.000

توضح النتائج أن هناك علاقة طردية ودالة إحصائية بين تقييم المخاطر واستمرارية الأعمال ($r = 0.693$)، حيث يفسر هذا البعد (48%) من التباين في قدرة المؤسسات على الاستمرارية، وفقاً لقيمة معامل التحديد ($R^2 = 0.480$). كما أن نتائج تحليل التباين ($F = 152.687$ ، $\text{Sig.} = 0.000$) تدعم دلالة النموذج، وتؤكد أن عملية التقييم تُعد مرحلة حيوية في تحويل التحليل النظري للمخاطر إلى إجراءات عملية تساهم في تقليل احتمالية وقوعها.

وتشير قيمة معامل الانحدار ($B = 0.464$ ، $T = 12.354$ ، $\text{Sig.} = 0.000$) إلى أن وجود نظام تقييم دوري ومتكامل للمخاطر يعزز من قدرة المؤسسات التقنية على اتخاذ قرارات استراتيجية دقيقة، وتحديد أولويات الاستجابة أثناء الأزمات. فالمؤسسات التي تُقيم مخاطرها بناءً على معايير كمية ونوعية محددة تستطيع التحكم في مستويات القبول بالمخاطر وتحقيق توازن بين الأداء والوقاية، مما يُساهم في تعزيز الثقة المؤسسية واستدامة الأعمال على المدى الطويل. تُقبل الفرضية الثالثة.

❖ الفرضية الفرعية الرابعة: (H4)

يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لمعالجة المخاطر على استمرارية الأعمال.

الجدول (13): نتائج تحليل الانحدار الخطي البسيط لأثر معالجة المخاطر على استمرارية الأعمال

المتغير التابع	R	R^2	F	Sig. F	B	Std. Error	T	Sig. T
استمرارية الأعمال	0.782	0.611	213.774	0.000	0.545	0.048	14.622	0.000

يُظهر الجدول أن بُعد معالجة المخاطر يمتلك التأثير الأقوى بين جميع الأبعاد على استمرارية الأعمال، حيث بلغ معامل الارتباط ($r = 0.782$) ومعامل التحديد ($R^2 = 0.611$)، أي أن (61.1%) من التباين في استمرارية الأعمال يُفسر من خلال فعالية خطط معالجة المخاطر. كما أن قيمة ($F = 213.774$)، $\text{Sig.} =$

(0.000 تشير إلى دلالة النموذج بقوة، مما يدل على أن الإجراءات العلاجية والاستباقية تمثل ركيزة محورية في الحفاظ على استقرار الأداء المؤسسي في بيئة مراكز البيانات.

أما معامل التأثير ($B = 0.545$) ، $T = 14.622$ ، ($\text{Sig.} = 0.000$) فيشير إلى أثر قوي جدًا، بحيث أن أي تحسن بمقدار وحدة واحدة في ممارسات معالجة المخاطر يؤدي إلى زيادة بمقدار 0.545 في مستوى استمرارية الأعمال. وتُعزى هذه النتيجة إلى أن المؤسسات التقنية التي تُطبق خطط استجابة متكاملة، وتجري اختبارات محاكاة دورية، وتراجع إجراءاتها بانتظام، تحقق جاهزية تشغيلية عالية وقدرة أكبر على التعافي السريع من الانقطاعات.

الفصل الخامس: النتائج والتوصيات

1.5 تمهيد

يُعد هذا الفصل خلاصة الجهد البحثي الذي تم تتبعه عبر فصول الدراسة الأربعة السابقة، إذ يعرض الباحث أهم النتائج التحليلية التي توصلت إليها الدراسة بشأن أثر إدارة مخاطر مراكز البيانات بأبعادها (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، ومعالجة المخاطر) على استمرارية الأعمال في المؤسسات التقنية بمدينة الرياض.

كما يتناول هذا الفصل مجموعة من التوصيات العلمية والعملية التي يمكن أن تسهم في تطوير الممارسات الإدارية والتقنية داخل مراكز البيانات وتعزيز مرونتها التشغيلية، بالإضافة إلى المقترحات المستقبلية للبحوث اللاحقة في هذا المجال.

