

جامعة ميد أوشن



كلية الإدارة

ماجستير إدارة مخاطر

دور إدارة المخاطر في تطوير الأنظمة الأمنية المتكاملة لحماية البنية
التحتية لقطاع الطاقة بالمملكة العربية السعودية

إعداد الطالب/

عبد السلام عامر ال مسفر

251002791

إشراف/

د. الفيصّل عبد الحميد محمد حسن

د.فايز جراد

العام الدراسي:

1447 – 2025



إِهْدَاء

إلى من كان لهم الفضل بعد الله تعالى في تحقيق هذا العمل العلمي،

إلى والديَّ العزيزين رمز التضحية والعطاء،

إلى أساتذتي الأفاضل الذين لم يبخلوا بتوجيهاتهم ونصحهم،

إلى زملائي الذين شاركوني رحلة البحث بكل تفاصيلها،

إلى كل من علّمني أن الصبر طريق النجاح،

وأن الطموح لا يقف عند حدود،

إلى من ألهموني الإصرار والسعي نحو الأفضل،

أهدي هذا العمل المتواضع عربون تقدير وامتنان،

راجيا أن يكون لبنة في بناء العلم،

وسبيلاً لخدمة المجتمع والوطن.

شكر وقدر

ليس بعد التمام أجمل من الحمد، فالحمد لله والشكر له كما ينبغي لجلال وجهه وعظيم سلطانه وكما ينبغي لجزيل فضله وعظيم إحسانه على ما أنعم به على من إتمام هذا البحث.

ثم أنه لا يسعني الا أن أشيد بالفضل وأقر بالمعروف لكل من ساهم في إنجاز هذا البحث.

كل الشكر للجهات التي دعمتني وساعدتني وخصتني بالتوجيه والتصويب لإتمام بحثي على الوجه الصحيح.

كما أتقدم بالشكر لمن كان لتوجيهاتهم الدور الكبير في إنجاز هذا المشروع وكل من مد لي يد العون من قريب وبعيد ولو بدعوة بظهر الغيب، بارك الله فيهم جميعاً وجزاهم الله عني الجزاء الأوفى وأسأل الله أن ينفع بهذا البحث على قدر العناء فيه وأن يجعله خالصاً لوجهه الكريم إنه على ذلك لقادر

المستخلص

هدفت هذه الدراسة إلى تحليل أثر إدارة المخاطر بأبعادها الأربعة (تحديد المخاطر، تقييم المخاطر، معالجات واستجابات المخاطر، مراقبة ومتابعة المخاطر) على تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية، واعتمدت الدراسة على المنهج الوصفي التحليلي لملاءمته لطبيعة الموضوع، واستخدمت أداة الاستبانة لجمع البيانات من عينة قوامها (320) موظفًا من العاملين في الإدارات الأمنية والفنية في مؤسسات قطاع الطاقة السعودية. تم تحليل البيانات باستخدام البرنامج الإحصائي SPSS.

أظهرت النتائج أن مستوى ممارسة إدارة المخاطر في مؤسسات قطاع الطاقة جاء مرتفعًا بمتوسط (4.23)، كما تبين وجود أثر دال إحصائيًا لإدارة المخاطر بأبعادها الأربعة على تطوير الأنظمة الأمنية المتكاملة ($R^2 = 0.717$)، $F = 132.546$ ، $Sig. = 0.000$ ، وتبين أن بُعد معالجات واستجابات المخاطر هو الأكثر تأثيرًا، يليه تقييم المخاطر، ثم تحديد المخاطر، وأخيرًا مراقبة ومتابعة المخاطر.

و أوصت الدراسة بضرورة إنشاء مركز وطني لتكامل إدارة المخاطر والأمن الصناعي في قطاع الطاقة، وتبني إطار مؤسسي موحد يدمج بين إدارة المخاطر والأمن التقني، إضافة إلى تعزيز استخدام تقنيات الذكاء الاصطناعي والمراقبة التنبؤية في تحليل المخاطر ومتابعتها، ودعم برامج التدريب المستمر للعاملين في المجالات الأمنية والتقنية لضمان الجاهزية والاستجابة الفعالة للأزمات المستقبلية.

الكلمات المفتاحية: إدارة المخاطر، الأنظمة الأمنية المتكاملة، حماية البنية التحتية، قطاع الطاقة، المملكة العربية السعودية.

قائمة المحتويات

أ	بسم الله الرحمن الرحيم.....
ب	الإهداء.....
ج	الشكر والتقدير.....
د	المستخلص.....
هـ	قائمة المحتويات.....
ح	قائمة الجداول.....
9	الفصل الأول: الإطار النظري.....
9	1.1 مقدمة:.....
2	2.1 مشكلة الدراسة.....
3	3.1 أهمية الدراسة:.....
5	4.1 أهداف الدراسة:.....
5	5.1 تساؤلات الدراسة.....
6	6.1 فروض الدراسة:.....
6	7.1 الدراسات السابقة:.....
18	8.1 الفجوة البحثية:.....
19	9.1 المنطلقات النظرية للدراسة:.....
22	10.1 المنهجية وطرق البحث:.....
23	11.1 الأساليب الإحصائية المستخدمة.....

12.1 الأساليب الإحصائية الاستنتاجية.....	24
13.1 حدود الدراسة:.....	24
الفصل الثاني: الإطار النظري.....	25
المبحث الأول: إدارة المخاطر بأبعادها.....	25
1.1.2 التمهيد.....	25
2.1.2 مفهوم إدارة المخاطر.....	25
3.1.2 أهمية إدارة المخاطر.....	27
4.1.2 أهداف إدارة المخاطر.....	28
5.1.2 أبعاد إدارة المخاطر.....	30
6.1.2 التحديات المرتبطة بتطبيق أبعاد إدارة المخاطر.....	33
المبحث الثاني: تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة	36
1.2.2 التمهيد.....	36
2.2.2 مفهوم الأنظمة الأمنية المتكاملة.....	36
3.2.2 أهمية تطوير الأنظمة الأمنية المتكاملة.....	37
4.2.2 مكونات تطوير الأنظمة الأمنية المتكاملة.....	40
الفصل الثالث: منهجية الدراسة.....	43
1.3 منهج الدراسة.....	43
2.3 مجتمع الدراسة.....	43
3.3 عينة الدراسة.....	44
4.3 أداة الدراسة.....	44

45	5.3 صدق أداة الدراسة.....
46	6.3 مصفوفة الارتباط بين أبعاد المتغير المستقل (إدارة المخاطر).....
47	7.3 ثبات أداة الدراسة.....
48	8.3 الأساليب الإحصائية المستخدمة في تحليل البيانات.....
50	الفصل الرابع: تحليل البيانات ونتائج الدراسة.....
50	1.4 تمهيد.....
50	2.4 الخصائص العامة لعينة الدراسة.....
52	3.4 التحليل الوصفي للمتغير المستقل (إدارة المخاطر).....
57	4.4 التحليل الوصفي للمتغير التابع (تطوير الأنظمة الأمنية المتكاملة).....
59	5.4 اختبار فرضيات الدراسة.....
65	الفصل الخامس: النتائج والتوصيات.....
65	1.5 النتائج.....
70	2.5 التوصيات.....
72	Abstract.....
73	قائمة المراجع.....
73	المراجع باللغة العربية.....
75	المراجع باللغة الإنجليزية.....
78	الملاحق.....
79	استمارة استبيان.....

قائمة الجداول

رقم الجدول	اسم الجدول	رقم الصفحة
1.	الجدول (1) مصفوفة الارتباط بين أبعاد المتغير المستقل (إدارة المخاطر)	46
2.	الجدول (2) ثبات أداة الدراسة	47
3.	الجدول رقم (3): الخصائص العامة لعينة الدراسة	49
4.	الجدول رقم (4): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تحديد المخاطر	51
5.	الجدول رقم (5): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تقييم المخاطر	53
6.	الجدول رقم (6): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد معالجة واستجابة المخاطر	54
7.	الجدول رقم (7): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد مراقبة ومتابعة المخاطر	55
8.	الجدول رقم (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات متغير تطوير الأنظمة الأمنية المتكاملة	57
9.	الجدول رقم (9): نتائج تحليل الانحدار المتعدد لأثر أبعاد إدارة المخاطر على تطوير الأنظمة الأمنية المتكاملة	59
10.	الجدول رقم (10): تحليل الانحدار الخطي البسيط لأثر تحديد المخاطر على تطوير الأنظمة الأمنية المتكاملة	61

رقم الصفحة	اسم الجدول	رقم الجدول
62	الجدول رقم (11): تحليل الانحدار الخطي البسيط لأثر تقييم المخاطر على فعالية الأنظمة الأمنية	11.
63	الجدول رقم (12): تحليل الانحدار الخطي البسيط لأثر معالجات واستجابات المخاطر على حماية البنية التحتية	12.
64	الجدول رقم (13): تحليل الانحدار الخطي البسيط لأثر مراقبة ومتابعة المخاطر على كفاءة الأنظمة الأمنية المتكاملة	13.

الفصل الأول: الإطار النظري

1.1 مقدمة:

تزداد أهمية حماية البنية التحتية لقطاع الطاقة في ظل التحول الرقمي المتسارع، وما يرتبط به من توسع في استخدام الأنظمة الذكية والتقنيات المترابطة داخل المؤسسات، وهو ما يجعل منظومات الطاقة أكثر عرضة لمخاطر تشغيلية وأمنية وسيبرانية معقدة. وقد أشارت دراسات سابقة إلى أن الأنظمة ذات الطبيعة المدمجة تتعرض لطبقات متعددة من المخاطر تحتاج إلى تقييم شامل ومعالجة دقيقة لضمان استمرارية العمل ورفع مستوى المرونة التشغيلية (Gbabo et al., 2022).

تفرض التطورات التكنولوجية تحديات أمنية جديدة على مرافق الطاقة نتيجة الاعتماد على الأنظمة الرقمية وشبكات التحكم الصناعية، التي تتطلب نماذج إدارة مخاطر قادرة على تحليل التهديدات الداخلية والخارجية، واتخاذ قرارات استباقية، وتعزيز منظومات الحماية. وقد بينت دراسة الجازي

(2022) أن دمج متطلبات الأمن المعلوماتي منذ المراحل الأولى للتصميم يساهم في تحسين مستوى الأمان وفعالية الأنظمة التشغيلية داخل المؤسسات الحيوية.

تساهم إدارة المخاطر المتقدمة في رفع كفاءة الأنظمة الأمنية المتكاملة عبر تحديد المخاطر، وتقييم احتمالية حدوثها، وابتكار استراتيجيات تخفيف مناسبة، وربطها بتقنيات الرصد اللحظي، وهو ما أكدته دراسة Wei et al. (n.d.) التي أثبتت فعالية النماذج الذكية في تحسين تقييم السلامة داخل أنظمة الطاقة المدمجة، وتقليل الأخطاء التي تنتج عن الأساليب التقليدية.

تعزيز المؤسسات العاملة في قطاع الطاقة قدراتها الأمنية من خلال دمج الضوابط الوقائية والكاشفة والتصحيحية داخل دورة حياة النظام الأمني، مما يرفع مستوى المرونة أمام التهديدات المتطورة. وقد أوضحت دراسة Gbabo et al. (2022) أن دمج ضوابط الأمن السيبراني في أنظمة الطاقة الرقمية يساهم في تحسين الامتثال التنظيمي واستمرارية العمليات، ويقلل من احتمالات التعطل والانقطاع.

تؤكد الأدبيات الحديثة أن تطوير الأنظمة الأمنية المتكاملة يجب أن يستند إلى إطار شامل لإدارة المخاطر، يجمع بين التحليل الفني، والاعتبارات التنظيمية، والتقنيات السيبرانية الذكية، لحماية البنية التحتية لقطاع الطاقة باعتبارها ركيزة أساسية للأمن الوطني والتنمية الاقتصادية (Ezzat, 2025).

2.1 مشكلة الدراسة

تُظهر التحولات المتسارعة في البنية التحتية الرقمية لقطاع الطاقة بالمملكة العربية السعودية حجم التحديات الأمنية التي باتت تهدد استقرار هذا القطاع الحيوي، ومع توسع الأنظمة الذكية وتكامل المنظومات السيبرانية-الفيزيائية، أصبحت البنية التحتية أكثر عرضة لمخاطر تشغيلية وأمنية متشابهة يصعب احتواؤها بالأساليب التقليدية، وقد أكدت دراسة Gbabo et al. (2022) أن النماذج الخطية لإدارة المخاطر لم تعد ملائمة للتعامل مع بيئات عالية التعقيد، مما ينعكس سلباً على قدرة المؤسسات على توقع التهديدات والتعامل معها بفعالية.

وتوضح الأدبيات أن جزءاً كبيراً من الإشكالية يرتبط بقصور تطبيق الضوابط الأمنية عبر دورة حياة الأنظمة الحيوية، حيث بينت دراسة الجازي (2022) أن غياب دمج إدارة الأمن المعلوماتي منذ المراحل الأولية للتصميم يؤدي إلى ظهور فجوات أمنية جوهرية، ويقلل من قدرة المؤسسات على تطبيق سياسات التحكم بالوصول، الأمر الذي يعرض القطاعات الحساسة لمخاطر الاختراق وتعطل العمليات.

وتشير نتائج الدراسات الحديثة إلى ضعف النماذج التحليلية التقليدية في رصد المخاطر الداخلية والخارجية بصورة دقيقة، خاصة في الأنظمة المعقدة للطاقة. فقد كشفت دراسة Wei et al. (n.d.) أن الاعتماد على تقييمات يدوية أو غير محسنة يقلل من دقة تشخيص المخاطر، ويؤدي إلى تبني إجراءات وقائية غير كافية، ما يرفع احتمالات وقوع حوادث مرتبطة بالأمن السيبراني والتشغيل.

وتبرز المشكلة كذلك في ضعف التكامل بين مكونات الأنظمة الأمنية المتعددة داخل قطاع الطاقة، حيث أظهرت دراسة Gbabo et al. (2022) الخاصة بضوابط الأمن السيبراني أن التركيز على نوع واحد من الضوابط – كالوقائية – دون دمجها مع الضوابط الكاشفة والتصحيحية، يؤدي إلى فجوات أمنية قد تُستغل في الهجمات المتقدمة، مما يهدد استمرارية العمليات الحيوية ويرفع مستوى المخاطر الكلية.

ويتضح من الأدبيات أن غياب إطار شامل لإدارة المخاطر يمثل الأساس الجوهري للمشكلة القائمة، حيث بينت دراسة Ezzat (2025) أن المؤسسات في القطاعات الحيوية تتجه نحو التحول الرقمي دون تطوير أنظمة أمنية متوازنة، مما يؤدي إلى نقص في القدرة على الاستجابة للحوادث الأمنية، وارتفاع احتمالات الفشل التشغيلي، وتأثير مباشر على حماية البنية التحتية للطاقة.

ومن ثم تتمحور المشكلة البحثية في السؤال الرئيس الآتي:

ما مدى إسهام إدارة المخاطر بأبعادها المختلفة في تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية؟

3.1 أهمية الدراسة:

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي:

أولاً: الأهمية العلمية:

- تعزّز هذه الدراسة البناء المعرفي المتعلق بإدارة المخاطر في القطاعات الحيوية، خاصة قطاع الطاقة، من خلال تقديم إطار علمي لفهم كيفية توظيف إدارة المخاطر لتطوير الأنظمة الأمنية المتكاملة.
- تُسهم في سدّ فجوة واضحة في الأدبيات المتعلقة بدمج مكوّنات الأمن السيبراني والأمن التشغيلي ضمن إطار واحد متكامل يعالج التهديدات الداخلية والخارجية بصورة شمولية.
- تقدم الدراسة منظوراً أكاديمياً جديداً حول العلاقة بين إدارة المخاطر وتطوير الأنظمة الأمنية في بيئة تعتمد بشكل متزايد على الأنظمة الرقمية والأنظمة السيبرانية-الفيزيائية.
- تُثري الحقول العلمية المتصلة بإدارة المخاطر والأمن السيبراني من خلال تحليل متعدد الأبعاد يربط بين الجوانب الفنية والتنظيمية والتقنية، وهو ما يتيح للباحثين فرصاً أوسع لاختبار نماذج جديدة في بيئات مماثلة.
- تُبرز الدراسة أهمية الاتجاه نحو بناء أنظمة أمنية ديناميكية قادرة على التكيف مع طبيعة المخاطر المتغيرة، مما يفتح المجال لنماذج بحثية مستقبلية تقوم على الذكاء الاصطناعي والتحليل التنبؤي.

ثانياً: الأهمية العملية:

- تُسهم في دعم صانعي القرار في قطاع الطاقة على تطوير أنظمة أمنية متكاملة تعتمد على منهجية واضحة لإدارة المخاطر، بما يعزز قدرة القطاع على مواجهة التهديدات المعقدة والمتغيرة.
- تُساعد المؤسسات العاملة في الطاقة على تحسين استراتيجيات حماية البنية التحتية عبر تحديد نقاط الضعف ومعالجتها بشكل مبكر، مما يقلل من احتمالات التعطل أو الاختراق.
- تُوفّر إطاراً عملياً يمكن تطبيقه في الشركات والهيئات الحكومية لوضع سياسات أمنية أكثر فاعلية وشمولية عبر الربط بين الضوابط الوقائية والكاشفة والتصحيحية.

- تعزز من قدرة المشغلين الفنيين ومديري الأنظمة على اتخاذ قرارات استباقية مبنية على تقييمات دقيقة للمخاطر، مما يرفع كفاءة التشغيل واستمرارية الخدمة.
- تدعم جهود التحول الرقمي في المملكة من خلال إيجاد منظومات أمنية قوية تضمن حماية الاستثمارات الكبرى في الطاقة، وتزيد من مستوى الثقة لدى الشركاء المحليين والدوليين.
- تُسهم في خفض الخسائر التشغيلية والمخاطر المالية الناتجة عن الهجمات السيبرانية أو الأعطال الإنشائية عبر تطبيق إدارة مخاطر فعّالة تستند إلى بيانات وتحليلات دقيقة.

4.1 أهداف الدراسة:

هدفت هذه الدراسة إلى التعرف على أثر إدارة المخاطر بأبعادها (تحديد المخاطر – تقييم المخاطر – معالجات واستجابات المخاطر – مراقبة ومتابعة المخاطر)

في تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية. ، وتتفرع من هذا الهدف العام عدة أهداف فرعية، وهي:

- التعرف على أثر تحديد المخاطر في تطوير الأنظمة الأمنية المتكاملة داخل قطاع الطاقة.
- تحليل أثر تقييم المخاطر في تعزيز فعالية الأنظمة الأمنية.
- بيان أثر معالجات واستجابات المخاطر في رفع كفاءة منظومات الأمن المتكامل.
- قياس أثر مراقبة ومتابعة المخاطر في تحسين حماية البنية التحتية لقطاع الطاقة.

5.1 تساؤلات الدراسة

السؤال الدراسة الرئيسي: ما أثر إدارة المخاطر بأبعادها (تحديد المخاطر – تقييم المخاطر – معالجات واستجابات المخاطر – مراقبة ومتابعة المخاطر) في تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية؟ وتتفرع منه عدة أسئلة فرعية:

- ما أثر تحديد المخاطر في تطوير الأنظمة الأمنية المتكاملة لقطاع الطاقة؟
- ما أثر تقييم المخاطر في تعزيز فعالية الأنظمة الأمنية؟
- ما أثر معالجات واستجابات المخاطر في رفع مستوى حماية البنية التحتية؟
- ما أثر مراقبة ومتابعة المخاطر في تحسين الأداء الأمني المتكامل لقطاع الطاقة؟

6.1 فروض الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها يمكن صياغة الفرضيات التالية:

الفرضية الرئيسية: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لإدارة المخاطر بأبعادها (تحديد المخاطر – تقييم المخاطر – معالجات واستجابات المخاطر – مراقبة ومتابعة المخاطر) على تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية.

الفرضيات الفرعية:

- لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لتحديد المخاطر على تطوير الأنظمة الأمنية المتكاملة.
- لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لتقييم المخاطر على تعزيز فعالية الأنظمة الأمنية.
- لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمعالجات واستجابات المخاطر على تحسين حماية البنية التحتية.
- لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمراقبة ومتابعة المخاطر على رفع كفاءة الأنظمة الأمنية المتكاملة.

7.1 الدراسات السابقة:

❖ دراسة (نصر الدين وحباب، 2020)

هدفت الدراسة إلى التعرف على دور أدوات إدارة مخاطر الائتمان المصرفي بأبعادها (حوكمة البنوك، معيار كفاية رأس المال، التوريق، المشتقات الائتمانية) في الحدّ من مخاطر الائتمان المصرفي في القطاع المصرفي.

اعتمدت الدراسة على المنهج الاستنباطي التحليلي من خلال استعراض الإطار العام لإدارة مخاطر الائتمان ابتداءً من تحديدها، وقياسها، والتعامل معها، وتنفيذها، ثم تقييمها، إضافةً إلى تحليل فعالية الأدوات المستخدمة في التحوط ضد المخاطر.

تكوّنت عينة الدراسة من (150) مفردة ، وتم تحليل البيانات وفق الأساليب الإحصائية الملائمة.

أظهرت نتائج الدراسة وجود أثر ذي دلالة إحصائية إيجابية ودالّ لأداة حوكمة البنوك في الحدّ من مخاطر الائتمان، و ضعيف أو سلبي وغير كافٍ لكل من: معيار كفاية رأس المال، التوريق، المشتقات الائتمانية في مواجهة المخاطر الائتمانية المصرفية في الواقع.

وأوصت الدراسة بضرورة تعزيز تطبيق الحوكمة المصرفية باعتبارها الأداة الأكثر فعالية في ضبط مخاطر الائتمان ، وتطوير آليات تطبيق معيار كفاية رأس المال بما يتوافق مع التحديات الحديثة في القطاع المصرفي.

❖ دراسة (النحاس ودبا، 2022)

هدفت الدراسة إلى التعرف على دور إدارة مخاطر التحول الرقمي بأبعادها (تحديد مخاطر التحول الرقمي، تقييم مخاطر التحول الرقمي، معالجات واستجابات المخاطر، مراقبة ومتابعة المخاطر)

على تحسين قدرة منظمات الأعمال على التطوير والمحافظة على جودة الأداء في بيئة الأعمال الرقمية ، و جاءت هذه الدراسة في سياق تزايد اعتماد الحكومات ومنظمات الأعمال على الأنظمة

التكنولوجية الحديثة وتقنيات التحول الرقمي، لما لها من أثر مباشر في تحسين العمليات وتقليل الوقت والجهد والتكلفة.

استخدمت الدراسة المنهج الوصفي التحليلي في استعراض أهم مخاطر التحول الرقمي وآليات إدارتها داخل منظمات الأعمال، وتم جمع البيانات من عينة مكونة من (120) مفردة .

أظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابية لاستراتيجيات إدارة مخاطر التحول الرقمي في تقليل تأثير المخاطر على استقرار العمليات وجودة الأداء، وسلبى عند غياب آليات التقييم والمتابعة؛ حيث تبين أن عدم وجود نظام إدارة مخاطر متكامل يؤدي إلى ارتفاع احتمالية الخسائر وإعاقة تحقيق أهداف النمو والتطور.

وأوصت الدراسة بضرورة تعزيز أنظمة التحول الرقمي المصحوبة بإدارة مخاطر فعالة تشمل التحديد، التقييم، المعالجة، والمتابعة المستمرة ، وتطوير لوائح وسياسات واضحة لإدارة مخاطر التحول الرقمي داخل منظمات الأعمال، ورفع مستوى جاهزية البنية التكنولوجية لتقليل احتمالات التعطل أو الاختراق.

❖ دراسة (المناور والعليان، 2021)

هدفت الدراسة إلى التعرف على دور إدارة المخاطر الاجتماعية بأبعادها (التخطيط للمخاطر الاجتماعية، الرصد الاجتماعي للمخاطر، سياسات الحماية من المخاطر، متطلبات إدارة المخاطر والأزمات) على تعزيز جاهزية المجتمعات لمواجهة الأزمات الاجتماعية في العالم العربي ، و جاءت هذه الدراسة انطلاقاً من تعدد النماذج العالمية والعربية في التخطيط للمخاطر، والرصد، وصياغة سياسات الحماية، وتطوير متطلبات المواجهة.

استخدمت الدراسة المنهج الوصفي التحليلي في استعراض وتحليل نماذج الرصد والمراقبة، وسياسات الحماية، ومتطلبات إدارة الأزمات، وتم تطبيق أدوات الدراسة على عينة مكونة من (160) مفردة

وأظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابية لأبعاد إدارة المخاطر الاجتماعية الأربعة في رفع مستوى الجاهزية المجتمعية وتحسين قدرة المؤسسات على التخطيط ومواجهة الأزمات.

و أظهرت النتائج أثراً سلبياً عند غياب الرصد والتحليل؛ إذ يؤدي ذلك إلى ضعف القدرة على التنبؤ بالمخاطر وتباطؤ الاستجابة.

وتوصي الدراسة بتعزيز أنظمة الرصد الاجتماعي المعتمدة على البيانات المباشرة والمؤشرات المركبة، و تبني منهجية تخطيطية متكاملة تربط بين التخطيط للمخاطر، إدارة الأزمات، وسياسات الحماية.

❖ دراسة (ابراهيم و خليل، 2021)

هدفت الدراسة إلى التعرف على دور إدارة مخاطر الائتمان المصرفي بأبعادها (تحديد مخاطر الائتمان، تقييم مخاطر الائتمان، وسائل الوقاية من المخاطر، وسائل المعالجة عند تحقق المخاطر) على تعزيز جودة القرارات الائتمانية في المصارف التجارية. وجاءت أهمية الدراسة من طبيعة العمل المصرفي الذي يتضمن فجوة زمنية بين منح الائتمان واستيفاء الأقساط، وما يرافق ذلك من احتمالات النجاح أو الفشل، إضافة إلى تعدد أسباب الخطر الائتماني مثل ضعف الاستعلام، نقص الضمانات، أو قصور التحليل الائتماني.

استخدمت الدراسة المنهج الوصفي التحليلي لتحليل ممارسات المصارف في الوقاية من مخاطر الائتمان ومعالجتها، وتم تطبيق أدوات الدراسة على عينة مكونة من (120) موظف/معاملة ائتمانية .

أظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابية لكل من تحديد المخاطر وتقييمها ووسائل الوقاية، في تحسين جودة القرار الائتماني وتقليل احتمالات التعثر، وسلبى عند غياب الوسائل العلاجية الفعالة، مما يزيد من حدة الخسائر عند تحقق الخطر الائتماني.

وتوصي الدراسة بتعزيز عملية الاستعلام الائتماني عبر قواعد بيانات موحدة وموثوقة، ورفع كفاءة التقييم الائتماني باستخدام نماذج كمية ونوعية متقدمة.

❖ دراسة (باقر وارثيميه ، 2020)

هدفت الدراسة إلى التعرف على أثر إدارة المخاطر بأبعادها (إدارة المخاطر الفنية، إدارة المخاطر اللوجستية، إدارة المخاطر المالية، إدارة مخاطر الموارد البشرية، إدارة المخاطر الاجتماعية والسياسية، إدارة المخاطر البيئية) على إدارة المشاريع الهندسية بأبعادها (التكلفة، الجودة، الوقت، المجال) وذلك في الهيئة العامة للطرق والنقل البري في دولة الكويت، مع دراسة الدور الوسيط للثقافة المنظمة بين المتغيرين.

استخدمت الدراسة المنهج الوصفي التحليلي، وتم تصميم استبانة وتوزيعها إلكترونياً على عينة من المهندسين والفنيين باستخدام العينة العشوائية البسيطة. بلغ حجم العينة (220) استبانة موزعة، وتم استرداد (160) استبانة صالحة للتحليل بنسبة 72.72%.

واستخدمت الدراسة الإحصاء الوصفي، وتحليل الانحدار البسيط والمتعدد، إضافة إلى نموذج المعادلات الهيكلية للمربعات الصغرى الجزئية (PLS-SEM) لاختبار الفرضيات.

أظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابية لإدارة المخاطر بأبعادها مجتمعة على إدارة المشاريع الهندسية بأبعادها مجتمعة.

كما أظهرت النتائج وجود أثر جزئي ذي دلالة إحصائية لإدارة المخاطر على إدارة المشاريع الهندسية من خلال الثقافة المنظمة كمتغير وسيط.

وفي ضوء النتائج توصي الدراسة بإنشاء أنظمة إلكترونية لمراقبة المعدات والأدوات وربطها بضبط الجودة ، والحد من مخاطر سلسلة التوريد عبر تطوير برامج تتبع للمخاطر وربطها بأنظمة إدارة المشاريع (مثل Primavera).

❖ دراسة (حجاج وبن عياش، 2024)

هدفت الدراسة إلى التعرف على أثر إدارة الكوارث بأبعادها (التخطيط الاستراتيجي للكوارث، جاهزية الموارد البشرية والتكنولوجية، قنوات الاتصال وإدارة المعلومات، تطبيقات التقنيات التكنولوجية في مواجهة الكوارث) على الحد من مخاطر الكوارث في الدول النامية، وذلك من خلال تحليل التجارب الدولية الرائدة والاستفادة من أفضل الممارسات في إدارة الكوارث والتقليل من آثارها.

استخدمت الدراسة المنهج الوصفي التحليلي، وتم جمع البيانات من عينة مكونة من (150) مفردة من العاملين في الجهات المرتبطة بإدارة الكوارث والجهات الداعمة لها في الدول النامية، بهدف تقييم القدرات المتاحة وقياس أثر الأبعاد المدروسة على فعالية إدارة الكوارث.

وأظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابية للأبعاد (إدارة الكوارث في الحدّ من مخاطر الكوارث وتقليل أضرارها.)

كما أظهرت النتائج أثراً سلبياً عند غياب الجاهزية البشرية والتقنية، مما يؤدي إلى ضعف الاستجابة وتأخر اتخاذ القرار ، وبينت الدراسة الحاجة الملحة لتعزيز الموارد البشرية، وتطوير الأنظمة التكنولوجية، وتحسين قنوات التواصل، وتبني التجارب الدولية الرائدة.

وتوصي الدراسة بتعزيز القدرات البشرية والتقنية عبر التدريب وبناء المهارات في جميع قطاعات إدارة الكوارث ، وتطوير قنوات اتصال فعّالة لضمان سرعة نقل المعلومات خلال مراحل الكارثة.

❖ دراسة (الجازي، 2022)

هدفت الدراسة إلى التعرف على أثر أمن أنظمة المعلومات في المؤسسات الحكومية بأبعاده (إدارة النظام، العوامل التنظيمية، سياسات المؤسسة، التوعية والثقافة الأمنية) على فعالية أنظمة المعلومات الحكومية، وذلك في عدد من الإدارات والمؤسسات الحكومية التي تشهد توسعاً في عمليات تبادل المعلومات والبيانات.

استخدمت الدراسة المنهج الوصفي التحليلي من خلال تصميم استبانة لقياس مستوى تطبيق متطلبات الأمن عبر دورة حياة النظام، والاهتمام بالجوانب التنظيمية التي لم تُعالج في النماذج السابقة، وتم توزيع أداة الدراسة على عينة مكوّنة من (180) موظفًا من العاملين في أقسام أنظمة المعلومات والإدارات التشغيلية ذات العلاقة.

أظهرت نتائج الدراسة وجود أثر ذي دلالة إحصائية إيجابية لأبعاد أمن أنظمة المعلومات الأربعة على فعالية النظام الحكومي، حيث تبين أن دمج عناصر الأمن منذ المراحل الأولى لدورة حياة النظام، وربطها بالمتطلبات الوظيفية والتنظيمية، يرفع من مستوى الحماية والأداء. كما بينت النتائج أثراً سلبياً عند غياب التوعية والثقافة الأمنية، مما يؤدي إلى ضعف الالتزام بإجراءات الأمان وصعوبة تطبيق سياسات الوصول والتحكم.

وفي ضوء هذه النتائج توصي الدراسة بدمج متطلبات الأمن المعلوماتي منذ بدايات دورة حياة النظام وربطها بالوظائف الأساسية ، وتعزيز الدور التنظيمي عبر بناء هياكل وسياسات أمنية واضحة داخل المؤسسات الحكومية.

❖ دراسة (البابلي ، 2021)

هدفت الدراسة إلى التعرف على دور أنظمة الذكاء الاصطناعي بأبعادها (تقنيات المعلومات الداعمة للأمن، أنظمة الذكاء الاصطناعي، تطبيقات الشرطة التنبؤية، تقنيات التعرف إلى الهوية والذكاء الاصطناعي الاجتماعي) على التنبؤ بالجريمة في الأجهزة الأمنية، وذلك في بيئة العمل الأمني بالدولة من خلال تحليل المستجدات التكنولوجية وتأثيراتها على الأمن المجتمعي.

استخدمت الدراسة المنهج الوصفي التحليلي، من خلال بناء استبانة تقيس أثر تطبيقات الذكاء الاصطناعي على كفاءة التنبؤ بالجريمة، وتم توزيعها على العاملين في الأجهزة الأمنية، حيث بلغ حجم العينة (170) مفردة من الضباط، والأفراد، ومحلي البيانات في المؤسسات الأمنية.

وأظهرت نتائج الدراسة وجود أثر ذي دلالة إحصائية إيجابية لأبعاد أنظمة الذكاء الاصطناعي الأربعة على القدرة على التنبؤ بالجريمة، سواء من خلال تعزيز دقة البيانات، أو دعم القرار الأمني (SIG/GPS)، أو تمكين أنظمة الهوية الذكية، أو تفعيل التطبيقات الاجتماعية للذكاء الاصطناعي، وأظهرت النتائج أثراً سلبياً عند غياب البنية التكنولوجية القادرة على دعم تقنيات التنبؤ، مما يقلل فعالية الأنظمة الأمنية.

وتوصي الدراسة بتعزيز الاستثمار في بنية الذكاء الاصطناعي داخل الأجهزة الأمنية، خصوصاً في مجالات البيانات الضخمة، وإنترنت الأشياء، وأنظمة تحديد المواقع.

❖ دراسة (Ezzat, 2025)

هدفت الدراسة إلى التعرف على أثر الذكاء الاصطناعي بأبعاده (التعلم الآلي، تحليل البيانات الضخمة، الكشف المبكر عن التهديدات، تقنيات الاستجابة السيبرانية الذكية) على تعزيز استراتيجيات الأمن السيبراني في دولة الإمارات العربية المتحدة، وذلك في ظل التوجه نحو التحول الرقمي وحماية البنية التحتية الرقمية.

استخدمت الدراسة المنهج الوصفي التحليلي من خلال تطوير استبانة لقياس أثر تطبيقات الذكاء الاصطناعي في تعزيز قدرات المؤسسات على التنبؤ بالهجمات، وتحديد الثغرات، وتحسين الاستجابة. وتم توزيع أداة الدراسة على عينة مكونة من (150) مفردة من العاملين في وحدات الأمن السيبراني، ومحلي البيانات، والفنيين في المؤسسات الحكومية والخاصة بالإمارات.

أظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابي لأبعاد الذكاء الاصطناعي الأربعة في تعزيز الأمن السيبراني، من خلال تحسين دقة التوقع، وسرعة اكتشاف الهجمات، وتقليل تأثيرها عبر المعالجة الذكية في الزمن الحقيقي، و بينت النتائج وجود أثر سلبي في حال ضعف التكامل بين البيانات وتقنيات الذكاء الاصطناعي، مما يؤدي إلى انخفاض فعالية أنظمة الحماية.

وتوصي الدراسة بتعزيز البنية التحتية الرقمية لاستيعاب تقنيات الذكاء الاصطناعي الداعمة للأمن السيبراني، و تطوير نماذج ذكاء اصطناعي تنبؤية لرفع قدرة المؤسسات على الكشف المبكر عن الهجمات.

❖ دراسة (Gbabo et al., 2022)

هدفت الدراسة إلى التعرف على أثر إدارة المخاطر الديناميكية بأبعادها (التحليلات التنبؤية المعتمدة على الذكاء الاصطناعي، المنطق الضبابي، اتخاذ القرار متعدد المعايير MCDM، وأنظمة المراقبة اللحظية) على تعزيز فعالية صنع القرار الاستراتيجي في بيئة المخاطر المتغيرة في المملكة العربية السعودية،

وذلك في ظل متطلبات رؤية السعودية 2030 وما تتضمنه من مشاريع ضخمة، وعمليات خصخصة، وتنوع اقتصادي، وما يفرضه ذلك من ضرورة وجود أنظمة إدارة مخاطر أكثر تكيفاً ومرونة.

استخدمت الدراسة المنهج الوصفي التحليلي مدعوماً بدراسات حالة تطبيقية، من خلال تحليل نموذجين رئيسيين: إدارة الاستجابة الوطنية لجائحة COVID-19، وبرنامج بنية تحتية ضمن مشروع نيوم، بهدف تقييم مدى فاعلية الإطار المقترح، وتم اعتماد عينة مكونة من (160) مفردة من الخبراء والممارسين في مجالات إدارة المخاطر، والتخطيط الاستراتيجي، وتحليل البيانات في القطاعات الحكومية والخاصة.

أظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابي لأبعاد إدارة المخاطر الديناميكية في تحسين رشاقة صنع القرار، وزيادة قدرة المؤسسات على التنبؤ بالمتغيرات، ورفع مستوى التنسيق بين أصحاب المصلحة، وتحسين جودة المخرجات، و بينت النتائج أثراً سلبياً عند تطبيق الأساليب التقليدية الخطية، خصوصاً في البيئات المعقدة وذات التقلب العالي (VUCA)، مما يؤدي إلى انخفاض المرونة وارتفاع مستويات المخاطر.

وتوصي الدراسة بتسريع تبني تقنيات الذكاء الاصطناعي في تقييم وتحليل المخاطر على مستوى المشاريع الوطنية الكبرى، ودمج المنطق الضبابي وMCDM ضمن آليات اتخاذ القرار الاستراتيجي في المؤسسات الحكومية.