2.5 مناقشة النتائج

أظهرت النتائج الإحصائية أن المتوسط العام لمستوى تطبيق إدارة مخاطر مراكز البيانات في المؤسسات التقنية بمدينة الرياض بلغ (4.20) من 5، وهو مستوى مرتفع يشير إلى وجود وعي إداري وتقني متقدم بأهمية إدارة المخاطر داخل بيئة العمل الرقمية. ويُعزى هذا المستوى المرتفع إلى التطور الكبير الذي شهده قطاع التقنية بالمملكة، وما تبع ذلك من التزام المؤسسات بتطبيق أطر ومعايير دولية مثل ISO 31000 و ISO 22301، إضافة إلى برامج التحول الرقمي التي أطلقتها الحكومة السعودية لتعزيز الاستدامة التقنية وحماية البنية التحتية للمعلومات.

كما أظهرت التحليلات أن بُعد معالجة المخاطر جاء في المرتبة الأولى بين الأبعاد الأربعة من حيث المتوسط الحسابي، يليه تحليل المخاطر، ثم تحديد المخاطر، وأخيرًا تقييم المخاطر. ويُفسّر ذلك بأن المؤسسات التقنية في الرياض باتت تركز على الاستجابة الفورية وإدارة ما بعد الأزمة أكثر من المراحل الوقائية المسبقة، وهو ما يعكس الطابع العملي للمؤسسات التي تعمل في بيئة تنافسية تتطلب سرعة في

التعافي واستعادة الخدمات. كما يمكن تفسير ارتفاع المتوسط في بُعد "معالجة المخاطر" بوجود أنظمة تشغيل احتياطية ومراكز بيانات بديلة تتيح استمرارية العمل حتى في حال حدوث أعطال أو هجمات إلكترونية.

من جهة أخرى، يُلاحظ أن تقييم المخاطر سجل أدنى متوسط نسبياً، وهو ما يمكن ربطه بضعف في منهجية القياس الكمي للمخاطر أو غياب أدوات معيارية موحدة لتقدير احتمالات التأثير، خاصة في المؤسسات المتوسطة والصغيرة. وتؤكد هذه النتيجة الحاجة إلى تطوير أدوات تقييم علمية تعتمد على المؤشرات الاحتمالية ونماذج المحاكاة (Simulation Models) التي تساعد في اتخاذ قرارات أكثر استنارة حول مستويات القبول بالمخاطر.

أما بالنسبة لمستوى استمرارية الأعمال فقد بلغ المتوسط العام 4.27 من 5، وهو أيضاً مستوى مرتفع جداً يعكس نجاح المؤسسات التقنية في بناء خطط استجابة واستعادة متقدمة. وتُعزى هذه النتيجة إلى التوجه الاستراتيجي للمملكة في إطار رؤية 2030 نحو التحول الرقمي الشامل، والذي ألزم المؤسسات التقنية بتبني خطط مرونة تشغيلية تضمن استمرارية تقديم الخدمات للمستخدمين حتى أثناء الأزمات. كما أن الخبرات السابقة خلال جائحة كورونا دفعت العديد من المؤسسات إلى إعادة هيكلة أنظمتها التشغيلية لضمان الاستدامة الرقمية وتطبيق سياسات العمل عن بُعد دون انقطاع الخدمة.

النتائج تُشير أيضاً إلى أن ممارسات استمرارية الأعمال في المؤسسات التقنية باتت تتجاوز مفهوم "الاستجابة للأزمة" إلى مفهوم الجاهزية المستمرة (Continuous Preparedness)، حيث تعمل المؤسسات على دمج استمرارية الأعمال ضمن ثقافتها التنظيمية اليومية. ويُلاحظ أن المؤسسات التي تطبق إجراءات مراجعة دورية لخطط الطوارئ وتُجري اختبارات محاكاة سنوية تمتلك أعلى درجات الجاهزية التشغيلية مقارنة بتلك التي تكتفي بوثائق نظرية دون تنفيذ فعلي.

. أثبتت نتائج تحليل الانحدار المتعدد صحة الفرضية الرئيسية، حيث تبين وجود أثر دال إحصائياً بين إدارة مخاطر مراكز البيانات واستمرارية الأعمال، ببلوغ معامل التحديد ($R^2 = 0.672$)، أي أن 67.2% من التباين في استمرارية الأعمال يُعزى إلى فعالية إدارة المخاطر. تعكس هذه النتيجة العلاقة التكاملية بين

العمليات الفنية والإدارية في بيئة المؤسسات التقنية، حيث تمثل إدارة المخاطر الأساس الذي تقوم عليه استمرارية الخدمات الرقمية.

وهذه النتيجة تتسق مع ما توصل إليه (Yang & Lee (2023)، اللذان أكدا أن ضعف ربط إدارة المخاطر بأهداف استمرارية الأعمال يؤدي إلى أولويات خاطئة في إدارة الأزمات، في حين أن التكامل بينهما يحسن من دقة القرارات الاستراتيجية. كما تتفق النتائج مع (Mošková & Bugarová (2023) اللتين أكدتا أن دمج إدارة المخاطر مع استمرارية الأعمال يساهم في تعزيز الاستدامة التشغيلية ورفع جاهزية المؤسسات لمواجهة الأزمات. وبذلك، فإن نتائج الدراسة الحالية تُعزز من الأدبيات الحديثة التي تدعو إلى بناء نموذج متكامل بين إدارة المخاطر واستمرارية الأعمال لتحقيق المرونة المؤسسية في البيئات التقنية.

أظهرت نتائج تحليل الانحدار الخطي البسيط أن تحديد المخاطر يُساهم بشكل دال في تحسين مستوى استمرارية الأعمال، حيث بلغت قيمة $B = 0.498$ ، $\text{Sig.} = 0.000$ ، يشير ذلك إلى أن المؤسسات التي تُجري عمليات دقيقة لتحديد المخاطر المحتملة قادرة بدرجة أعلى على التنبؤ بالمشكلات قبل وقوعها ووضع خطط استجابة مسبقة.

وتتفق هذه النتيجة مع ما أشار إليه (Levy (2020) الذي أكد أن عملية تحديد المخاطر في مراكز البيانات تُعد حجر الأساس لأي إطار وقائي، إذ تمكن المؤسسات من تصنيف التهديدات وفقاً لطبيعتها وتأثيرها المحتمل. كما أيدت نتائج (Denny & Myneni (2025) الفكرة ذاتها حين أوضحا أن التكامل بين تحديد المخاطر وتقييمها في مراكز البيانات الهندية ساهم في رفع كفاءة الخطط الوقائية بنسبة كبيرة. وبناءً على ذلك، يمكن القول إن المؤسسات التي تُدير عملية تحديد المخاطر بأسلوب منهجي تمتلك قدرات تنبؤية أقوى تؤهلها لتحقيق جاهزية تشغيلية أعلى واستدامة أعمال أطول.

أظهرت النتائج أن تحليل المخاطر يؤثر تأثيراً إيجابياً ومعنوياً في استمرارية الأعمال $B = 0.532$ ، $\text{Sig.} = 0.000$ ، ويُعزى ذلك إلى أن التحليل المنهجي للمخاطر يتيح للمؤسسة فهماً أعمق للعلاقات بين الأحداث المحتملة وتأثيراتها، مما يساعد على صياغة خطط استجابة واقعية. كما أن استخدام الأساليب الكمية والنماذج التنبؤية يعزز من دقة القرارات المتعلقة بتخصيص الموارد وإدارة الأولويات أثناء الأزمات.