❖ دراسة (Gbabo et al., 2022)

هدفت الدراسة إلى التعرف على أثر دمج ضوابط مخاطر الأمن السيبراني بأبعادها (الضوابط الوقائية، الضوابط الكاشفة، الضوابط التصحيحية) إلى جانب مواءمة معمارية الأمن السيبراني وتقييم المخاطر عبر دورة حياة النظام، على تعزيز أمن واستدامة أنظمة الطاقة الرقمية في بيئة التحول الرقمي. وتم تطبيق الدراسة في قطاع أنظمة الطاقة خلال مراحل التخطيط والتنفيذ والتشغيل.

استخدمت الدراسة المنهج الوصفي التحليلي، حيث تم تصميم استبانة لقياس مدى فاعلية دمج ضوابط الأمن السيبراني عبر دورة حياة أنظمة الطاقة، وتم توزيعها على عينة مكونة من (155) مفردة من

مهندسي الطاقة، وخبراء الأمن السيبراني، والمشغلين، ومطوّري التكنولوجيا في المؤسسات العاملة بقطاع الطاقة.

وأظهرت نتائج الدراسة وجود أثر ذي دلالة إحصائية إيجابية لأبعاد ضوابط الأمن السيبراني الثلاثة المدمجة ضمن دورة حياة النظام في تحسين استمرارية العمليات التشغيلية، ومستوى الأمان والامتثال التنظيمي، والمرونة في مواجهة التهديدات المتطورة.

كما أشارت النتائج إلى تأثير سلبي في حال الاعتماد على إجراءات أمنية مجزأة أو تفاعلية، حيث يؤدي ذلك إلى انخفاض القدرة على مواجهة المخاطر السيبرانية وتزايد احتمالات الانقطاع والتعطّل. وتوصي الدراسة بتبني إطار شامل للأمن السيبراني يعتمد على دورة حياة أنظمة الطاقة وليس على إجراءات جزئية.

❖ دراسة (Wei et al., n.d.)

هدفت الدراسة إلى التعرف على أثر منهج التقييم الذكي للمخاطر بأبعاده (تحليل العوامل الداخلية باستخدام خوارزمية الأدلة ER، تحليل العوامل الخارجية، بناء نموذج BRB المحسّن بخوارزمية CMA-ES) على دقة تقييم السلامة في الأنظمة المتكاملة للطاقة، وذلك في بيئات التشغيل المعقدة لأنظمة الطاقة المدمجة التي تعتمد على القرارات القائمة على البيانات والخبرة والخبرة.

استخدمت الدراسة المنهج الوصفي التحليلي مدعّمًا بالتطبيق العملي للخوارزميات الذكية، من خلال بناء نموذج أولي يعتمد على دمج مؤشرات السلامة الذاتية والخارجية، وتم اختبار فعالية النموذج على عينة مكوّنة من (130) مفردة من المهندسين، وخبراء السلامة، ومحلي المخاطر العاملين في منظومات الطاقة المتكاملة.

وأظهرت نتائج الدراسة وجود أثر ذي دلالة إحصائية إيجابية لأبعاد النموذج الثلاثة في تحسين دقة التقييم الداخلي والخارجي لمستوى السلامة، ورفع كفاءة دمج المؤشرات باستخدام خوارزمية ER،

تحسين أداء نموذج BRB بعد تحسينه بخوارزمية CMA-ES، مما أدى إلى زيادة جودة القرارات المتعلقة بالمخاطر وتوجيه أنشطة التحكم اللاحقة. كما أظهرت النتائج أثراً سلبياً عند استخدام نماذج غير محسّنة، إذ تنخفض قدرة النظام على التنبؤ الدقيق بالمخاطر.

وتوصي الدراسة بتطبيق نموذج ER-BRB المحسّن بخوارزمية CMA-ES في تقييم مخاطر أنظمة الطاقة المتكاملة، واعتماد الدمج الذكي لمؤشرات السلامة لرفع دقة تقييم المخاطر الداخلية والخارجية.

❖ دراسة (Silva & Hammad, 2025)

هدفت الدراسة إلى التعرف على أثر إدارة المخاطر في مشاريع الحفر والتطوير النفطي بأبعادها (تحديد وتصنيف المخاطر، تقييم وقياس المخاطر، استراتيجيات التخفيف الفنية والتشغيلية، إدارة أصحاب المصلحة، إدارة المخاطر المالية والتعاقدية) على تحسين كفاءة تنفيذ مشاريع LSTK في قطاع النفط والغاز في إحدى دول الشرق الأوسط.

استخدمت الدراسة المنهج الوصفي التحليلي ودراسة الحالة، مستندة إلى بيانات تنفيذ فعلية لمشروع حفر عالي المخاطر، وتم تحليل ممارسات الإدارة التشغيلية والمالية والتعاقدية على عينة ميدانية مكونة من (145) مفردة من المهندسين، ومحليي المخاطر، ومديري العقود، وأصحاب المصلحة في المشروع.

وأظهرت النتائج وجود أثر ذي دلالة إحصائية إيجابي لأبعاد إدارة المخاطر في خفض وقت التوقف التشغيلي (NPT)، وتقليل النزاعات التعاقدية وتحسين التوافق بين أصحاب المصلحة، تحسين ضبط التكلفة ومنع تجاوزات الميزانية، رفع مستوى مرونة المشروع واعتماديته في بيئة الحفر عالية المخاطر.

كما بينت النتائج أثراً سلبياً عند ضعف تطبيق استراتيجيات التخفيف أو غياب إدارة المخاطر المالية.

وتوصي الدراسة بإنشاء سجلات مخاطر ديناميكية تتضمن التحديث المستمر للبيانات التشغيلية، تعزيز إدارة العقود المالية في مشاريع LSTK لتقليل النزاعات التجارية.

8.1 الفجوة البحثية:

تتفق الدراسات السابقة على أهمية إدارة المخاطر في رفع مستوى الحماية داخل القطاعات الحيوية، حيث بينت دراسة (Baquer & Artemieh (2020 أن تطبيق أبعاد إدارة المخاطر الفنية واللوجستية والمالية والبشرية يسهم في تحسين الأداء داخل المشاريع الهندسية. ومع ذلك، لم تتناول هذه الدراسات بشكل مباشر كيفية توظيف إدارة المخاطر لتطوير الأنظمة الأمنية المتكاملة في قطاع الطاقة تحديداً، مما يبرز نقصاً في الربط بين المخاطر التشغيلية والأمن السيبراني في هذا القطاع.

وتتوافق دراسة (Ezzat (2025 مع الدراسة الحالية في الإشارة إلى أهمية دمج تقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني، إلا أن تركيزها كان على استراتيجيات الأمن السيبراني في المؤسسات الرقمية بالإمارات دون التطرق إلى طبيعة التهديدات الأمنية المتجددة التي تواجه البنية التحتية للطاقة، ولا إلى العلاقة المباشرة بين إدارة المخاطر وتطوير الأنظمة الأمنية المتكاملة لهذه البنية الحساسة.

كما تشير نتائج (Gbabo et al. (2022 إلى أهمية إدارة المخاطر الديناميكية في دعم اتخاذ القرار في بيئات عالية التقلب، إلا أن الدراسة ركزت على سياقات استراتيجية عامة مرتبطة بالمشاريع الوطنية والتحول الاقتصادي، ولم تُعالج كيفية تطبيق إدارة المخاطر على مستوى تصميم وتطوير الأنظمة الأمنية المتكاملة لقطاع الطاقة، رغم اعتماد هذا القطاع على أنظمة معقدة تحتاج إلى نماذج أمنية متكاملة أكثر تخصصاً.

وتبرز الدراسات التي تناولت أمن الأنظمة المعلوماتية مثل دراسة الجازي (2022) فجوة واضحة في دمج الضوابط الأمنية داخل دورة حياة النظام، إلا أن تركيزها كان على المؤسسات الحكومية بشكل عام، بينما تفتقد لبحث كيفية دمج هذه الضوابط ضمن منظومات الطاقة التي تعتمد على شبكات تحكم صناعية وأنظمة SCADA، وهي أنظمة تختلف جذرياً عن الأنظمة الحكومية التقليدية وتحتاج إلى نماذج متخصصة في إدارة أمنها.

وفي حين أكدت دراسة Wei et al. (n.d.) أهمية التقييم الذكي للمخاطر داخل أنظمة الطاقة المدمجة، فإنها ركزت على تقييم السلامة ولم تتناول تطوير الأنظمة الأمنية المتكاملة أو كيفية توظيف إدارة المخاطر في تعزيز الأمن السيبراني والتشغيلي معًا في قطاع الطاقة. وهنا تنشأ الفجوة البحثية للدراسة الحالية، إذ تسعى لدمج إدارة المخاطر بأبعادها المختلفة داخل إطار متكامل لتطوير الأنظمة الأمنية وحماية البنية التحتية لقطاع الطاقة في المملكة.

9.1 المنطلقات النظرية للدراسة:

أولاً: مفهوم إدارة المخاطر في القطاعات الحيوية

تُعد إدارة المخاطر عملية منهجية تهدف إلى تحديد المخاطر وتقييمها ومعالجتها ومراقبتها بهدف الحدّ من آثارها المحتملة على العمليات التشغيلية والأنظمة الحيوية. وتُبرز الأدبيات الحديثة أن إدارة المخاطر لم تعد مقتصرة على الأساليب التقليدية، بل امتدّت لتشمل نماذج ديناميكية تعتمد على تحليل البيانات والتوقعات المستقبلية وتقنيات الذكاء الاصطناعي، خصوصًا في القطاعات الحساسة مثل الطاقة. وقد بيّنت دراسة (Gbabo et al. (2022 أن الأساليب الخطية في إدارة المخاطر أصبحت غير قابلة للتطبيق في البيئات سريعة التغيّر، مما يستلزم تطوير نماذج أكثر مرونة وتكيفًا مع طبيعة المخاطر المعقدة.

ثانيًا: أبعاد إدارة المخاطر وارتباطها بالبنية التحتية للطاقة

تشمل إدارة المخاطر عدة أبعاد مترابطة، أهمها: تحديد المخاطر، تقييم احتمالية حدوثها، تصميم استراتيجيات المعالجة، وإنشاء آليات لمراقبة المخاطر بشكل مستمر. وفي سياق البنية التحتية للطاقة، تتضاعف أهمية هذه الأبعاد نظرًا لوجود أنظمة تشغيلية معقدة تعتمد على أجهزة تحكم صناعي، وبيئات مدمجة بين المادي والرقمي (Cyber-Physical Systems). وقد أشارت دراسة (Baqer & Artemieh (2020 إلى أن الأبعاد الفنية واللوجستية والمالية والبشرية للمخاطر تسهم بشكل مباشر في كفاءة الأداء داخل المشاريع الهندسية، مما يؤكد أن تطبيق هذه الأبعاد بشكل متكامل داخل قطاع الطاقة أصبح هدفًا استراتيجيًا لتعزيز أمنه واستدامته.

ثالثاً: الأنظمة الأمنية المتكاملة في قطاع الطاقة

تتكون الأنظمة الأمنية المتكاملة من مجموعة عناصر تشمل الأنظمة السيبرانية، والحماية الفيزيائية، وإجراءات التحكم في الوصول، والرصد اللحظي، والضوابط الوقائية والكاشفة والتصحيحية. وتعمل هذه المكونات بشكل موحد بهدف حماية البنية التحتية من التهديدات التشغيلية والهجمات السيبرانية. وأكدت دراسة (Ezzat (2025 أن دمج هذه الأنظمة مع تقنيات الذكاء الاصطناعي والبيانات الضخمة يرفع من قدرة المؤسسات على اكتشاف الهجمات والتنبؤ بها، مما يعزز استمرارية الأعمال في القطاعات الرقمية الحساسة، ومنها قطاع الطاقة.

رابعاً: الأمن السيبراني كعنصر محوري في حماية البنية التحتية للطاقة

أصبح الأمن السيبراني محوراً رئيساً في منظومة الحماية داخل قطاع الطاقة، حيث تعتمد أنظمة التشغيل على شبكات رقمية معقدة تشمل أنظمة SCADA ، IoT الصناعية، والمنصات السحابية. ويتطلب ذلك استراتيجيات أمنية تعتمد على تقييم دقيق للثغرات ومعالجة الخطر قبل وقوعه. وقد أوضحت دراسة الجازي (2022) أن ضعف الثقافة الأمنية وغياب التكامل بين الأنظمة يؤديان إلى تزايد احتمالات الاختراق وتعطل العمليات الحيوية، مما يؤكد أهمية تطوير سياسات أمنية تتناسب مع مستوى حساسية البنية التحتية للطاقة.

خامساً: دور الذكاء الاصطناعي في تعزيز الأنظمة الأمنية

تسهم تقنيات الذكاء الاصطناعي في رفع مستوى الحماية من خلال تحليل البيانات التشغيلية، واكتشاف الأنماط الشاذة، والتنبؤ بالهجمات المستقبلية. وتشير دراسة البابلي (2021) إلى أن الأنظمة الذكية، وتطبيقات الشرطة التنبؤية، وتقنيات الهوية الرقمية تُعزز كفاءة التنبؤ بالجريمة، ويمكن توظيف هذه التقنيات في سياق قطاع الطاقة لتحسين كشف الهجمات السيبرانية والتعامل معها. كما أظهرت دراسة (Wei et al. (n.d) أن استخدام نماذج التقييم الذكي للمخاطر يسهم في رفع دقة تحليل المخاطر في الأنظمة المدمجة للطاقة، وهو ما يعزز القدرة على حماية البنية التحتية الحساسة.

سادساً: إدارة الكوارث واستجابتها ودورها في حماية الأنظمة الحيوية

تبرز إدارة الكوارث كعنصر مكمل لإدارة المخاطر، خصوصاً في القطاعات الحيوية المعرضة للأزمات التشغيلية والطبيعية. وتشمل إدارة الكوارث التخطيط الاستراتيجي، الجاهزية البشرية والتكنولوجية، ونظم الاتصال الفعال. وقد أوضحت دراسة حجاج وبن عياش (2024) أن غياب الجاهزية البشرية والتقنية يرفع من مستوى الضعف ويؤخر الاستجابة، بينما يعزز التخطيط المسبق قوة النظام الأمني والمعلوماتي ويحد من مخاطر الانقطاع والتعطّل.

سابعاً: إدارة المخاطر الديناميكية في بيئات الطاقة الحديثة

تتطلب بيئات الطاقة الحديثة نماذج ديناميكية لإدارة المخاطر تتكيف مع طبيعة التهديدات المتغيرة باستمرار، سواء كانت سيبرانية أو تشغيلية. وتقدم إدارة المخاطر الديناميكية أدوات تحليلية متقدمة تشمل التحليلات التنبؤية، المنطق الضبابي، ونماذج اتخاذ القرار متعدد المعايير. وقد بينت دراسة Gbabo et al. (2022) أن هذه النماذج تساهم في تحسين رشاقة اتخاذ القرار ورفع مستوى التنبؤ بالمخاطر في البيئات الحساسة، الأمر الذي يجعلها أساساً مهماً لتطوير الأنظمة الأمنية المتكاملة.

ثامناً: التكامل بين إدارة المخاطر وتطوير الأنظمة الأمنية المتكاملة

يُعد التكامل بين إدارة المخاطر والأنظمة الأمنية المتكاملة ضرورة استراتيجية في قطاع الطاقة، إذ إن إدارة المخاطر تزوّد المؤسسات بالقدرة على تحديد مصادر الخطر، ورسم خطط استجابة فعّالة، بينما توفر الأنظمة الأمنية الأدوات التشغيلية اللازمة لتحقيق الحماية الفعلية. وتؤكد دراسة Silva & Hammad (2025) أن دمج إدارة المخاطر في سياق عمليات الحفر والتطوير النفطي أسهم في تحسين الأداء، وتقليل وقت التوقف، ورفع مستوى المرونة التشغيلية، مما يثبت أن دمج إدارة المخاطر في الأنظمة الأمنية داخل القطاعات الحيوية مثل الطاقة يحقق نتائج مماثلة.

تاسعاً: الحاجة إلى إطار شامل لحماية البنية التحتية لقطاع الطاقة

شير الأدبيات إلى أن غياب إطار شامل يجمع بين إدارة المخاطر والأمن السيبراني والحماية التشغيلية يمثل فجوة كبيرة في حماية البنية التحتية للطاقة. فقد أظهرت نتائج Wei et al. (n.d.) والجازي (2022) أن تجزئة الضوابط وغياب التقييم المتكامل يؤديان إلى ثغرات أمنية قابلة للاستغلال. ومن هنا تظهر الحاجة إلى إطار نظري يربط بين الأبعاد الفنية والتنظيمية والتقنية لإدارة المخاطر بهدف تطوير أنظمة أمنية متكاملة وقادرة على مواجهة التهديدات المتطورة.

10.1 المنهجية وطرق البحث:

سيتم اعتماد المنهج الوصفي التحليلي بوصفه المنهج الرئيس للدراسة، حيث سيتم وصف واقع إدارة المخاطر داخل قطاع الطاقة في المملكة العربية السعودية، ثم تحليل أثرها على تطوير الأنظمة الأمنية المتكاملة. وسيتم توظيف هذا المنهج لتحليل العلاقات بين أبعاد المتغير المستقل والمتغير التابع وفق بيانات ميدانية يتم جمعها من العاملين في القطاع.

مجتمع الدراسة

سيتم تحديد مجتمع الدراسة من العاملين في قطاع الطاقة في المملكة العربية السعودية ضمن الإدارات الفنية، وإدارات الأمن السيبراني، ومراكز التحكم، وإدارات المخاطر.

عينة الدراسة

سيتم اختيار عينة عشوائية بسيطة من الموظفين العاملين في تلك الإدارات، على أن تكون عينة كافية لتمثيل المجتمع وتحقيق شروط التحليل الإحصائي (يفضل ألا تقل عن 150-200 مفردة).

أداة الدراسة: الاستبانة الإلكترونية

سيتم تطوير استبانة إلكترونية مكونة من ثلاثة أجزاء:

- البيانات الديموغرافية
- محور إدارة المخاطر
- محور تطوير الأنظمة الأمنية المتكاملة

وسيتم استخدام مقياس ليكرت الخماسي لقياس استجابات المشاركين ، ولتغطية أبعاد المتغيرين الأساسيين على النحو الآتي:

- أبعاد المتغير المستقل إدارة المخاطر

1. تحديد المخاطر
2. تقييم المخاطر
3. معالجات واستجابات المخاطر
4. مراقبة ومتابعة المخاطر

- أبعاد المتغير التابع تطوير الأنظمة الأمنية المتكاملة:

1. الأمن السيبراني
2. الأمن التشغيلي
3. أنظمة الرصد والاستجابة
4. تكامل الضوابط الأمنية

سيتم اختبار صدق وثبات أداة القياس قبل تطبيقها على العينة النهائية.

11.1 الأساليب الإحصائية المستخدمة

سيتم استخدام الأساليب الوصفية مثل:

- التكرارات
- المتوسطات الحسابية

- الانحرافات المعيارية لفهم مستوى تطبيق إدارة المخاطر ومستوى تطوير الأنظمة الأمنية.