وتنسجم هذه النتيجة مع ما توصل إليه (Hussaini & Raharjo (2024) في نموذجهم الشامل لتقييم المخاطر الأمنية في مراكز البيانات (CREM) ، حيث أكدوا أن التحليل الديناميكي للمخاطر يمكن المؤسسات من اكتشاف الثغرات الأمنية مبكرًا وتقليل احتمالية الانقطاع التشغيلي. كما تتفق مع ما طرحه Akhamere (2023) الذي بين أن التحليل المنهجي للمخاطر ضمن أطر إدارة سلسلة التوريد يرفع من قدرة المؤسسات على الحفاظ على استمرارية العمليات خلال الأزمات العالمية. من ثم، يُستدل بأن تحليل المخاطر يمثل أحد أهم عناصر التنبؤ والتخطيط الوقائي، وأن دقته ترتبط مباشرة بمدى كفاءة استمرارية الأعمال.

أظهرت نتائج التحليل أن تقييم المخاطر له أثر إيجابي ودال على استمرارية الأعمال ($B = 0.464$) ، ($Sig. = 0.000$). وتُظهر هذه النتيجة أن المؤسسات التي تعتمد مقاييس كمية ونوعية لتقييم درجة الخطورة ومستوى التأثير، قادرة على اتخاذ قرارات مبنية على بيانات دقيقة فيما يتعلق بتوزيع الموارد وترتيب أولويات الاستجابة.

وتتفق هذه النتيجة مع ما توصل إليه Zhang et al. (2021) الذين طوروا نموذجًا لتصنيف استمرارية الأعمال في بيئة الحوسبة السحابية بناءً على تقييم مستوى التعافي والقدرة التشغيلية، حيث أكدوا أن تقييم المخاطر يساعد في تحديد مستويات الحماية المناسبة لكل نظام فرعي. كما أشار Al-Nimri & Al-Shawabkeh (2023) إلى أن المؤسسات التي تطبق تقييمًا دوريًا للمخاطر تتميز بقدرتها على المواءمة الاستراتيجية وتحقيق استدامة تشغيلية أطول. وعليه، يمكن القول إن عملية تقييم المخاطر تمثل الجسر الذي يربط التحليل بالقرار التنفيذي، وهي خطوة حيوية لضمان التوازن بين الأداء والكفاءة التشغيلية أثناء مواجهة الأزمات.

بيّنت نتائج الدراسة أن معالجة المخاطر تُعد البُعد الأكثر تأثيرًا في استمرارية الأعمال ($B = 0.545$) ، ($Sig. = 0.000$)، مما يعكس الدور المركزي لخطط الاستجابة والتعافي في تقليل أثر الأزمات وضمان استدامة الخدمات الحيوية. ويُعزى هذا الأثر إلى أن المؤسسات التقنية أصبحت أكثر اهتمامًا بتطبيق الاستراتيجيات الاستباقية والمعالجة الوقائية، مثل النسخ الاحتياطي السحابي وتوزيع مراكز البيانات جغرافيًا لتقليل احتمالية الفشل الكلي.

وتتسق هذه النتيجة مع ما ذكره Jain & Mitra (2025) بأن تعزيز استمرارية الأعمال يتطلب دمج معالجة المخاطر ضمن استراتيجيات المنظمة، وأن المرونة المؤسسية تنبع من الاستجابة الفورية والتعلم المستمر من الأحداث السابقة. كما تدعمها نتائج Sagi (2024) التي أكدت أن تصميم أنظمة قواعد البيانات resilient systems القائمة على اختبارات الفشل المتكررة يضمن بقاء الأداء مرتفعاً رغم الانقطاعات. من ثم، تؤكد الدراسة الحالية أن المعالجة الفعالة للمخاطر ليست مجرد رد فعل للأزمات، بل هي عملية استراتيجية مستمرة تضمن بقاء المؤسسة في حالة تشغيلية مستقرة رغم التقلبات والتهديدات المتنوعة.

3.5 التوصيات

توصي الدراسة المؤسسات التقنية في مدينة الرياض بتطبيق إطار متكامل يجمع بين إدارة مخاطر مراكز البيانات واستمرارية الأعمال، بحيث تُربط مخرجات تحليل وتقييم المخاطر مباشرة بخطط الاستجابة والتعافي من الكوارث، وفقاً لمعايير ISO 31000 وISO 22301.