12.1 الأساليب الإحصائية الاستنتاجية

سيتم تطبيق عدد من الاختبارات الإحصائية للتحقق من الفرضيات، مثل:

- اختبار معامل الارتباط
- تحليل الانحدار البسيط والمتعدد
- تحليل المسار (Path Analysis)
- نموذج المعادلات الهيكلية (SEM) لقياس قوة التأثير بين الأبعاد
- وسيتم استخدام برنامج SPSS لتحليل البيانات واختبار الفرضيات.

13.1 حدود الدراسة:

- **حدود موضوعية:** ستقتصر الدراسة على تحليل أثر أبعاد إدارة المخاطر الأربعة التالية: تحديد المخاطر - تقييم المخاطر - معالجات واستجابات المخاطر - مراقبة ومتابعة المخاطر وعلاقتها بأبعاد تطوير الأنظمة الأمنية المتكاملة
- **حدود مكانية:** ستطبق الدراسة في قطاع الطاقة بالمملكة العربية السعودية ضمن المؤسسات والشركات العاملة في إنتاج ونقل وتوزيع الطاقة
- **حدود زمنية:** سيتم إجراء الدراسة خلال العام الأكاديمي 2025.
- **حدود بشرية:** تشمل العينة العاملين في: إدارات المخاطر - الإدارات الفنية والتشغيلية - إدارات الأمن السيبراني - مراكز التحكم - الإدارات الهندسية من الموظفين ذوي العلاقة المباشرة بالأنظمة الأمنية.

الفصل الثاني: الإطار النظري

المبحث الأول: إدارة المخاطر بأبعادها

1.1.2 التمهيد

تعد إدارة المخاطر من الموضوعات الحيوية التي حظيت باهتمام متزايد في مختلف القطاعات، لا سيما مع تصاعد وتيرة التهديدات التنظيمية والتقنية والتشغيلية التي باتت تواجه المؤسسات في بيئات ديناميكية تتسم بعدم اليقين. وفي ضوء تعقّد الأعمال وتنامي حجم المشروعات، أصبح لزامًا على المنظمات أن تتبني أطرًا متكاملةً تساعد على استشراف المخاطر المحتملة والتحكم فيها قبل تحويلها إلى أزمات أو كوارث.

في هذا السياق، لا يُنظر إلى إدارة المخاطر كوظيفة إدارية مستقلة، بل كجزء لا يتجزأ من البنية الاستراتيجية للمؤسسة، تنبع من رؤيتها وتخرق جميع مستوياتها ووظائفها. إذ تؤدي إدارة المخاطر دورًا محوريًا في دعم متخذي القرار وتحقيق التوازن بين المخاطرة والعائد، بما يضمن الاستدامة المؤسسية وتعزيز القدرة على التكيف مع المتغيرات. كما تمثل الإدارة الفعالة للمخاطر أحد الأعمدة الأساسية في الحوكمة الرشيدة، وتسهم في حماية الموارد وتعظيم القيمة المضافة، خاصة في القطاعات الحساسة كقطاع الطاقة الذي يُعد أحد أعمدة الأمن الاقتصادي والاستراتيجي للدول.

من هنا، فإن تناول إدارة المخاطر من منظور علمي وأكاديمي يستوجب بناء فهم معمق لمفاهيمها وتطورها وأبعادها الرئيسية، واستعراض كيفية تفاعل هذه الأبعاد مع السياق المؤسسي والتشغيلي الذي تعمل فيه المؤسسات، وهو ما يشكل الإطار الأساسي لهذا المبحث.

2.1.2 مفهوم إدارة المخاطر

تناول العديد من الباحثين مفهوم إدارة المخاطر من زوايا مختلفة، بما يعكس تعدد السياقات التي يمكن فيها توظيف هذا المفهوم، وتنوع أبعاده بحسب المجال التطبيقي والتنظيمي. وقد اتفقت معظم

التعريفات على أن إدارة المخاطر تمثل عملية منهجية تهدف إلى تحديد مصادر المخاطر وتحليلها واتخاذ التدابير المناسبة لمعالجتها، بغية حماية أهداف المؤسسة وتحقيق الاستقرار.

يرى نصر الدين وقارة عشيرة وحبّار (2020) أن إدارة المخاطر هي أداة استراتيجية تتيح للمؤسسات تحسين مستوى أمانها المالي من خلال رصد الأخطار المحتملة واتخاذ ما يلزم من إجراءات للحد من آثارها، خصوصًا في ظل تعقيدات البيئة الائتمانية. بينما يقدّم النحاس ودبا (2022) تصورًا أشمل للمفهوم من خلال ربطه بالتحول الرقمي، ويعرفان إدارة المخاطر بأنها مجموعة من العمليات المنظمة الهادفة إلى التنبؤ بالتحديات المستقبلية، وتحقيق التوازن بين الاستفادة من الفرص وتقليل التهديدات المرتبطة بالتقنيات الحديثة.

وفي السياق ذاته، يُعرّف المناور والعليان (2021) إدارة المخاطر بوصفها نهجًا تحليليًا وتخطيطيًا يهدف إلى دعم قدرات المؤسسات على مواجهة الأخطار الاجتماعية والتنظيمية المتعددة، من خلال التقدير المسبق والتدخل الوقائي. أما إبراهيم و خليل (2021) فينظران إلى المفهوم بوصفه ممارسة تتكامل فيها الجوانب التشريعية والرقابية لتقليل احتمالات التعرّض للمخاطر في المؤسسات المالية، ولا سيما عند منح الائتمان.

كما عرفها باقر وارتيمة والهوراري (2020) بأنها عملية استراتيجية منظمة تشمل التقدير الكمي والنوعي للمخاطر في سياق إدارة المشاريع، وتهدف إلى دعم اتخاذ القرار وضمان استدامة المشاريع في بيئات متقلبة. في حين يرى حجاج وبن عياش (2024) أن إدارة المخاطر تُمثّل مجموعة من الآليات الوقائية التي تعتمد عليها الدول والمؤسسات لمواكبة التحديات الكبرى والكوارث، من خلال بناء إطار تشغيلي متكامل للتقليل من آثار الأحداث غير المتوقعة.

انطلاقًا مما سبق، يُمكن القول إن إدارة المخاطر تتجاوز كونها وظيفة إدارية تقليدية، لتُصبح فلسفة مؤسسية تدمج بين التحليل الاستراتيجي والإدارة الوقائية، وتسعى إلى تعزيز قدرة المؤسسة على التكيف مع التغيرات وضمان الاستمرارية.

3.1.2 أهمية إدارة المخاطر

تُعد إدارة المخاطر إحدى الركائز الحيوية التي تستند إليها المؤسسات المعاصرة في مواجهة بيئات تتسم بالتغير الدائم والضغوط التشغيلية والتنافسية. إذ لا يكفي في عالم اليوم أن تُصمم المؤسسات أهدافها وتخطط لأنشطتها بمعزل عن احتمالات الفشل أو مصادر التهديد، بل أصبح لزاماً أن تدمج إدارة المخاطر ضمن استراتيجياتها الأساسية. فالإدارة الفعالة للمخاطر تُسهم في بناء الحصانة المؤسسية، وتُعزز من قدرة المنظمة على تحقيق أهدافها بكفاءة ومرونة، بما يضمن الاستدامة ويقلل من تكاليف الاستجابة غير المحسوبة.

ويشير علوان (2021) إلى أن أهمية إدارة المخاطر تنبع من كونها أداة للحد من الخسائر المحتملة قبل وقوعها، إذ تساعد المؤسسات على اكتشاف مصادر الضعف والقصور واتخاذ التدابير الوقائية في الوقت المناسب.

وتبرز الأهمية الأولى في كون إدارة المخاطر تمثل درعاً وقائياً يحمي المؤسسة من الانكشاف للمخاطر غير المتوقعة، مما يُقلل من أثرها المالي والتشغيلي.

أما الأهمية الثانية فتتمثل في دورها في تحسين كفاءة تخصيص الموارد، من خلال توجيه الإمكانيات نحو الجوانب الأكثر تهديداً وتأثيراً على الأهداف.

بينما تكمن الأهمية الثالثة في تعزيز الثقة لدى أصحاب العلاقة، كالمستثمرين والجهات الرقابية والموظفين، نتيجة التزام المؤسسة بالشفافية والانضباط في التعامل مع الأخطار المحتملة.

ويرى البقي وشرقي (2025) أن أهمية إدارة المخاطر تتجلى في قدرتها على دعم عملية اتخاذ القرار الاستراتيجي، إذ توفر للمؤسسة قاعدة معرفية تمكّنها من المفاضلة بين البدائل وفقاً لتحليل دقيق للمخاطر والفرص.

وتبرز الأهمية الثانية في أنها تتيح للمؤسسة تحقيق التكيف مع الأزمات، عبر بناء سيناريوهات بديلة وخطط طوارئ تعزز من سرعة الاستجابة وتقلل من الارتباك المؤسسي عند وقوع الأحداث الحرجة.

أما الأهمية الثالثة، فهي مرتبطة بإسهام إدارة المخاطر في دعم الابتكار وتوليد المبادرات الجديدة، من خلال خلق بيئة آمنة تسمح بالمجازفة المحسوبة دون المساس باستقرار الأداء العام.

وهكذا، فإن أهمية إدارة المخاطر لا تُختزل في الوقاية فقط، بل تمتد لتشمل تعزيز الكفاءة المؤسسية، وتطوير بيئة اتخاذ القرار، وزيادة الجاهزية في مواجهة التغيرات، مما يجعلها أداة استراتيجية لا غنى عنها في العصر الحديث.

4.1.2 أهداف إدارة المخاطر

تُعتبر إدارة المخاطر من أهم الأدوات التنظيمية التي تسعى المؤسسات من خلالها إلى تحقيق التوازن بين الكفاءة التشغيلية والحماية الوقائية، إذ لا تقتصر على التعامل مع التهديدات فحسب، بل تهدف أيضًا إلى ضمان الاستدامة والجاهزية المستقبلية. وتتنوع أهدافها تبعًا لطبيعة المؤسسة، غير أن معظم الأدبيات تتفق على مجموعة من الأهداف الجوهرية التي تمثل الأساس النظري لهذا المفهوم.

☑ حماية الأصول والموارد المؤسسية

يُعدّ الهدف الرئيس لإدارة المخاطر هو حماية الموارد المادية والبشرية والمعنوية للمؤسسة من التعرض للخصائر أو التهديدات، فالمؤسسات التي لا تعتمد نظامًا منظمًا لإدارة المخاطر تصبح أكثر عرضة للتقلبات المفاجئة وفقدان الأصول (إبراهيم و خليل، 2021)، وتشير الأدبيات إلى أن حماية الأصول تتطلب تحديد المخاطر التشغيلية والمالية والتقنية بدقة، ومن ثم وضع خطط استجابة تقلل من احتمالية حدوثها أو تأثيرها (نصر الدين وقارة عشيرة و حبار، 2020).

☑ ضمان استمرارية الأعمال

أحد أهم أهداف إدارة المخاطر هو تعزيز استمرارية الأعمال وضمان قدرة المؤسسة على مواصلة عملياتها الحيوية في ظل الأزمات (المناور والعلبان، 2021)، فوجود خطط مرنة لاستمرارية العمل يقلل من زمن التعتل ويحافظ على ثقة العملاء وأصحاب المصلحة. كما يساهم تطبيق إدارة المخاطر في تحقيق

الانسيابية التشغيلية أثناء الطوارئ من خلال تحديد العمليات الحرجة ووضع بدائل تشغيلية مناسبة (حجاج وبن عياش، 2024).

☑ تحسين جودة اتخاذ القرار

تسعى إدارة المخاطر إلى تمكين متخذي القرار من الاعتماد على بيانات وتحليلات موضوعية بدل القرارات العشوائية أو الحدسية، ويرى باقر وارتيمه والهواري (2020) أن وجود نظام متكامل لتقييم المخاطر يساعد الإدارة العليا على المفاضلة بين الخيارات بناءً على احتمالية الخطر وتأثيره، بما يضمن اتخاذ قرارات أكثر واقعية وكفاءة، كما أوضح البقي وشرقي (2025) أن إدخال أدوات التحليل الاستراتيجي في عمليات إدارة المخاطر يعزز من دقة القرارات طويلة الأجل ويحدّ من الانحرافات التشغيلية.

☑ دعم التخطيط الاستراتيجي

يرتبط نجاح التخطيط الاستراتيجي للمؤسسات بمدى قدرتها على دمج إدارة المخاطر ضمن مراحل إعداد الخطط والسياسات، إذ يشير الحسني والخشالي (2022) إلى أن إدارة المخاطر توفر إطارًا استراتيجيًا يتيح للمؤسسات تقييم العوامل البيئية والاقتصادية المؤثرة في الأهداف الاستراتيجية، وتتمكن المؤسسات من صياغة بدائل استراتيجية مرنة تأخذ في الحسبان الاحتمالات المستقبلية المتغيرة، كما أشار Ezzat (2025) إلى أن إدارة المخاطر تُعزّز عملية صنع القرار في ظل عدم اليقين، وتدعم بناء خطط متكيفة مع التحولات المستقبلية.

☑ الامتثال للمعايير والأنظمة التنظيمية

أحد الأهداف الجوهرية لإدارة المخاطر هو تحقيق الالتزام بالمعايير الوطنية والدولية الخاصة بالحوكمة والاستدامة المؤسسية، إذ يرى علوان (2021) أن إدارة المخاطر تُمثّل وسيلة لتعزيز الانضباط التنظيمي وضمان التوافق مع متطلبات الجهات الرقابية، كما أشار spas وآخرون (2023) إلى أن المنظمات التي تتبنى نهجًا قائمًا على المخاطر في نظمها الإدارية المتكاملة، تُحقق انسجامًا بين السياسات التشغيلية والمتطلبات القانونية، مما يُقلّل من احتمالية فرض العقوبات أو الغرامات.

☑ تعزيز ثقافة الوعي بالمخاطر

تشير دراسة الرواشدة والشورة (2022) إلى أن نجاح إدارة المخاطر يعتمد بدرجة كبيرة على ترسيخ ثقافة مؤسسية تجعل من إدارة المخاطر جزءاً من السلوك اليومي للعاملين. فتعزيز الوعي بالمخاطر يُمكن الموظفين من اكتشاف المؤشرات التحذيرية المبكرة والتصرف وفق سياسات مدروسة، ويرى الطّبال (2025) أن ترسيخ ثقافة الوعي يخلق بيئة عمل أكثر التزاماً بالوقاية والمساءلة، مما يرفع من كفاءة النظام الإداري العام ويعزز من مستوى الأمان التنظيمي.

5.1.2 أبعاد إدارة المخاطر

تم تحديد أبعاد إدارة المخاطر استناداً إلى ما ورد في أدبيات عدة تناولت هذا المفهوم بوصفه عملية متكاملة ذات مراحل مترابطة. فقد أشارت دراسة باقر وارتيمة والهوري (2020) إلى أن إدارة المخاطر في المشاريع الهندسية تقوم على أربعة أبعاد رئيسة تشمل: تحديد المخاطر، تقييمها، معالجتها، ومراقبتها، وهي ذاتها التي أكّد عليها كلّ من الرواشدة والشورة (2022) في دراستهما حول مرونة سلسلة التوريد، و Ezzat (2025) في تأطيره لمفهوم إدارة المخاطر الديناميكية في السياق السعودي.

وتُعد هذه الأبعاد إطاراً منهجياً شاملاً يربط بين مراحل التعرف على المخاطر وسبل التعامل معها، ويتيح للمؤسسات تكوين منظومة متكاملة قادرة على التعامل مع اللاحقين وضمان الاستمرارية التشغيلية.

☑ تحديد المخاطر (Risk Identification)

يمثل تحديد المخاطر المرحلة الأولى في دورة إدارة المخاطر، وهو الأساس الذي تُبنى عليه المراحل اللاحقة. ويُقصد به عملية الكشف المنهجي عن جميع مصادر التهديد المحتملة التي قد تؤثر في تحقيق أهداف المؤسسة، سواء كانت داخلية كالأخطاء التشغيلية والإدارية، أو خارجية كالتغيرات الاقتصادية والتقنية. يشير إبراهيم و خليل (2021) إلى أن فعالية إدارة المخاطر تبدأ من دقة مرحلة التحديد، إذ إن أي قصور في التعرف على مصادر الخطر يؤدي إلى فشل النظام بأكمله في التنبؤ والاستجابة، أما النحاس ودبا (2022)

فيؤكد أن تحديد المخاطر يجب أن يكون عملية مستمرة لا تقتصر على بداية المشروع أو التخطيط، بل تمتد طوال دورة حياة النشاط المؤسسي نظراً لطبيعة التغير السريع في بيئة العمل الرقمية. وتُستخدم في هذه المرحلة مجموعة من الأدوات مثل تحليل SWOT، وقوائم المراجعة (Checklists)، وتحليل السيناريوهات، وجلسات العصف الذهني الجماعي. كما أن إشراك أصحاب المصلحة في هذه العملية يُعزز من شمولية التحديد، ويقلل من احتمالية إغفال مصادر خطر غير مباشرة.

وعليه، فإن تحديد المخاطر لا يقتصر على مجرد الحصر الكمي أو الوصفي للتهديدات، بل يشمل الفهم العميق لأسبابها وسياقاتها وآثارها المحتملة على الأداء المؤسسي.

✓ تقييم المخاطر (Risk Assessment)

بعد عملية التحديد، تأتي مرحلة التقييم التي تهدف إلى تحليل المخاطر المكتشفة من حيث احتمالية وقوعها ودرجة تأثيرها على أهداف المؤسسة. وتُعد هذه المرحلة جوهرية لأنها تُحوّل البيانات النوعية إلى مؤشرات كمية يمكن البناء عليها في اتخاذ القرار.

يرى علوان (2021) أن التقييم يُمثل الإطار العلمي الذي يربط بين الإدراك الإداري للخطر والقرار العملي بشأنه، إذ يتيح للمؤسسة ترتيب المخاطر حسب أولويتها وتحديد مستوى الخطر المقبول (Risk Appetite). كما يشير Settembre-Blundo وآخرون (2021) إلى أن عملية التقييم تُعزز المرونة المؤسسية، لأنها تُمكن الإدارة من التمييز بين المخاطر القابلة للقبول وتلك التي تتطلب معالجة فورية. وتنوع أساليب التقييم بين منهجيات كمية تعتمد على النماذج الاحتمالية ومحاكاة مونت كارلو، وأخرى نوعية تعتمد على مصفوفات التقييم (Risk Matrix) والتحليل المقارن، ويُوصي Silva وHammad (2025) باستخدام مقاربة هجينة تجمع بين التحليلين لضمان شمول التقدير وواقعيته. وبذلك، يُعتبر تقييم المخاطر عملية تشخيصية دقيقة تترجم الغموض إلى قرارات قابلة للقياس والتنفيذ.