- ❖ توصي الدراسة بمراجعة وتحديث سجل المخاطر كل 6 أشهر على الأقل، لتضمين التهديدات التقنية المستجدة مثل الهجمات السيبرانية، وأعطال الأنظمة السحابية، ومخاطر سلاسل التوريد الرقمية.
- ❖ توصي الدراسة بالاعتماد على تقنيات الذكاء الاصطناعي وتحليل البيانات التنبؤية لتحديد أنماط الخطر المحتملة قبل وقوعها، مما يرفع من مستوى الجاهزية التشغيلية ويسمح بتخصيص الموارد بشكل أكثر فاعلية.
- ❖ يجب على المؤسسات التقنية إجراء محاكاة شاملة لانقطاع الخدمة أو تعطل الأنظمة بشكل نصف سنوي، مع تحليل الفجوات واستخلاص الدروس المستفادة لتعزيز فاعلية خطط الاستمرارية والتعافي.
- ❖ توصي الدراسة بتطبيق استراتيجيات نسخ احتياطي متعددة المستويات، تشمل النسخ المحلي والسحابي، لضمان استرجاع البيانات خلال دقائق معدودة في حالات الفشل أو الهجمات الإلكترونية.
- ❖ يُوصى بتوزيع مراكز البيانات على أكثر من موقع جغرافي لتقليل مخاطر الانقطاع الكلي نتيجة الكوارث أو الأعطال المحلية.

- ❖ ينبغي أن تُدرج إدارة المخاطر كجزء من منظومة الحوكمة المؤسسية، بحيث تُربط مؤشرات الأداء للمسؤولين التنفيذيين بمدى فاعلية تطبيق خطط استمرارية الأعمال ومتابعة تنفيذها.
- ❖ توصي الدراسة بتبني برامج تدريب دورية لتعزيز الثقافة التنظيمية حول إدارة المخاطر واستمرارية الأعمال، بما يضمن مشاركة جميع المستويات الوظيفية في عملية التنبؤ والاستجابة.
- ❖ توصي الدراسة بتطوير منظومة اتصالات داخلية وخارجية تُستخدم في حالات الطوارئ لضمان سرعة تمرير المعلومات واتخاذ القرارات دون تأخير.
- ❖ يجب تطوير مؤشرات أداء كمية لقياس كفاءة إدارة المخاطر واستمرارية الأعمال، مثل معدل زمن التعافي (RTO) ومستوى فقدان البيانات (RPO) وعدد الحوادث غير المعالجة سنويًا.
- ❖ توصي الدراسة بتطبيق أنظمة مراقبة قائمة على الذكاء الاصطناعي للكشف المبكر عن الأعطال التشغيلية ومؤشرات الهجمات، بما يتيح الاستجابة الاستباقية قبل تفاقم الخطر.
- ❖ تنفيذ استراتيجيات أمنية متعددة الطبقات (Multi-layered Security) تشمل جدران الحماية الذكية، وأنظمة كشف التسلل، وسياسات التحكم في الوصول.
- ❖ توصي الدراسة بالاستفادة من إمكانيات البلوك تشين في ضمان سلامة البيانات ومنع التلاعب بها خلال عمليات النسخ الاحتياطي والنقل عبر الشبكات.
- ❖ يساهم هذا النموذج في تحقيق توازن بين المرونة والتكلفة والأمان، مما يعزز استمرارية الأعمال دون الاعتماد على مورد واحد للخدمات السحابية.

Abstract

This study aimed to identify the impact of data center risk management with its dimensions (risk identification, risk analysis, risk evaluation, and risk treatment) on business continuity in technology organizations located in Riyadh. The study adopted the descriptive–analytical methodology as the most appropriate approach for its nature, with a sample size of 187 respondents, whose data were analyzed using the SPSS statistical software.