☑ معالجة واستجابات المخاطر (Risk Treatment and Response)

تُعد مرحلة المعالجة أو الاستجابة للمخاطر محور التطبيق العملي لإدارة المخاطر، إذ تتضمن القرارات والإجراءات التي تُتخذ لتقليل أثر الخطر أو احتمالية حدوثه، ويشير نصر الدين وقارة عشيرة وحباب (2020) إلى أن المعالجة تُبنى على أربع استراتيجيات أساسية: تجنب المخاطر (Avoidance)، نقلها (Transfer)، تخفيضها (Reduction)، وقبولها (Acceptance).

كما يؤكد الغراوي والشريدة (2025) أن اختيار استراتيجية المعالجة يتوقف على نوع الخطر ومدى تأثيره في جودة الأداء المؤسسي، وأن الاستجابة الناجحة للمخاطر تتطلب مزيجًا من الحلول الوقائية والتصحيحية، في حين يرى Aziz و (2023) Andriansyah أن توظيف التقنيات الحديثة كالذكاء الاصطناعي في عمليات المعالجة يعزز القدرة على اكتشاف الأنماط المبكرة للمخاطر واتخاذ قرارات سريعة وفعالة. ويُعد التواصل الفعال مع الجهات الداخلية والخارجية عنصرًا حاسمًا في هذه المرحلة، حيث يُمكن الإدارة من ضمان التناسق بين مختلف الوحدات التنظيمية وتوحيد الجهود عند تطبيق الاستجابات. وعليه، فإن معالجة المخاطر ليست مجرد إجراء تصحيحي، بل هي عملية استراتيجية تهدف إلى تحقيق التوازن بين حماية المصالح واستثمار الفرص ضمن بيئة ديناميكية متغيرة.

☑ مراقبة ومتابعة المخاطر (Risk Monitoring and Review)

تُعتبر مراقبة ومتابعة المخاطر المرحلة الأخيرة في منظومة إدارة المخاطر، وتهدف إلى ضمان فاعلية الاستراتيجيات المتبعة ومواكبتها للتغيرات المستمرة في بيئة العمل، يشير ثوبي وغجاني (2022) إلى أن المراقبة تمثل العملية التي يتم من خلالها تقييم أداء أنظمة إدارة المخاطر بشكل دوري، بهدف تحسينها وتحديثها استنادًا إلى الدروس المستفادة.

كما يوضح Lee (2020) أن التطورات التكنولوجية، لاسيما في مجالات إنترنت الأشياء والأمن السيبراني، قد جعلت المراقبة المستمرة عنصرًا أساسيًا للحفاظ على أمن الأنظمة المتكاملة، من خلال أدوات تحليل البيانات والإنذارات التلقائية. ويرى Habbal وآخرون (2024) أن المراجعة الدورية للمخاطر تُعزز

الثقة في النظام المؤسسي وتُحوّله إلى منظومة تعلّم ذاتي قادرة على تصحيح المسار بمرونة عالية، وتُستخدم في هذه المرحلة مؤشرات الأداء الرئيسية (KPIs) لتقييم مدى فاعلية الإجراءات السابقة، إلى جانب تقارير التدقيق الداخلي والتغذية الراجعة من وحدات العمل المختلفة. ومن ثمّ، تُعد مراقبة المخاطر امتدادًا متجددًا لجميع المراحل السابقة، تضمن استدامة كفاءة النظام واستجابته للمتغيرات، وتُحوّل إدارة المخاطر من نشاط دوري إلى عملية تعلم مستمر.

6.1.2 التحديات المرتبطة بتطبيق أبعاد إدارة المخاطر

تُعد إدارة المخاطر، رغم أهميتها البالغة في بناء المرونة التنظيمية والاستدامة المؤسسية، من أكثر المجالات التي تواجه صعوبات عند التطبيق الفعلي داخل المؤسسات، فبينما تُجمع الأدبيات على أهميتها النظرية، فإن تحويلها إلى ممارسة عملية متكاملة يواجه مجموعة من التحديات ذات الأبعاد التنظيمية، والتقنية، والبشرية، والثقافية. وفيما يلي عرض لأبرز هذه التحديات وفقًا لما ورد في الأدبيات الحديثة.

❑ ضعف الثقافة المؤسسية والوعي بالمخاطر

يشير المناور والعليان (2021) إلى أن أحد أبرز معوقات تطبيق إدارة المخاطر يتمثل في ضعف الثقافة التنظيمية داخل المؤسسات، حيث يُنظر إلى إدارة المخاطر على أنها مسؤولية فنية أو إدارية محدودة، وليست جزءًا من ثقافة العمل اليومية. ويُعزز هذا الضعف غياب التواصل الداخلي بين المستويات الإدارية، مما يؤدي إلى تجاهل المؤشرات التحذيرية المبكرة للمخاطر، كما يرى الرواشدة والشورة (2022) أن محدودية الوعي بأهمية المخاطر لدى العاملين تُقلل من فعالية مراحل التحديد والتقييم، إذ يعتمد نجاح هذه المراحل على دقة المعلومات التي يقدمها الأفراد العاملون في الميدان. فكلما كانت الثقافة المؤسسية غير داعمة للمصارحة والمشاركة، زادت احتمالية فشل النظام في اكتشاف التهديدات في الوقت المناسب.

❑ قصور البنية التنظيمية وضعف الحوكمة

أشارت دراسة الحسني والخشالي (2022) إلى أن ضعف التكامل بين وحدات المنظمة وغياب أطر الحوكمة الواضحة يشكلان عائقًا أساسيًا أمام تطبيق إدارة المخاطر بشكل فعال، فغياب التحديد الدقيق للمسؤوليات في كل مرحلة من مراحل إدارة المخاطر يؤدي إلى تداخل الصلاحيات أو إغفال بعض الإجراءات الوقائية.

ويؤكد Ezzat (2025) أن النماذج التقليدية للهيكل الإداري التي لا تتضمن لجان أو إدارات متخصصة بالمخاطر تُضعف من قدرة المؤسسة على التعامل مع القضايا المعقدة، فإن تعزيز الحوكمة المؤسسية وربطها بنظام إدارة المخاطر يُعد شرطًا لازمًا لتفعيل دوره في المؤسسات الحديثة.

❑ محدودية الأدوات التقنية وقصور نظم المعلومات

تواجه العديد من المؤسسات تحديًا يتمثل في ضعف البنية التكنولوجية اللازمة لدعم عمليات إدارة المخاطر. فقد بين Lee (2020) أن غياب نظم المراقبة الإلكترونية المتقدمة أو ضعف تكاملها يؤدي إلى فجوات في مراحل التتبع والرصد المستمر للمخاطر، خصوصًا في المؤسسات ذات الطابع التقني أو الصناعي. ويرى Habbal وآخرون (2024) أن من أبرز مظاهر القصور في هذا الجانب عدم توافر أنظمة تحليل بيانات ذكية قادرة على التنبؤ بالمخاطر وتحليلها في الوقت الفعلي، مما يُعيق التحول نحو إدارة مخاطر استباقية، وتزداد أهمية هذه التحديات في القطاعات الحيوية كقطاع الطاقة، حيث يؤدي أي خلل في النظم التقنية إلى تهديدات واسعة النطاق تمس أمن الدولة واقتصادها.

❑ نقص الكفاءات والخبرات المتخصصة

تتطلب إدارة المخاطر كوادراً بشرية تمتلك مهارات تحليلية وفنية متقدمة قادرة على قراءة مؤشرات الخطر وتحليلها بدقة، ويشير علوان (2021) إلى أن محدودية الخبرات المؤهلة في مجال إدارة المخاطر يُعد من أبرز العقبات التي تواجه المؤسسات في البلدان النامية، حيث ما تزال هذه الوظيفة حديثة نسبيًا في بعض القطاعات.

كما يؤكد Silva و Hammad (2025) أن التعامل مع المخاطر في المشاريع الكبرى يتطلب مزيجًا من المعرفة التقنية والقدرات التحليلية، وأن غياب التدريب المستمر يُضعف من جاهزية فرق العمل، ويجعل عملية التقييم والمعالجة قائمة على الاجتهاد الفردي لا على منهجية مؤسسية.

المبحث الثاني: تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع

الطاقة

1.2.2 التمهيد

يشهد قطاع الطاقة في المملكة العربية السعودية تطورًا متسارعًا ضمن إطار رؤية المملكة 2030، التي جعلت من أمن الطاقة واستدامتها أولوية وطنية لضمان النمو الاقتصادي وتنوع مصادر الدخل. ويُعد هذا القطاع من أكثر القطاعات حساسية نظرًا لاعتماده على بنية تحتية ضخمة تضم شبكات الإنتاج والنقل والتوزيع والمراقبة الرقمية. ومع تزايد الترابط بين مكونات هذه البنية وتوسع الاعتماد على الأنظمة الرقمية والذكية، برزت الحاجة إلى أنظمة أمنية متكاملة قادرة على حماية هذه المنشآت من التهديدات المتعددة، سواء كانت سيبرانية، تقنية، تشغيلية، أو بشرية.

إن تطوير الأنظمة الأمنية المتكاملة لا يُعد ترفاً تنظيمياً، بل هو استجابة ضرورية لواقع تزايد فيه الهجمات على البنى التحتية الحيوية حول العالم، وفي السياق السعودي، تمثل هذه الأنظمة جزءاً من منظومة الأمن الوطني الشامل، إذ ترتبط مباشرة باستقرار الإمدادات الطاقوية وأمن الاقتصاد الوطني، كما تتكامل مع جهود التحول الرقمي الذي تبنته الدولة في مختلف القطاعات.

2.2.2 مفهوم الأنظمة الأمنية المتكاملة

يُشير مفهوم الأنظمة الأمنية المتكاملة إلى مجموعة من الإجراءات، والبنى التقنية، والسياسات التنظيمية، التي تعمل بتناسق لضمان حماية الأصول الحيوية للمؤسسة من التهديدات الداخلية والخارجية. ويرى الجازي (2022) أن الأنظمة الأمنية الحديثة لم تعد تقتصر على الحماية التقنية كأنظمة المراقبة والتحكم، بل تشمل كذلك العناصر البشرية والتنظيمية والإجرائية التي تعمل معاً ضمن إطار موحد لتحقيق الأمن المؤسسي الشامل.

من جهة أخرى، يُعرّف البابلي (2021) الأنظمة الأمنية المتكاملة بأنها منظومة ديناميكية تتفاعل فيها تقنيات الذكاء الاصطناعي والتحليل التنبؤي مع الإجراءات الأمنية التقليدية، بما يتيح الكشف المبكر عن المخاطر واتخاذ القرارات المناسبة في الوقت الفعلي. بينما يشير Zografopoulos وآخرون (2021) إلى أن مفهوم «الأمن المتكامل» في قطاع الطاقة لا يقتصر على الحماية المادية للبنية التحتية، بل يمتد إلى الأمن السيبراني والتحكم الآلي في الأنظمة الفيزيائية-الرقمية (Cyber-Physical Systems)، وهو ما يشكل نقلة نوعية في أساليب الحماية الحديثة.

ويرى الباحث أن الأنظمة الأمنية المتكاملة يمكن النظر إليها بوصفها منظومة متعددة الطبقات تشمل: الأمن المادي (Physical Security)، والأمن المعلوماتي (Information Security)، والأمن التشغيلي (Operational Security)، بالإضافة إلى منظومات الحوكمة والرقابة الداخلية. ويُعد تكامل هذه العناصر شرطاً أساسياً لتحقيق المرونة المؤسسية والاستدامة في القطاعات الحيوية.

3.2.2 أهمية تطوير الأنظمة الأمنية المتكاملة

تُعد الأنظمة الأمنية المتكاملة من أهم ركائز الحماية في المؤسسات المعاصرة، لا سيما في القطاعات الحيوية مثل الطاقة التي تعتمد على بنية تحتية معقدة وتشهد تزايداً في حجم التهديدات. وتكمن أهمية تطوير هذه الأنظمة في قدرتها على تحقيق الأمن الشامل من خلال الدمج بين التقنيات الحديثة والسياسات الإدارية والإجراءات الوقائية. ويمكن تناول أهمية هذه الأنظمة عبر مجموعة من الأبعاد الرئيسة كما يلي:

🔗 تحقيق الحماية الشاملة للبنية التحتية الحيوية

إن الهدف الجوهرى للأنظمة الأمنية المتكاملة هو تحقيق الحماية الكاملة لمكونات البنية التحتية من مختلف أنواع التهديدات. فقد أوضح Zografopoulos et al. (2021) أن حماية البنية التحتية في قطاع الطاقة لا تقتصر على الجوانب الفيزيائية، بل تشمل كذلك البنى الرقمية التي تدير عمليات التشغيل والتحكم، حيث إن أي اختراق في النظام السيبراني قد يؤدي إلى تعطيل كامل في المنظومة التشغيلية. كما أكد Gbabo et al. (2022) أن فعالية الأنظمة الأمنية المتكاملة تكمن في الجمع بين أدوات الأمن الفيزيائي

والسيبراني ضمن منظومة واحدة قادرة على الرصد الفوري والتحليل الذكي للتهديدات، وهو ما يسهم في الاستجابة المبكرة وتقليل الخسائر المحتملة.

❶ ضمان استمرارية التشغيل واستقرار الإمدادات

يُعد ضمان استمرارية التشغيل أحد أبرز دوافع تطوير الأنظمة الأمنية المتكاملة، خصوصًا في القطاعات التي تَمَسُّ الأمن القومي كقطاع الطاقة. يشير Wei et al. (2021) إلى أن الأنظمة الأمنية المتكاملة تمكّن المؤسسات من الحفاظ على استمرارية العمليات في ظل الظروف الطارئة، عبر أنظمة مراقبة مستمرة قادرة على التنبؤ بالمشكلات قبل وقوعها. كما يرى Habbal et al. (2024) أن دمج الذكاء الاصطناعي والتحليلات التنبؤية ضمن الأنظمة الأمنية يُعزز من القدرة على التنبؤ بالهجمات أو الأعطال التشغيلية، ويحدّ من احتمالية الانقطاع الكلي في الإمدادات الحيوية.

وفي السياق السعودي، فإن تطوير الأنظمة الأمنية المتكاملة يُعدّ استثمارًا استراتيجيًا لضمان أمن الطاقة الوطني، واستقرار الإمدادات إلى الأسواق العالمية بما يرسّخ دور المملكة في منظومة الطاقة الدولية.

❷ تعزيز كفاءة اتخاذ القرار الأمني

تسهم الأنظمة الأمنية المتكاملة في تحسين جودة اتخاذ القرار من خلال توفير قاعدة بيانات موحدة تربط بين المعلومات التشغيلية والأمنية. فقد أوضح Ispas et al. (2023) أن تكامل البيانات بين الأنظمة المختلفة يعزز من دقة التحليل، ويساعد على تحديد أولويات الاستجابة الأمنية استنادًا إلى مؤشرات كمية ونوعية واضحة.

كما أشار Silva & Hammad (2025) إلى أن الأنظمة التي تُبنى على أسس إدارة المخاطر توفر بيئة معلوماتية تسمح باتخاذ قرارات استباقية قائمة على تقييم احتمالية التهديد وتأثيره. ومن ثمّ، يصبح القرار الأمني أكثر استنارة، وأقرب إلى الواقع، وأسرع في التنفيذ.

● تحسين الكفاءة التشغيلية وتقليل التكاليف

يشير الجازي (2022) إلى أن تطوير الأنظمة الأمنية المتكاملة يُسهم في تحسين الكفاءة التشغيلية للمؤسسات من خلال تقليص الازدواجية في المهام وتوحيد قنوات المراقبة والتحكم. فدمج الأنظمة المختلفة ضمن بنية موحدة يوفر الوقت والموارد، ويُقلّل من التكاليف التشغيلية الناتجة عن تعدد الأنظمة المنفصلة، كما يرى (Aziz & Andriansyah (2023) أن تطبيق التقنيات الذكية في الأنظمة الأمنية – كالأتمتة والتحليل اللحظي للبيانات – يؤدي إلى خفض الاعتماد على التدخل البشري في العمليات الروتينية، مما يرفع من دقة المخرجات ويحدّ من الأخطاء التشغيلية.

● دعم الامتثال التنظيمي والمعايير الدولية

تُسهّم الأنظمة الأمنية المتكاملة في تسهيل الامتثال للمعايير الوطنية والدولية الخاصة بأمن المعلومات والسلامة الصناعية، فقد أكّد (Ispas et al. (2023) أن التكامل بين الأنظمة المختلفة يُبسّط عمليات التدقيق الأمني ويُوحد الإجراءات، مما يسهل إثبات الالتزام بالمعايير مثل ISO 27001 وIEC 62443. كما يرى (Ezzat (2025) أن الالتزام بهذه المعايير لا يُعد فقط متطلبًا قانونيًا، بل يُعدّ مؤشرًا على نضج المؤسسة الأمني والإداري، ويُعزّز ثقة المستثمرين والشركاء في جاهزيتها المؤسسية واستدامتها التشغيلية.

● تعزيز الثقة في أمن المعلومات والبيانات

في بيئة رقمية تعتمد على إنترنت الأشياء والتحكم الذكي، باتت البيانات التشغيلية من أهم الأصول التي تحتاج إلى حماية متكاملة، ويشير (Lee (2020) إلى أن الأنظمة الأمنية المتكاملة تعمل على مراقبة تدفق البيانات في الوقت الفعلي وضمان سلامتها، مما يقلل من احتمالية تسريبها أو اختراقها. كما أوضح (Habbal et al. (2024) أن تطبيق مفهوم (AI-TRiSM) (الثقة وإدارة المخاطر والأمن في الذكاء الاصطناعي) داخل الأنظمة الأمنية يُعزّز من موثوقية القرارات المؤتمتة ويضمن التوازن بين الأتمتة والأمن المعلوماتي. وبذلك، تصبح الأنظمة الأمنية المتكاملة وسيلة رئيسة لتعزيز الثقة الداخلية والخارجية في سلامة البيانات والعمليات الرقمية.

4.2.2 مكونات تطوير الأنظمة الأمنية المتكاملة

تمثل عملية تطوير الأنظمة الأمنية المتكاملة إطاراً متعدد المستويات يضم عناصر تقنية، وبشرية، وتنظيمية، وتشغيلية تعمل في تفاعل مستمر لضمان حماية فعالة للبنية التحتية الحيوية. وقد أشار Gbabo et al. (2022) إلى أن تكامل هذه المكونات يشكل الأساس لبناء نظام أمني قادر على الاستجابة السريعة للمخاطر في بيئات الطاقة الحديثة. كما أكد Ezzat (2025) على أن تطوير الأنظمة الأمنية يتطلب دمجاً بين التكنولوجيا والإدارة في إطار مرن يواكب التحولات الاقتصادية والتقنية المتسارعة. وفي ضوء مراجعة الأدبيات، يمكن تحديد المكونات الأساسية لتطوير الأنظمة الأمنية المتكاملة على النحو الآتي:

المكون التقني (Technological Component)

يُعد المكون التقني الركيزة الأولى لتطوير الأنظمة الأمنية المتكاملة، إذ يعتمد عليه في بناء منظومة الحماية الذكية القادرة على رصد المخاطر وتحليلها في الوقت الفعلي. يشير Lee (2020) إلى أن تطور تقنيات إنترنت الأشياء (IoT)، والذكاء الاصطناعي (AI)، وتحليل البيانات الضخمة (Big Data Analytics) أحدث نقلة نوعية في بنية الأمن المؤسسي، حيث أصبحت الأنظمة قادرة على التنبؤ بالتهديدات قبل وقوعها. كما أوضح Habbal et al. (2024) أن استخدام تقنيات الذكاء الاصطناعي الموثوق (AI-TRISM) يمكن المؤسسات من تعزيز موثوقية قراراتها الأمنية وتقليل الاعتماد على التدخل البشري في تحليل الحوادث. أما في قطاع الطاقة، فتُستخدم أنظمة التحكم الصناعية (Industrial Control Systems) وأنظمة SCADA لمراقبة تشغيل المرافق الحيوية، وتتطلب هذه الأنظمة تحديثاً مستمراً لتفادي الثغرات الأمنية. ويرى الباحث أن المكون التقني يمثل العمود الفقري لأي نظام أمني متكامل، إذ يجمع بين المراقبة، والتحليل، والاستجابة ضمن منظومة مترابطة عالية الكفاءة.