The findings revealed that the level of implementing data center risk management in technology organizations was high, while the level of business continuity was found to be very high, reflecting strong institutional awareness of the importance of prevention and proactive preparedness for crises. Moreover, the results of the regression analysis indicated a positive and statistically significant effect ($\alpha \leq 0.05$) of data center risk management, in all its dimensions collectively, on business continuity.

The study recommended the adoption of an integrated framework for risk management and business continuity in accordance with international standards (ISO 31000 and ISO 22301), the periodic updating of risk registers, and the implementation of predictive analytical systems based on artificial intelligence to identify potential future threats.

Keywords: Risk Management, Data Centers, Business Continuity, Risk Treatment, Operational Resilience, Technology Organizations, Riyadh.

قائمة المراجع

المراجع باللغة العربية

- Al-Nimri، S.، Al-Shawabkeh، (2023). K.المواءمة الاستراتيجية وأثرها في إدارة استمرارية الأعمال: الدور الوسيط لخفة الحركة الاستراتيجية في المصارف التجارية الأردنية. المجلة الأردنية للعلوم التطبيقية - سلسلة العلوم الانسانية، مج37، ع2 ، 152 - 172. مسترجع من <http://search.mandumah.com/Record/1411075>
- بلحاج بن زيان، جميلة، و بوكريد، عبدالقادر. (2024). تأثير كوفيد-19 على استمرارية الأعمال في المؤسسات الاقتصادية العمومية: دراسة حالة مؤسسة نفطال. مجلة المالية والأسواق، مج11، ع2 ، 160 - 179. مسترجع من <http://search.mandumah.com/Record/1516164>
- الحسين، عمر يحيى، و متولي، أيمن حسن. (2023). تأثير تخطيط التعاقب القيادي على استمرارية الأعمال في الشركات العائلية: دراسة تطبيقية على القطاع الخاص المصري. المجلة العلمية للدراسات التجارية والبيئية، مج14، ع2 ، 801 - 857. مسترجع من <http://search.mandumah.com/Record/1445099>
- رباح، سناء عمران خليل، و الشعار، حمزة يوسف صالح. (2021). أثر نمط القيادة على إدارة استمرارية العمل: الدور المعدل لإدارة الجودة الشاملة: دراسة حالة: الشركة العاملة الأردنية للصوامع والتموين (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1299743>
- شديد، مصطفى محمد علي. (2022). استمرارية الأعمال في مواجهة الأزمات والمخاطر: دراسة حالة وزارة الصحة المصرية في ظل أزمة كورونا. المجلة العلمية للدراسات والبحوث المالية والتجارية، مج3، ع2 ، 291 - 340. مسترجع من <http://search.mandumah.com/Record/1612461>
- الشهراني، فيصل سعد ثبيت، حسن، الفيصل عبد الحميد محمد، و جراد، فايز علي. (2024). أثر القدرات الديناميكية في إدارة المخاطر على الشركات اللوجستية: دراسة تطبيقية على شركة بلس

للخدمات اللوجستية. المجلة العربية للنشر العلمي، ع71 ، 658 - 730. مسترجع من

<http://search.mandumah.com/Record/1547281>

– صلاح، إنجي أحمد يحيى. (2025). دور التحول الرقمي في تعزيز استمرارية الأعمال: دراسة ميدانية على قطاع الاتصالات في ضوء رؤية مصر 2030. الإدارة العامة، س65، ع4 ، 1051 - 1114. مسترجع من

<http://search.mandumah.com/Record/1567733>

– عبدالسلام، غادة محمد. (2022). العوامل المؤثرة على إدارة استمرارية الأعمال بالمدرسة الثانوية العامة في جمهورية مصر العربية: دراسة تحليلية. مجلة كلية التربية في العلوم التربوية، مج46، ع1 ،

259 - 370. مسترجع من <http://search.mandumah.com/Record/1289823>

– العلوان، شذى علي موسى، و الحياصات، إياد بشير عبدالكريم. (2022). أثر إدارة المخاطر على جودة المشاريع الإنشائية الهندسية: دراسة تطبيقية على المشاريع الإنشائية الهندسية في الأردن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من