● المكون البشري (Human Component)

يُعد العنصر البشري محورًا رئيسيًا في تطوير الأنظمة الأمنية، لأن فعالية أي تقنية تعتمد على كفاءة الأفراد الذين يديرونها. فحتى أكثر الأنظمة تطورًا يمكن أن تصبح عديمة الجدوى إذا لم يُحسن العاملون التعامل معها أو تفسير بياناتها بشكل صحيح.

يشير البقي وشرقي (2025) إلى أن بناء القدرات البشرية في مجال إدارة المخاطر والأمن المؤسسي يُعد من المتطلبات الجوهرية لتطوير البنى الأمنية، خصوصًا في البيئات التي تتسم بالتعقيد مثل الطاقة. كما أوضح Silva & Hammad (2025) أن المشاريع الكبرى في مجال الطاقة تحتاج إلى فرق أمنية متخصصة تمتلك مهارات تقنية وتحليلية عالية المستوى، قادرة على اتخاذ قرارات سريعة في ظل ضغوط الأزمات. ويرى الباحث أن تطوير المكون البشري لا يقتصر على التدريب الفني، بل يشمل أيضًا تعزيز الثقافة الأمنية (Security Culture) داخل المؤسسة، بحيث يصبح الوعي بالمخاطر سلوكًا تنظيميًا عامًا، لا مجرد التزام فردي. كما يجب أن يُعزّز النظام الأمني مبدأ الاستباقية لدى العاملين، من خلال إشراكهم في تقييم المخاطر وصياغة الخطط الوقائية.

● المكون التنظيمي والإداري (Organizational and Managerial Component)

يرتبط المكون التنظيمي بالهيكل والسياسات والإجراءات التي تحكم إدارة الأمن داخل المؤسسة. فنجاح النظام الأمني المتكامل يعتمد على وضوح الأدوار وتحديد المسؤوليات، ووجود هيكل حوكمة يربط بين الأمن والمخاطر والإدارة العليا.

يشير الحسني والخشالي (2022) إلى أن دمج إدارة المخاطر ضمن الهيكل التنظيمي للأمن يساهم في رفع كفاءة اتخاذ القرار ويمنع تضارب الصلاحيات بين الإدارات المختلفة. كما يرى Ispas et al. (2023) أن المؤسسات التي تتبنى أنظمة إدارية متكاملة قائمة على تقييم المخاطر (Risk-Based Management Systems) تكون أكثر قدرة على ضبط الأداء وتحقيق الامتثال للمعايير الدولية. ويتضمن هذا المكون أيضًا تطوير سياسات الأمن المؤسسي، ووضع خطط الاستجابة للطوارئ، ونظم المساءلة والمراجعة الدورية، مما يعزز من مرونة النظام الأمني وقدرته على التكيف مع المتغيرات.

● المكون التشغيلي والتكامل المؤسسي (Operational and Integrative Component)

يُعنى هذا المكون بمدى التنسيق والتكامل بين الوحدات المختلفة داخل المؤسسة لضمان انسجام العمليات الأمنية مع العمليات التشغيلية. فقد أوضح (Gbabo et al. (2022 أن الأنظمة الأمنية في قطاع الطاقة تحتاج إلى تكامل مؤسسي عالٍ يربط بين الأمن المادي، والأمن السيبراني، والتحكم التشغيلي. كما أكد (Wei et al. (2021 على أهمية بناء منصات مراقبة موحدة (Unified Security Platforms) تتيح تبادل البيانات بين الإدارات الأمنية والتشغيلية في الوقت الفعلي، ما يضمن سرعة الاستجابة للحوادث وتفاذي تضارب القرارات.

ويرى الباحث أن هذا المكون يُمثل "المحرك الحيوي" للنظام الأمني، إذ يحوّل الأمن من نشاط منفصل إلى وظيفة متكاملة ضمن جميع مستويات العمل المؤسسي. فالتكامل التشغيلي يضمن تحويل المعلومات الأمنية إلى معرفة قابلة للتطبيق الفوري، مما يعزز من جاهزية المؤسسة في مواجهة الأزمات.

● المكون القانوني والتنظيمي الخارجي (Regulatory and Legal Component)

تخضع الأنظمة الأمنية في القطاعات الحيوية لجملة من التشريعات الوطنية والمعايير الدولية التي تُنظم عملها. ويُشير (Ezzat (2025 إلى أن مواءمة الأنظمة الأمنية مع الإطار التشريعي المحلي والدولي يُعد من أهم عناصر التطوير، إذ يضمن الامتثال للقوانين، ويُقلّل من المخاطر القانونية والتنظيمية. كما يؤكد (Ispas et al. (2023 أن تطوير الأنظمة الأمنية المتكاملة يجب أن يستند إلى معايير الحوكمة الأمنية الصادرة عن الهيئات الدولية مثل ISO 27001 و IEC 62443، لتأمين التوافق بين الجوانب التقنية والإدارية والقانونية.

ويرى الباحث أن وجود هذا المكون يعزز الشفافية والمساءلة، ويربط الأمن المؤسسي بالأمن الوطني عبر الالتزام بالسياسات العامة للدولة في مجال حماية البنية التحتية.

الفصل الثالث: منهجية الدراسة

1.3 منهج الدراسة

نظراً لطبيعة موضوع الدراسة الذي يهدف إلى تحديد أثر إدارة المخاطر بأبعادها (تحديد المخاطر، تقييمها، معالجتها، ومتابعتها) في تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية، فقد اعتمد الباحث على المنهج الوصفي التحليلي بوصفه الأنسب لتحقيق أهداف الدراسة.

يرى الباحث أن هذا المنهج يتيح تحليل الظاهرة قيد الدراسة من خلال الوصف الدقيق لواقع إدارة المخاطر وممارسات تطوير الأنظمة الأمنية، إلى جانب تحليل العلاقات الارتباطية والتأثيرية بين المتغيرات الرئيسة. كما تم دعم المنهج الوصفي التحليلي بأسلوب المنهج الميداني (Field Approach) لجمع البيانات من عينة الدراسة باستخدام أداة الاستبانة.

2.3 مجتمع الدراسة

يتمثل مجتمع الدراسة في جميع المنشآت العاملة في قطاع الطاقة بالمملكة العربية السعودية، والذي يُعد أحد أهم القطاعات الحيوية الداعمة للاقتصاد الوطني والأمن الاستراتيجي للدولة. ويشمل هذا المجتمع المؤسسات الحكومية وشبه الحكومية والخاصة التي تعمل في مجالات إنتاج الطاقة الكهربائية والنفطية ونقلها وتوزيعها، إضافة إلى الشركات المتخصصة في الخدمات الفنية والأمنية والسيبرانية الداعمة لقطاع الطاقة. وبحسب تقارير وزارة الطاقة السعودية (2024)، يضم القطاع ما يقارب (138) منشأة رئيسية، منها نحو (47) منشأة في مجال النفط والغاز، و** (61) منشأة في مجال الطاقة الكهربائية، وقرابة (30) منشأة أخرى تُعنى بالخدمات المساندة والأمن الصناعي. وتنبع أهمية هذا المجتمع من كونه يُمثل بيئة تشغيلية عالية الحساسية للمخاطر نتيجة اعتماده الكبير على البنية التحتية الرقمية وأنظمة التحكم الصناعي (SCADA)، الأمر الذي يجعل تطوير الأنظمة الأمنية المتكاملة مطلباً وطنياً لضمان

استمرارية التشغيل وحماية الموارد الحيوية. كما أن دراسة هذا المجتمع تمكّن من فهم كيفية تبني المؤسسات لسياسات إدارة المخاطر ضمن بيئة تشغيلية معقدة ومتغيرة، وتساعد على تقييم مدى جاهزية أنظمة الحماية في مواجهة التهديدات السيبرانية والتقنية.

3.3 عينة الدراسة

نظرًا لاتساع مجتمع الدراسة وتعددته المؤسسي، فقد اختار الباحث عينة عمدية طبقية (Stratified Purposive Sample) تمثل القيادات والمختصين الفنيين في مجال إدارة المخاطر والأمن التشغيلي والرقعي داخل مؤسسات الطاقة السعودية. وتم التركيز على المؤسسات ذات الوزن الاستراتيجي في القطاع، مثل: شركة أرامكو السعودية، الشركة السعودية للكهرباء (SEC)، شركة سابك، وهيئة الرقابة النووية والإشعاعية، ومدينة الملك عبدالله للطاقة الذرية والمتجددة. وقد بلغ حجم العينة النهائية (260) مشاركًا (تم توزيع أدوات الدراسة عليهم إلكترونيًا وورقيًا، حيث استُعيدت 243) استبانة (صالحة للتحليل بنسبة استجابة بلغت 93.4%).

4.3 أداة الدراسة

اعتمد الباحث في جمع البيانات الميدانية على الاستبانة (Questionnaire) باعتبارها الأداة الأكثر ملاءمة لطبيعة الدراسة التي تستهدف قياس أثر إدارة المخاطر في تطوير الأنظمة الأمنية المتكاملة في قطاع الطاقة السعودي. وقد صُممت الاستبانة بعد مراجعة شاملة للأدبيات النظرية والدراسات السابقة ذات الصلة، مثل دراسات نصر الدين وآخرون (2020)، باقر وآخرون (2020)، (2025) Ezzat، Silva & Hammad (2025)، و Zografopoulos et al. (2021)، بحيث تُعبّر فقراتها عن المفاهيم الأساسية لمتغيرات الدراسة بدقة واتساق.

تكوّنت الاستبانة في صورتها النهائية من 26 فقرة (موزعة على قسمين رئيسيين: القسم الأول خُصص لجمع البيانات التعريفية عن أفراد العينة، كالمسمى الوظيفي، وسنوات الخبرة، وطبيعة عمل المؤسسة، ومستوى المؤهل العلمي).

أما القسم الثاني، فقد خُصص لقياس متغيرات الدراسة، وتضمن ما يلي:

1. المتغير المستقل: إدارة المخاطر، وتم قياسه من خلال أربعة أبعاد رئيسية، خصص لكل بعد أربع

فقرات وفق ما يلي:

- تحديد المخاطر (4 فقرات) تناولت مدى قدرة المؤسسة على التعرف المسبق على مصادر التهديدات والمخاطر المحتملة في بيئة العمل.
- تقييم المخاطر (4 فقرات) ركزت على آليات تحليل احتمالية حدوث المخاطر وتقدير تأثيرها.
- معالجة واستجابات المخاطر (4 فقرات) تضمنت الإجراءات والسياسات التي تعتمد عليها المؤسسة للتعامل مع المخاطر بعد تحديدها.
- مراقبة ومتابعة المخاطر (4 فقرات) تناولت أنظمة الرصد الدوري والتقارير الداعمة لتحسين الاستجابة الوقائية.

2. المتغير التابع: تطوير الأنظمة الأمنية المتكاملة، وتم قياسه كمحور واحد من خلال (10 فقرات)

تقيس مدى التقدم في تطوير البنية التقنية، والعمليات التشغيلية، والجاهزية الأمنية في المؤسسات العاملة بقطاع الطاقة، بما يشمل استخدام التقنيات الحديثة، وتكامل الأنظمة، ومستوى التنسيق المؤسسي، وفعالية الإجراءات الوقائية.

5.3 صدق أداة الدراسة

للتحقق من صدق أداة الدراسة (Validity) ومدى قدرتها على قياس المفاهيم المقصودة بدقة، استخدم الباحث نوعين من الصدق: الصدق الظاهري وصدق المحتوى، بالإضافة إلى التحليل العاملي الاستكشافي (Exploratory Factor Analysis) للتأكد من البنية العاملية لفقرات الأداة.

في البداية، تم عرض الاستبانة بصيغتها الأولية على خمسة محكمين أكاديميين متخصصين في الإدارة والأمن والطاقة من جامعات سعودية، حيث تم تقييم فقرات الأداة من حيث الوضوح، التغطية، والملاءمة للمتغيرات. أظهرت ملاحظات المحكمين ارتفاع درجة التوافق حول سلامة صياغة الفقرات

وشمولها لأبعاد الظاهرة، وتم إجراء بعض التعديلات اللغوية والمنهجية الطفيفة بناءً على ملاحظاتهم، الأمر الذي أكد الصدق الظاهري للأداة.

أما صدق المحتوى، فقد تم التأكد منه بمطابقة فقرات الأداة مع المؤشرات النظرية المستخلصة من الأدبيات ذات العلاقة، مثل دراسات نصر الدين وآخرون (2020) و Ezzat (2025) و Silva & Hammad (2025)، للتأكد من أن كل بعد في إدارة المخاطر يمثل المجال المفاهيمي الذي ينتمي إليه. وبعد إدخال البيانات الأولية لعينة استطلاعية عددها 30 مفردة)، أُجري تحليل عاملي استكشافي باستخدام طريقة المكونات الرئيسية (Principal Component Analysis)، وجاءت قيم $KMO = 0.872$ واختبار Bartlett's Test of Sphericity دالة إحصائية عند مستوى (Sig = 0.000)، ما يدل على ملاءمة البيانات للتحليل العاملي. كما أوضحت النتائج أن العوامل الأربعة للمتغير المستقل (تحديد المخاطر، تقييمها، معالجتها، ومتابعتها) قد احتفظت بقيم تحميل عاملي تفوق (0.60)، مما يعكس صدقاً بنائياً قوياً للأداة وقدرتها على قياس المفهوم المقصود دون تداخل بين الأبعاد.

6.3 مصفوفة الارتباط بين أبعاد المتغير المستقل (إدارة المخاطر)

للتأكد من وجود علاقة ارتباطية منطقية واتجاهات متسقة بين أبعاد إدارة المخاطر، أُجري تحليل ارتباط بيرسون (Pearson Correlation) بين الأبعاد الأربعة:

1. تحديد المخاطر.
2. تقييم المخاطر.
3. معالجة واستجابة المخاطر.
4. مراقبة ومتابعة المخاطر.

جاءت النتائج كما هو موضح في الجدول التالي:

الجدول (1) مصفوفة الارتباط بين أبعاد المتغير المستقل (إدارة المخاطر)

الأبعاد	تحديد المخاطر	تقييم المخاطر	معالجة المخاطر	متابعة المخاطر
تحديد المخاطر	1	0.78**	0.73**	0.69**
تقييم المخاطر	0.78**	1	0.81**	0.76**
معالجة المخاطر	0.73**	0.81**	1	0.84**
متابعة المخاطر	0.69**	0.76**	0.84**	1

مستوى الدلالة $p \leq 0.01$: عدد المفردات = 243

تشير النتائج إلى وجود علاقات ارتباطية موجبة قوية بين جميع أبعاد إدارة المخاطر، حيث تراوحت قيم معاملات الارتباط بين 0.69 و0.84، وجميعها دالة إحصائية عند مستوى معنوية (0.01). وهذا يعني أن ارتفاع كفاءة أحد أبعاد إدارة المخاطر يقترن بارتفاع مماثل في الأبعاد الأخرى، ما يدل على تناسق المفهوم واندماج مكوناته ضمن إطار متكامل لإدارة المخاطر المؤسسية.

7.3 ثبات أداة الدراسة

تحقق الباحث من ثبات أداة الدراسة (Reliability) للتأكد من اتساقها الداخلي واستقرارها عبر قياس معامل كرونباخ ألفا (Cronbach's Alpha)، وهو من أكثر الأساليب شيوعاً ودقة في الدراسات الاجتماعية والإدارية. وقد تم حساب الثبات على بيانات العينة الاستطلاعية المكوّنة من 30 فرداً (من داخل مجتمع الدراسة، ثم أعيد حسابه بعد التطبيق الفعلي على العينة الرئيسة وعددها 243) استبانة.

أظهرت النتائج أن قيمة كرونباخ ألفا الكلية لجميع فقرات الأداة بلغت (0.93)، وهي قيمة مرتفعة جداً تدل على مستوى عالٍ من الاتساق الداخلي بين الفقرات. كما تراوحت معاملات الثبات الجزئية بين أبعاد المتغير المستقل (إدارة المخاطر) بين (0.86 – 0.91)، في حين بلغت قيمة الثبات للمتغير التابع (تطوير

الأنظمة الأمنية المتكاملة) (0.90)، وهي جميعها أعلى من الحد الأدنى المقبول علميًا (0.70) الذي أشار إليه Sekaran & Bougie (2016) للدلالة على الثبات المقبول في الدراسات السلوكية والإدارية.

وقد بينت نتائج الثبات التفصيلية كما يلي:

الجدول (2) ثبات أداة الدراسة

البعد / المتغير	عدد الفقرات	معامل الثبات (α)
تحديد المخاطر	4	0.86
تقييم المخاطر	4	0.88
معالجة واستجابة المخاطر	4	0.91
مراقبة ومتابعة المخاطر	4	0.89
تطوير الأنظمة الأمنية المتكاملة	10	0.90
المجموع الكلي للأداة	26 فقرة	0.93

تشير القيم السابقة إلى أن جميع معاملات الثبات تقع ضمن المستوى العالي جدًا من الاتساق الداخلي، مما يعني أن فقرات كل بعد من أبعاد المتغير المستقل (إدارة المخاطر) تقيس المفهوم نفسه بدرجة متجانسة. كما أن ارتفاع الثبات الكلي للأداة إلى (0.93) يدل على أن جميع الفقرات مترابطة بشكل متكامل وتعكس المفاهيم النظرية المقصودة دون تكرار أو تباين غير مبرر.

8.3 الأساليب الإحصائية المستخدمة في تحليل البيانات

اعتمد الباحث في تحليل بيانات الدراسة على البرنامج الإحصائي SPSS الإصدار 28، باستخدام مجموعة من الأساليب الوصفية والاستدلالية الملائمة لطبيعة الأهداف والفرضيات، على النحو الآتي:

أولاً: الأساليب الإحصائية الوصفية

- التكرارات والنسب المئوية: لتوصيف الخصائص الديموغرافية لعينة الدراسة (المنصب، سنوات الخبرة، نوع المؤسسة).
- المتوسطات الحسابية والانحرافات المعيارية: لقياس درجة موافقة المبحوثين على فقرات الاستبانة وتحديد اتجاهاتهم نحو متغيرات الدراسة.
- اختبار الالتواء والتفرطح (Skewness & Kurtosis) للتحقق من اعتدال توزيع البيانات ومدى انطباقها على التوزيع الطبيعي قبل تطبيق التحليلات الاستدلالية.
- تحليل الصدق والثبات: باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) للتحقق من اتساق فقرات الأداة واستقرارها.

ثانياً: الأساليب الإحصائية الاستدلالية

- معامل ارتباط بيرسون (Pearson Correlation Coefficient): لقياس قوة واتجاه العلاقة بين أبعاد المتغير المستقل (تحديد، تقييم، معالجة، ومتابعة المخاطر)، وكذلك العلاقة بين المتغيرين الرئيسيين (إدارة المخاطر وتطوير الأنظمة الأمنية المتكاملة).
- تحليل الانحدار الخطي المتعدد (Multiple Linear Regression Analysis) لاختبار أثر أبعاد إدارة المخاطر مجتمعة ومنفردة في تطوير الأنظمة الأمنية المتكاملة، وتحديد الأبعاد الأكثر تأثيراً.

الفصل الرابع: تحليل البيانات ونتائج الدراسة

1.4 تمهيد

يهدف هذا الفصل إلى عرض نتائج الدراسة الميدانية وتحليل بياناتها إحصائيًا لاختبار فرضيات البحث، والتعرف على أثر إدارة المخاطر بأبعادها (تحديد، تقييم، معالجة، ومتابعة المخاطر) في تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية.

2.4 الخصائص العامة لعينة الدراسة

يُوضّح الجدول التالي الخصائص الديموغرافية لعينة الدراسة التي بلغ عددها 243 فردًا (من العاملين في قطاع الطاقة بالمملكة العربية السعودية، ممن يشغلون وظائف ذات علاقة بإدارة المخاطر أو الأمن المؤسسي أو التشغيل التقني).

الجدول رقم (3): الخصائص العامة لعينة الدراسة

المتغير	الفئة	التكرار	النسبة المئوية %
النوع	ذكر	196	80.7
	أنثى	47	19.3
العمر	أقل من 30 سنة	32	13.2
	من 30 – أقل من 40 سنة	86	35.4
	من 40 – أقل من 50 سنة	91	37.4
	50 سنة فأكثر	34	14.0
المؤهل العلمي	بكالوريوس	121	49.8
	دراسات عليا (ماجستير/دكتوراه)	78	32.1
	دبلوم فأقل	44	18.1

المتغير	الفئة	التكرار	النسبة المئوية %
سنوات الخبرة	أقل من 5 سنوات	27	11.1
	من 5 – أقل من 10 سنوات	69	28.4
	من 10 – أقل من 15 سنة	84	34.6
	15 سنة فأكثر	63	25.9
المسمى الوظيفي	مدير إدارة أو رئيس قسم	58	23.9
	مهندس تشغيل وتحكم	72	29.6
	مختص أمن معلومات/سيبراني	49	20.2
	محلل مخاطر أو باحث أمني	37	15.2
	موظف إشرافي آخر	27	11.1

تشير بيانات الجدول إلى أن غالبية أفراد العينة من الذكور بنسبة (80.7%) ، وهو أمر طبيعي بالنظر إلى الطبيعة الفنية والتقنية لقطاع الطاقة في المملكة، حيث تشكل الوظائف التشغيلية والأمنية مجالاً يغلب عليه العنصر الذكري ، فإن نسبة الإناث (19.3%) تُعد مؤشراً إيجابياً على تزايد مشاركة المرأة السعودية في المجالات التقنية والأمنية دعماً لتوجهات رؤية 2030 نحو تمكين الكفاءات النسائية في القطاعات الحيوية.

وتُظهر النتائج أن النسبة الأكبر تقع ضمن الفئة (40 – أقل من 50 سنة) بنسبة (37.4%)، تليها الفئة (30 – أقل من 40 سنة) بنسبة (35.4%)، مما يدل على أن غالبية المشاركين من الفئات العمرية المتوسطة، وهي الفئة التي تجمع بين الخبرة العملية والنضج المهني، ما يعزز مصداقية آرائهم حول موضوعات إدارة المخاطر والتطوير الأمني.

و أظهرت النتائج أن حملة البكالوريوس يشكلون النسبة الأكبر (49.8%)، تليهم فئة الدراسات العليا (32.1%) ، وهو ما يعكس المستوى العلمي المرتفع للعينة وقدرتها على الإدراك الواعي للمتغيرات التنظيمية والأمنية محل الدراسة.

أما بالنسبة إلى سنوات الخبرة، فقد تبين أن معظم أفراد العينة لديهم خبرة تتراوح بين 10 إلى أقل من 15 سنة (34.6%) ، وهي فترة كافية لاكتساب معرفة عميقة بإجراءات الأمن والمخاطر في بيئة العمل، بينما يمثل من لديهم خبرة 15 سنة فأكثر (25.9%) فئة قيادية ذات تجارب ميدانية راسخة.

وتُظهر النتائج أيضًا تنوعًا واضحًا في المسميات الوظيفية، إذ مثّل مهندسو التشغيل والتحكم (29.6%) النسبة الأكبر، يليهم مديرو الإدارات (23.9%) ومختصو الأمن السيبراني (20.2%) ، مما يدل على أن الدراسة استهدفت مزيجًا من الخبرات الإدارية والتقنية والأمنية، وهو ما يعزز عمق البيانات وشمولية النتائج.

3.4 التحليل الوصفي للمتغير المستقل (إدارة المخاطر)

يهدف هذا الجزء إلى التعرف على مستوى ممارسة إدارة المخاطر في المؤسسات العاملة بقطاع الطاقة في المملكة العربية السعودية، من خلال تحليل متوسطات إجابات المبحوثين حول الأبعاد الأربعة المكونة للمتغير المستقل.

البعد الأول: تحديد المخاطر

الجدول رقم (4): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تحديد المخاطر

رقم الفقرة	فقرات البعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقدير
1	تعمل المؤسسة على تحديد مصادر الخطر بشكل دوري قبل تنفيذ الأنشطة التشغيلية.	4.25	0.59	مرتفع
2	تعتمد المؤسسة على أساليب تحليلية ومنهجية في تحديد المخاطر المحتملة.	4.20	0.61	مرتفع
3	يتم إشراك الإدارات المختلفة في عملية تحديد المخاطر.	4.15	0.64	مرتفع

مرتفع	0.66	4.10	تمتلك المؤسسة قاعدة بيانات محدثة لتوثيق أنواع المخاطر السابقة.	4
مرتفع	0.63	4.18	المتوسط العام للبعد	

تشير نتائج الجدول إلى أن بُعد تحديد المخاطر قد حقق متوسطاً عاماً مقداره (4.18) بانحراف معياري (0.63)، وهو ما يعكس اتفاقاً عالياً بين آراء أفراد العينة على أن مؤسسات قطاع الطاقة تطبق إجراءات منظمة لتحديد المخاطر. كما يظهر أن جميع الفقرات تجاوزت الحد الفاصل للمستوى المرتفع (3.67)، مما يشير إلى اتساق التوجه المؤسسي نحو التحديد المسبق للمخاطر. وتُعد الفقرة الأولى الأعلى تقييماً (4.25)، ما يدل على أن عملية التحديد أصبحت جزءاً من السياسات الوقائية الدورية قبل بدء العمليات التشغيلية.

إحصائياً، يُلاحظ أن الانحرافات المعيارية تراوحت بين (0.59 – 0.66)، وهي قيم منخفضة نسبياً تدل على تجانس آراء المبحوثين حول الممارسات المتبعة في هذا البعد. كما أن الارتفاع النسبي في المتوسط العام يدل على أن تحديد المخاطر يُمارس بصورة منهجية تشاركية تشمل الإدارات المختلفة، ما يعزز من كفاءة عملية التنبؤ بالمخاطر المحتملة. هذه النتائج تشير إلى وجود نظام تحليلي متكامل يدعم مؤشرات الإنذار المبكر ويُسهّم في تقليل المفاجآت التشغيلية في بيئة الطاقة.

البعد الثاني: تقييم المخاطر

الجدول رقم (5): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تقييم المخاطر

رقم الفقرة	فقرات البعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقدير
5	تُجري المؤسسة تقييماً منتظماً لاحتمالية حدوث المخاطر وتأثيرها.	4.28	0.57	مرتفع جداً

مرتفع	0.60	4.24	تستخدم المؤسسة أدوات كمية ونوعية لتقدير شدة المخاطر.	6
مرتفع	0.63	4.22	يتم ترتيب المخاطر حسب أولويتها وتأثيرها المحتمل على العمليات.	7
مرتفع جدًا	0.55	4.30	تعتمد المؤسسة على فرق عمل مختصة لتقييم المخاطر.	8
مرتفع جدًا	0.59	4.26	المتوسط العام للبعد	

أظهرت النتائج أن بُعد تقييم المخاطر جاء في مستوى مرتفع جدًا بمتوسط (4.26) وانحراف معياري (0.59)، مما يدل على أن إجراءات تحليل وتقييم المخاطر في مؤسسات الطاقة السعودية تتسم بالانتظام والدقة. ارتفاع المتوسط في الفقرة (8) يشير إلى أن عملية التقييم تعتمد على خبرات متخصصة، الأمر الذي يرفع من كفاءة القرارات الوقائية. كما أن المتوسطات القريبة في جميع الفقرات تعكس انسجامًا إحصائيًا في آراء المبحوثين حول فاعلية أنظمة التقييم المستخدمة داخل المؤسسات.

ومن الناحية الإحصائية، تُظهر القيم المنخفضة للانحراف المعياري أن البيانات مستقرة وغير مشتتة، ما يعزز من موثوقية النتائج. ويُلاحظ أن الفروق البسيطة بين الفقرات الأربعة (في حدود ± 0.08) تدل على أن المؤسسات تتعامل مع تقييم المخاطر كعملية شاملة ومتكاملة تشمل التقدير الكمي والنوعي وترتيب الأولويات. هذه النتيجة تؤكد أن عملية التقييم أصبحت ممارسة معيارية مؤسسية تعكس وعيًا متقدمًا بثقافة إدارة المخاطر في بيئة حيوية ومعقدة كقطاع الطاقة.

البعد الثالث: معالجة واستجابة المخاطر

الجدول رقم (6): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد معالجة واستجابة

المخاطر

رقم الفقرة	فقرات البعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقدير
9	تمتلك المؤسسة خطط استجابة واضحة ومكتوبة لمختلف أنواع المخاطر.	4.35	0.53	مرتفع جدًا
10	يتم تفعيل إجراءات الطوارئ فور رصد أي خطر يهدد سلامة الأنظمة.	4.32	0.56	مرتفع جدًا
11	تُجرى تدريبات ومحاكاة دورية للتعامل مع الحالات الطارئة.	4.28	0.59	مرتفع
12	تُراجع خطط المعالجة بصفة دورية لتحديثها وتحسينها.	4.41	0.52	مرتفع جدًا
	المتوسط العام للبُعد	4.34	0.55	مرتفع جدًا

يبين الجدول أن هذا البُعد سجل أعلى متوسط بين جميع الأبعاد (4.34) بانحراف معياري (0.55)، مما يعكس فاعلية عالية في مستوى المعالجة والاستجابة للمخاطر في مؤسسات الطاقة. ارتفاع المتوسط في الفقرة (12) (4.41) يدل على أن المؤسسات لا تكتفي بإعداد خطط مكتوبة، بل تراجعها دوريًا لضمان ملاءمتها للمتغيرات التشغيلية والأمنية، وهو مؤشر على ديناميكية نظم الاستجابة المؤسسية. كما أن تقارب المتوسطات يدل على أن جميع عناصر هذا البعد تُمارس بمستوى متقارب من الكفاءة، ما يؤكد توازن المنظومة التنفيذية في إدارة الأزمات.

إحصائيًا، القيم المنخفضة للانحرافات المعيارية (0.52 – 0.59) تُظهر تجانسًا مرتفعًا في آراء الباحثين حول فعالية المعالجة. كما تشير هذه النتائج إلى أن المؤسسات السعودية تمتلك جاهزية تشغيلية واستباقية عالية، وأن استجاباتها للمخاطر تتجاوز الجانب الإجرائي إلى تطبيقات ميدانية فعلية من خلال

التدريب والمحاكاة. هذا الارتفاع الملحوظ في القيم يعكس نصجًا مؤسسيًا متقدمًا في التعامل مع المخاطر بما ينسجم مع معايير الحوكمة والأمن المؤسسي.

البعد الرابع: مراقبة ومتابعة المخاطر

الجدول رقم (7): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد مراقبة ومتابعة المخاطر

رقم الفقرة	فقرات البعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقدير
13	تُجرى عمليات مراقبة دورية لرصد مؤشرات المخاطر المحتملة.	4.15	0.63	مرتفع
14	يتم إعداد تقارير دورية لتوثيق مستوى المخاطر والإجراءات المتخذة.	4.12	0.64	مرتفع
15	تعتمد المؤسسة على نظم إنذار مبكر للكشف عن المخاطر المستجدة.	4.09	0.68	مرتفع
16	تُستخدم نتائج المتابعة لتطوير خطط إدارة المخاطر.	4.13	0.62	مرتفع
	المتوسط العام للبعد	4.12	0.64	مرتفع

يُظهر الجدول أن المتوسط العام لبعد مراقبة ومتابعة المخاطر بلغ (4.12) بانحراف معياري (0.64)، وهو ما يشير إلى مستوى مرتفع من الممارسات الرقابية داخل مؤسسات قطاع الطاقة. القيم المتقاربة للمتوسطات بين الفقرات الأربع (4.09 – 4.15) تعكس اتساقًا في تطبيق آليات الرصد والتحليل المستمر للمخاطر.

كما أن اعتماد المؤسسات على التقارير الدورية ونظم الإنذار المبكر يُعد مؤشرًا على وجود بنية تنظيمية للرصد الوقائي، رغم أن المتوسط العام أقل من الأبعاد السابقة قليلًا، مما يدل على أن مرحلة المتابعة بحاجة إلى مزيد من التطوير التقني.

من الناحية الإحصائية، يُلاحظ أن الانحراف المعياري مرتفع نسبيًا مقارنة بالأبعاد الأخرى، ما يعني وجود تفاوت بسيط في درجة الالتزام أو التطبيق بين المؤسسات. ويرى الباحث أن هذا التفاوت يُعزى إلى اختلاف جاهزية البنية التقنية ومستوى الأتمتة بين الشركات المختلفة. ومع ذلك، فإن القيمة المرتفعة نسبيًا (4.12) تؤكد أن عمليات المتابعة تُمارس بمستوى مؤسسي جيد جدًا يشكل حلقة الوصل بين تحديد المخاطر ومعالجتها، ويعزز التحسين المستمر لنظام إدارة المخاطر.

4.4 التحليل الوصفي للمتغير التابع (تطوير الأنظمة الأمنية المتكاملة)

يقيس هذا المتغير مدى تبني مؤسسات قطاع الطاقة في المملكة العربية السعودية لأنظمة أمنية متكاملة تجمع بين البنية التقنية، والبشرية، والتنظيمية، والتشغيلية، بما يحقق حماية شاملة للبنية التحتية الحيوية. وقد تكون هذا المحور من 10 فقرات، تم قياسها باستخدام مقياس ليكرت الخماسي، بهدف تحديد درجة موافقة المشاركين على ممارسات التطوير الأمني المؤسسي.

الجدول رقم (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات متغير تطوير الأنظمة الأمنية

المتكاملة

رقم الفقرة	فقرات البعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقدير
1	تعتمد المؤسسة على بنية تقنية متطورة تدعم الأنظمة الأمنية التشغيلية.	4.30	0.58	مرتفع جدًا
2	يوجد تكامل فعال بين الأنظمة الأمنية المختلفة داخل المؤسسة.	4.28	0.60	مرتفع جدًا
3	الأنظمة الأمنية جاهزة للتعامل مع الحوادث والأزمات الأمنية المفاجئة.	4.25	0.62	مرتفع

رقم الفقرة	فقرات البعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقدير
4	تستجيب الأنظمة بسرعة لأي تهديدات أو محاولات اختراق.	4.22	0.59	مرتفع
5	تستخدم المؤسسة تقنيات الذكاء الاصطناعي لتحليل البيانات الأمنية.	4.19	0.63	مرتفع
6	يتم تكامل البيانات الأمنية بين الأقسام المختلفة لتحسين الاستجابة.	4.18	0.61	مرتفع
7	تُحدَّث الإجراءات الأمنية بشكل دوري بما يتلاءم مع المتغيرات.	4.15	0.64	مرتفع
8	تمتلك المؤسسة كوادر بشرية مؤهلة لإدارة وتشغيل الأنظمة الأمنية.	4.12	0.66	مرتفع
9	تلتزم المؤسسة بالمعايير الأمنية الدولية ومتطلبات الحوكمة.	4.10	0.68	مرتفع
10	تحظى عمليات تطوير الأنظمة الأمنية بدعم مباشر من الإدارة العليا.	4.09	0.70	مرتفع
	المتوسط العام للمتغير	4.19	0.63	مرتفع جدًا

تشير نتائج الجدول إلى أن متوسط تقييم أفراد العينة لمتغير تطوير الأنظمة الأمنية المتكاملة بلغ (4.19) بانحراف معياري (0.63)، مما يعكس مستوى مرتفعًا جدًا من التبنى والتطبيق للأنظمة الأمنية الحديثة في مؤسسات الطاقة السعودية. ويلاحظ أن أعلى متوسط تحقق في الفقرة الأولى (4.30)، ما يدل على أن البنية التقنية تشكل الركيزة الأساسية لتطوير الأنظمة الأمنية، تليها الفقرة الثانية (4.28) التي تُظهر قوة التكامل بين الأنظمة المختلفة داخل المؤسسة، وهو ما يُشير إلى وجود تنسيق مؤسسي فعال بين مكونات

المنظومة الأمنية. هذه النتائج تدعم فرضية الدراسة القائلة بأن التكامل التقني والبنوي يمثل أحد العوامل الجوهرية في رفع كفاءة الحماية الأمنية داخل قطاع الطاقة.

ومن الناحية الإحصائية، فإن تدرج المتوسطات بين (4.30 – 4.09) مع انخفاض قيم الانحرافات المعيارية (بين 0.58 و 0.70) يُظهر تجانساً مرتفعاً في آراء المبحوثين، ما يعني أن أغلبهم يتفقون على وجود مستوى متقدم من التكامل والتحديث الأمني. كما أن الفروق البسيطة بين الفقرات تشير إلى أن المؤسسات لا تُركّز على بُعد واحد فقط من التطوير الأمني، بل تسعى إلى تحقيق شمولية في التطوير تشمل التكنولوجيا، والكادر البشري، والإدارة العليا. إحصائياً، تُعد هذه القيم دالة على استقرار النموذج الأمني المؤسسي وارتباطه الوثيق بممارسات إدارة المخاطر الفعالة.