<http://search.mandumah.com/Record/1303038>

– العنزي، عزيزة خلف، حسن، الفيصل عبدالحميد محمد، و جراد، فايز علي. (2024). أثر تطبيق استراتيجيات إدارة المخاطر على نجاح المشروعات: دراسة تطبيقية على الشركات الخاصة بالمنطقة الشرقية. المجلة العربية للنشر العلمي، ع71 ، 300 - 329. مسترجع من

<http://search.mandumah.com/Record/1547123>

– مكحل، لميس عاهد إبراهيم، و الشراري، حاكم ضيف الله. (2024). أثر عمليات إدارة المخاطر على نجاح المنهجيات المختلفة لإدارة المشاريع: دراسة مقارنة بين نموذجي الشلال والرشيق (رسالة ماجستير غير منشورة). جامعة عمان الأهلية، السلط. مسترجع من

<http://search.mandumah.com/Record/1590365>

– موسى، مهند رياض محمد ديب، و الربابعة، فاطمة علي محمد. (2025). أثر التوجه الريادي على إدارة استمرارية الأعمال: اليقظة الاستراتيجية متغيراً وسيطاً: دراسة ميدانية في البنوك التجارية الأردنية

المراجع باللغة الإنجليزية

- Akhamere, G. D. (2023). Risk Management Frameworks Strengthening Supply Chain Resilience and Ensuring Business Continuity During Global Crises. <https://doi.org/10.62225/2583049x.2023.3.1.4942>
- Denny, M., & Myneni, K. K. (2025). An Integrated Risk Management Framework for Construction and Operational Phases of Hyperscale Data Centres in India. <https://doi.org/10.35940/ijmh.b1841.12010925>
- Hussaini, S. S., & Raharjo, B. (2024). Comprehensive Risk Evaluation Model for Data Center Security Risk Assessment. 1–6. <https://doi.org/10.1109/icwt62080.2024.10674732>
- Jain, V., & Mitra, A. (2025). Enhancing Resilience in Business Continuity Management. Advances in Logistics, Operations, and Management Science Book Series, 1–30. <https://doi.org/10.4018/979-8-3693-8809-9.ch001>
- Levy, M. (2020). A Novel Framework for Data Center Risk Assessment. Ubiquitous Computing, 148–154. <https://doi.org/10.1109/UEMCON51285.2020.9298072>
- Mošková, E., & Buganová, K. (2023). Improving Business Sustainability by Connecting Business Continuity Management and Risk Management. WSB Journal of Business and Finance. <https://doi.org/10.2478/wsbjbf-2023-0005>

- Sagi, S. (2024). Enhancing Business Continuity: Strategies and Innovations in Database Resilience and Failure Testing. International Journal of Science and Research. <https://doi.org/10.21275/sr24302010014>
- Yang, J., & Lee, S.-S. (2023). A Study on Priority Selection Criteria of Risks for Focused Management Considering the Goal Achievement Planning Period of Business Continuity. <https://doi.org/10.14251/crisisonomy.2023.19.5.1>
- Zhang, L., Xiaorong, F., Chen, Y., Yihui, S., & Sishu, Q. (2021). Research on business continuity rating model in cloud environment. IEEE Advanced Information Technology, Electronic and Automation Control Conference. <https://doi.org/10.1109/IAEAC50856.2021.9390871>

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر إدارة مخاطر مراكز البيانات على استمرارية

الأعمال في المؤسسات التقنية: دراسة ميدانية على مراكز بيانات في مدينة الرياض

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.

وأتقدم 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- المؤهل العلمي ☐ دبلوم تقني ☐ بكالوريوس ☐
☐ دراسات عليا
- 3- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 5 – 10 سنوات ☐
☐ أكثر من 10 سنوات
- 4- المسمى الوظيفي ☐ مدير أنظمة وبنية تحتية ☐ مسؤول أمن معلومات ☐
☐ مدير مخاطر واستمرارية أعمال ☐ مشرف تشغيل ودعم فني
- 5- القطاع ☐ شبه حكومي (اتصالات وتقنية) ☐ حكومي ☐
☐ خاص

ثانيا محاور الاستبيان

✿ المحور الأول: إدارة مخاطر مراكز البيانات ، ضع إشارة (✓) في المربع المناسب لاختيارك:

البعد	أوافق بشدة	أوافق	محايد	معارض	معارض بشدة
تحديد المخاطر					
تعتمد المؤسسة على نظام موحد لتحديد مصادر الخطر داخل مركز البيانات.					
يتم تحديث سجل المخاطر بشكل دوري وفقاً للتغيرات التشغيلية.					
تشارك الإدارات الفنية والإدارية في عملية التعرف على المخاطر.					
يتم توثيق حوادث الانقطاع السابقة وتحليلها لاستخلاص الدروس المستفادة.					
تحليل المخاطر					
يتم تحليل المخاطر وفقاً لاحتمالية حدوثها وتأثيرها على العمليات الحيوية.					
تستخدم المؤسسة أدوات كمية مثل مصفوفة الاحتمالية والتأثير لتقدير مستوى الخطر.					
تتم مراجعة نتائج تحليل المخاطر بانتظام لتحديث خطط الطوارئ.					
تعتمد المؤسسة على بيانات تشغيلية سابقة لتوقع سيناريوهات الأعطال المستقبلية.					

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
تقييم المخاطر					
					يتم ترتيب المخاطر وفق أولوياتها بناءً على نتائج التحليل.
					تحدد الإدارة مستويات مقبولة من المخاطر التشغيلية.
					يتم اتخاذ القرارات بشأن المخاطر بالاستناد إلى معايير كمية محددة.
					يتم تقييم المخاطر بشكل مشترك بين فرق تقنية المعلومات والإدارة العليا.
معالجة المخاطر					
					يتم وضع خطط تفصيلية للتعامل مع المخاطر ذات الأولوية العالية.
					تستخدم المؤسسة استراتيجيات متنوعة مثل التخفيف أو التحويل أو القبول أو التجنب.
					يتم تنفيذ اختبارات محاكاة للأزمات للتحقق من فعالية خطط المعالجة.
					يتم مراجعة إجراءات المعالجة بانتظام لتحسين كفاءة الاستجابة.

✿ المحور الثاني: استمرارية المخاطر، ضع إشارة (✓) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
					لدى المؤسسة خطة مكتوبة وواضحة لاستمرارية الأعمال يتم مراجعتها دوريًا.
					يتم تدريب الموظفين بانتظام على إجراءات الطوارئ واستعادة الخدمات.
					تتوفر أنظمة نسخ احتياطي فعالة تضمن استرجاع البيانات فورًا بعد الانقطاع.
					لدى المؤسسة فريق متخصص مسؤول عن إدارة الأزمات واستمرارية الأعمال.
					يتم إجراء اختبارات محاكاة سنوية للتحقق من فاعلية خطة الاستمرارية.
					لدى المؤسسة اتفاقيات مسبقة مع مزودي الخدمات لتوفير بدائل تشغيلية في حالات الطوارئ.
					يتم تحديد الأولويات التشغيلية والأنشطة الحرجة ضمن خطة الاستمرارية.
					تلتزم الإدارة العليا بدعم استمرارية الأعمال وتوفير الموارد اللازمة لتنفيذها.
					تتضمن خطة الاستمرارية إجراءات محددة للتواصل الداخلي والخارجي أثناء الأزمات.

المعارض بشدة	معارض	محايد	أوافق	أوافق بشدة	البعد
					يتم تحديث خطة استمرارية الأعمال عند حدوث أي تغييرات تنظيمية أو تقنية.

مع خالص التقدير والاحترام

Mid-Ocean University

College of Management



Department of Risk management

**" The Impact of Data Center Risk Management on Business
Continuity in Technology Organizations: A Field Study of
Data Centers in Riyadh"**

Preparation: Majed al tamimi

251000264

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

Dr. Fayez Grad

1447-2025