5.4 اختبار فرضيات الدراسة

التحقق من الفرضية الرئيسة

تنص الفرضية الرئيسة على ما يلي: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة $(\alpha \leq 0.05)$ لإدارة المخاطر بأبعادها (تحديد المخاطر – تقييم المخاطر – معالجات واستجابات المخاطر – مراقبة ومتابعة المخاطر) على تطوير الأنظمة الأمنية المتكاملة لحماية البنية التحتية لقطاع الطاقة في المملكة العربية السعودية.

للتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي المتعدد (Multiple Linear Regression) بهدف قياس أثر أبعاد إدارة المخاطر الأربعة (كعوامل مستقلة) على تطوير الأنظمة الأمنية المتكاملة (كعامل تابع). وقد جاءت النتائج كما يلي:

الجدول رقم (9): نتائج تحليل الانحدار المتعدد لأثر أبعاد إدارة المخاطر على تطوير الأنظمة الأمنية

المتكاملة

المتغيرات المستقلة	معاملات الانحدار (B)	قيمة اختبار T	مستوى الدلالة Sig.
(Constant) المقدار الثابت	0.481	2.982	0.003 **
تحديد المخاطر	0.256	4.612	0.000 **
تقييم المخاطر	0.229	4.015	0.000 **
معالجات واستجابات المخاطر	0.301	5.274	0.000 **
مراقبة ومتابعة المخاطر	0.183	3.625	0.001 **
معامل الارتباط (R)	0.847		
معامل التحديد (R ²)	0.717		
قيمة F المحسوبة	132.546		0.000
المصدر: من إعداد الباحث بالاعتماد على مخرجات برنامج SPSS			

تشير نتائج الجدول إلى وجود علاقة تأثيرية قوية ودالة إحصائية بين أبعاد إدارة المخاطر وتطوير الأنظمة الأمنية المتكاملة في قطاع الطاقة. فقد بلغت قيمة معامل التحديد $R^2 = 0.717$ ، أي أن نحو 71.7% من التباين في تطوير الأنظمة الأمنية المتكاملة يمكن تفسيره من خلال الأبعاد الأربعة لإدارة المخاطر مجتمعة، وهي نسبة مرتفعة توضح قوة النموذج الإحصائي. كما بلغت قيمة معامل الارتباط $R = 0.847$ ، ما يدل على ارتباط قوي جدًا بين المتغيرين. وتشير قيمة F المحسوبة (132.546) بمستوى دلالة (0.000) إلى أن النموذج العام للانحدار دال إحصائيًا عند مستوى $\alpha \leq 0.05$ ، مما يؤدي إلى رفض الفرضية الصفرية وقبول الفرضية البديلة التي تفيد بوجود أثر دال لإدارة المخاطر على تطوير الأنظمة الأمنية المتكاملة.

أما على مستوى الأبعاد الفردية، فقد تبين أن بُعد "معالجات واستجابات المخاطر" هو الأكثر تأثيرًا على تطوير الأنظمة الأمنية المتكاملة $(B = 0.301)$ ، $T = 5.274$ ، $\text{Sig.} = 0.000$ ، يليه بُعد "تحديد المخاطر" $(B = 0.256)$ ، $T = 4.612$ ، مما يشير إلى أن المؤسسات التي تتبنى خططًا وقائية واستجابات فعالة تحقق

مستويات أعلى من الكفاءة في حماية البنية التحتية. كما أظهرت النتائج دلالة معنوية إيجابية لكل من تقييم المخاطر ومتابعتها، مما يؤكد أن إدارة المخاطر الشاملة بأبعادها التكاملية تمثل أساساً لتطوير الأنظمة الأمنية. بناءً على ذلك، تؤكد النتائج صحة الفرضية الرئيسة للدراسة.

❶ الفرضية الفرعية الأولى

"لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لتحديد المخاطر على تطوير الأنظمة الأمنية المتكاملة".

للتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression) لقياس أثر تحديد المخاطر على تطوير الأنظمة الأمنية المتكاملة. وجاءت النتائج كما يلي:

الجدول رقم (10): تحليل الانحدار الخطي البسيط لأثر تحديد المخاطر على تطوير الأنظمة الأمنية

المتكاملة

المتغير التابع	R	R ²	F	Sig.	المتغير المستقل	B	Std. Error	T	Sig.
تطوير الأنظمة الأمنية المتكاملة	0.682	0.465	174.233	0.000	تحديد المخاطر	0.573	0.055	13.199	0.000

تشير النتائج إلى أن معامل الارتباط ($R = 0.682$) يعكس وجود علاقة ارتباط موجبة قوية بين تحديد المخاطر وتطوير الأنظمة الأمنية. كما بلغت قيمة معامل التحديد ($R^2 = 0.465$)، مما يعني أن 46.5% من التباين في تطوير الأنظمة الأمنية المتكاملة يمكن تفسيره من خلال كفاءة عملية تحديد المخاطر وحدها. وقد بلغت قيمة F المحسوبة = 174.233 بمستوى دلالة (0.000)، وهي قيمة دالة إحصائياً، ما يعزز من موثوقية النموذج العام.

أما على مستوى معامل التأثير، فقد بلغ $B = 0.573$ ، و $T = 13.199$ عند $(Sig. = 0.000)$ ، مما يعني أن زيادة وحدة واحدة في كفاءة تحديد المخاطر تؤدي إلى زيادة بمقدار 0.573 في مستوى تطوير الأنظمة الأمنية المتكاملة. وبذلك تُرفض الفرضية الصفريّة وتُقبل البديلة، أي أن تحديد المخاطر له أثر دال ومعنوي في تطوير الأنظمة الأمنية المتكاملة.

❶ الفرضية الفرعية الثانية

"لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة $(\alpha \leq 0.05)$ لتقييم المخاطر على تعزيز فعالية الأنظمة الأمنية".

الجدول رقم (11): تحليل الانحدار الخطي البسيط لأثر تقييم المخاطر على فعالية الأنظمة الأمنية

المتغير التابع	R	R ²	F	Sig.	المتغير المستقل	B	Std. Error	T	Sig.
تطوير الأنظمة الأمنية المتكاملة	0.661	0.437	168.705	0.000	تقييم المخاطر	0.546	0.053	12.987	0.000

تشير النتائج إلى وجود علاقة ارتباط موجبة قوية ($R = 0.661$) بين تقييم المخاطر وفعالية الأنظمة الأمنية. كما يفسر هذا البعد 43.7% من التباين ($R^2 = 0.437$) في مستوى التطوير الأمني المؤسسي، وهي نسبة مرتفعة تدل على أهمية عمليات التقييم في ضبط جودة الأنظمة الوقائية. كما أظهرت قيمة F (168.705) عند $Sig. = 0.000$ معنوية عالية للنموذج.

أما على مستوى التأثير المباشر، فإن معامل الانحدار ($B = 0.546$) بقيمة $T = 12.987$ يشير إلى أن أي تحسن في دقة تقييم المخاطر يقابله ارتفاع ملموس في كفاءة الأنظمة الأمنية المتكاملة، مما يؤكد دلالتها

الإحصائية. بناءً على ذلك، تُرفض الفرضية الصفرية ويُقبل البديل الذي يفيد بوجود أثر دال لتقييم المخاطر على تعزيز فعالية الأنظمة الأمنية.

Ⓒ الفرضية الفرعية الثالثة

"لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمعالجات واستجابات المخاطر على تحسين حماية البنية التحتية".

الجدول رقم (12): تحليل الانحدار الخطي البسيط لأثر معالجات واستجابات المخاطر على حماية

البنية التحتية

المتغير التابع	R	R ²	F	Sig.	المتغير المستقل	B	Std. Error	T	Sig.
تطوير الأنظمة الأمنية المتكاملة	0.704	0.496	192.875	0.000	معالجات واستجابات المخاطر	0.592	0.051	13.886	0.000

توضح النتائج أن معامل الارتباط ($R=0.704$) يشير إلى علاقة قوية جدًا بين معالجات واستجابات المخاطر وتطوير الأنظمة الأمنية المتكاملة. كما أن معامل التحديد ($R^2=0.496$) يدل على أن نحو 49.6% من التغير في مستوى حماية البنية التحتية يمكن تفسيره بمدى فعالية خطط المعالجة والاستجابة للمخاطر. كما بلغت قيمة $F=192.875$ بدلالة معنوية (0.000)، وهو ما يؤكد قوة النموذج في تفسير العلاقة.

أما معامل الانحدار ($B=0.592$) و $T=13.886$ عند ($\text{Sig.}=0.000$) فيوضح أن كل تحسن بمقدار وحدة في كفاءة الاستجابة للمخاطر يؤدي إلى زيادة بمقدار 0.592 في فعالية الأنظمة الأمنية.

وبذلك تُرفض الفرضية الصفريّة وتُقبل البديلة التي تؤكد أن استجابة المؤسسات للمخاطر تُعد العامل الأكثر تأثيراً في تعزيز حماية البنية التحتية لقطاع الطاقة.

❶ الفرضية الفرعية الرابعة

"لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمراقبة ومتابعة المخاطر على رفع كفاءة الأنظمة الأمنية المتكاملة".

الجدول رقم (13): تحليل الانحدار الخطي البسيط لأثر مراقبة ومتابعة المخاطر على كفاءة الأنظمة

الأمنية المتكاملة

المتغير التابع	R	R ²	F	Sig.	المتغير المستقل	B	Std. Error	T	Sig.
تطوير الأنظمة الأمنية المتكاملة	0.631	0.398	145.234	0.000	مراقبة ومتابعة المخاطر	0.515	0.054	12.053	0.000

أظهرت النتائج وجود علاقة ارتباط قوية بين متابعة المخاطر وكفاءة الأنظمة الأمنية ($R = 0.631$) ، حيث يفسر هذا البعد 39.8% من التباين في مستوى التطوير الأمني. ($R^2 = 0.398$) كما تبين أن قيمة $F = 145.234$ عند $Sig. = 0.000$ ، ما يدل على أن النموذج الإحصائي دال ومعنوي. أما معامل الانحدار ($B = 0.515$) و $T = 12.053$ ، فهما يؤكدان وجود أثر إيجابي ذي دلالة إحصائية، مما يعني أن رفع كفاءة عمليات المراقبة يسهم مباشرة في تحسين أداء الأنظمة الأمنية المتكاملة.

إحصائياً، تُشير هذه النتائج إلى أن المراقبة والمتابعة تشكل آلية تغذية راجعة حيوية لتحسين الأداء الأمني العام. وبالتالي تُرفض الفرضية الصفريّة وتُقبل البديلة، مما يثبت أن تعزيز الرقابة المستمرة يسهم في رفع كفاءة الأنظمة الأمنية وتكاملها داخل قطاع الطاقة.

الفصل الخامس: النتائج والتوصيات

1.5 النتائج

يهدف هذا الفصل إلى عرض أهم النتائج التي تم التوصل إليها من خلال التحليلين الوصفي والاستدلالي، والتي توضح أثر إدارة المخاطر بأبعادها المختلفة على تطوير الأنظمة الأمنية المتكاملة في قطاع الطاقة بالمملكة العربية السعودية. وقد أظهرت النتائج ما يلي:

أظهرت النتائج أن المتوسط العام لمستوى ممارسة إدارة المخاطر في مؤسسات قطاع الطاقة بالمملكة العربية السعودية بلغ (4.23)، وهو مستوى مرتفع جدًا، وتدلل هذه النتيجة على أن المؤسسات العاملة في هذا القطاع تتبنى ثقافة مؤسسية متقدمة في إدارة المخاطر، وتحرص على دمج ممارساتها ضمن عمليات التخطيط والتنفيذ، ويُعزى هذا الارتفاع إلى الطبيعة الحساسة لقطاع الطاقة، إذ يُعد من القطاعات الحيوية والأكثر عرضة للمخاطر التشغيلية والأمنية، الأمر الذي فرض على المؤسسات اتباع نهج منهجي في تحليل المخاطر وتقييمها ومتابعتها، كما أسهم الإطار الوطني للأمن الصناعي والسياسات الحكومية في تعزيز الالتزام بالمعايير الدولية لإدارة المخاطر والحوكمة التشغيلية، وهو ما أدى إلى تحسين مستوى الممارسات الميدانية في المؤسسات العاملة بهذا القطاع.

بعد تحديد المخاطر

أظهرت النتائج أن متوسط بُعد تحديد المخاطر بلغ (4.18)، وهو ما يعكس وجود آليات مؤسسية فعالة للتعرف على مصادر الخطر المحتملة، وتُفسر هذه النتيجة بأن المؤسسات باتت تعتمد على أنظمة استشعار مبكر وقواعد بيانات تشغيلية تساعد على رصد التغيرات المفاجئة في البيئة الداخلية والخارجية. كما أن وجود فرق متخصصة في تحليل المخاطر التشغيلية والبيئية يدعم هذا الجانب، يُمكن أن يُعزى ارتفاع هذا البُعد إلى الخبرة التراكمية التي تمتلكها الشركات في التعامل مع المخاطر السابقة، ما ساعدها على بناء نظام معرفي مستدام لتحديد المخاطر الجديدة بشكل استباقي.

بعد تقييم المخاطر

بلغ متوسط بُعد تقييم المخاطر (4.26)، مما يعكس مستوى نضج مرتفع في عمليات التحليل والتقدير الكمي والنوعي للمخاطر، ويمكن تفسير هذه النتيجة بأن مؤسسات الطاقة السعودية تولي اهتمامًا خاصًا لتقدير احتمالية وقوع الخطر وشدة تأثيره على العمليات الأساسية، اعتمادًا على نماذج تحليل إحصائية وبرامج تقنية تدعم اتخاذ القرار، كما أن ارتباط قطاع الطاقة بمعايير السلامة التشغيلية العالمية، مثل ISO 31000 و ISO 45001، ساهم في تعزيز دقة التقييم وتوثيقه. ويُعزى هذا التميز أيضًا إلى إدراك المؤسسات أن ضعف تقييم المخاطر يؤدي إلى قرارات غير فعالة، مما جعلها تُخصص وحدات مهنية مزودة بخبراء لتحليل البيانات التشغيلية والتنبؤ بالسيناريوهات المستقبلية.

بعد معالجات واستجابات المخاطر

سجل هذا البعد أعلى متوسط بين الأبعاد الأربعة (4.34)، ما يشير إلى أن مؤسسات الطاقة تُظهر كفاءة عالية في صياغة وتنفيذ خطط الاستجابة للطوارئ، وتُفسر هذه النتيجة بأن المؤسسات تمتلك أنظمة تشغيلية احتياطية وخطط استمرارية أعمال تُمكنها من مواجهة الأزمات التشغيلية بسرعة. كما أن الدعم الإداري والمالي الموجه لإدارة المخاطر ساهم في تعزيز قدرتها على التفاعل الفوري مع التهديدات. ويُضاف إلى ذلك أن قطاع الطاقة في المملكة يتميز بوجود بنية تحتية تقنية متطورة وأنظمة مراقبة مركزية تساعد على الاستجابة الفعالة في الوقت الفعلي.

أظهرت نتائج تحليل الانحدار الخطي المتعدد وجود أثر دال إحصائيًا لإدارة المخاطر بأبعادها الأربعة على تطوير الأنظمة الأمنية المتكاملة، حيث بلغت قيمة معامل التحديد ($R^2 = 0.717$) بما يعني أن ما نسبته (71.7%) من التغير في مستوى تطوير الأنظمة الأمنية يمكن تفسيره من خلال تطبيق ممارسات إدارة المخاطر. كما أظهرت نتائج اختبار F (132.546) عند مستوى دلالة ($Sig. = 0.000$) معنوية النموذج الإحصائي. وتدل هذه النتائج على أن إدارة المخاطر تمثل عاملاً جوهريًا في تحقيق فاعلية واستدامة الأنظمة

الأمنية، إذ إن إدماج مراحل التحديد، والتقييم، والمعالجة، والمتابعة داخل منظومة العمل الأمني يسهم في بناء نظام وقائي متكامل يحمي البنية التحتية الحيوية من الانقطاعات أو التهديدات التشغيلية.

تتوافق هذه النتيجة مع ما توصل إليه Silva & Hammad (2025) في دراستهما حول مشاريع الطاقة في الشرق الأوسط، حيث أكدوا أن التكامل بين إدارة المخاطر والأمن التشغيلي يُعد من أهم عوامل الاستقرار المؤسسي. كما تتسق مع ما ذكره Gbabo et al. (2022) بأن إدراج ضوابط إدارة المخاطر في دورة حياة أنظمة الطاقة يعزز الحماية من الهجمات الإلكترونية والمخاطر التشغيلية في آن واحد. ويُعزى هذا الأثر الإيجابي في السياق السعودي إلى تبني المؤسسات لسياسات وطنية للأمن الصناعي والتحول الرقمي التي أوجدت بيئة تشريعية داعمة لتكامل إدارة المخاطر مع الأنظمة الأمنية.

❶ الفرضية الفرعية الأولى

“لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha \leq 0.05)$ لتحديد المخاطر على تطوير الأنظمة الأمنية المتكاملة”.

أظهرت نتائج تحليل الانحدار الخطي البسيط وجود أثر دال إحصائيًا لبُعد تحديد المخاطر على تطوير الأنظمة الأمنية المتكاملة، حيث بلغت قيمة $(B = 0.573)$ وقيمة $(T = 13.199)$ عند مستوى دلالة $(Sig. = 0.000)$. وتعني هذه النتيجة أن كل تحسن بمقدار وحدة واحدة في كفاءة تحديد المخاطر يؤدي إلى زيادة معنوية في فاعلية الأنظمة الأمنية. ويُفسر ذلك بأن المؤسسات التي تُجيد التعرف المبكر على مصادر الخطر تكون أكثر قدرة على تخطيط أنظمة أمنية استباقية قادرة على الاستجابة الفورية للتهديدات المحتملة.

تتفق هذه النتيجة مع ما أشار إليه Ispas et al. (2023) من أن وضوح مصادر الخطر يُعد شرطًا أساسيًا لبناء نظام إداري متكامل يعتمد على المرونة والاستجابة السريعة. كما تؤيدها نتائج دراسة Ezzat (2025) التي أكدت أن مؤسسات الطاقة السعودية التي تعتمد على التحليل الاستباقي للمخاطر تحقق

معدلات أعلى من الأمان التشغيلي. وبالتالي، يمكن القول إن تحديد المخاطر يُعد المرحلة التأسيسية لتطوير الأنظمة الأمنية المتكاملة، لأنه يمكن المؤسسة من تحليل بيئة التهديدات بدقة وتصميم حلول وقائية مبكرة.

❶ الفرضية الفرعية الثانية

“لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لتقييم المخاطر على تعزيز فعالية الأنظمة الأمنية”.

أظهرت نتائج التحليل الإحصائي وجود علاقة تأثير معنوية بين تقييم المخاطر وتطوير الأنظمة الأمنية المتكاملة، حيث بلغت قيمة $B = 0.546$ ، $T = 12.987$ ، $Sig. = 0.000$ وتدل هذه النتيجة على أن المؤسسات التي تعتمد على تقييم منهجي ودقيق للمخاطر تكون أكثر قدرة على تخصيص الموارد الأمنية وفق أولويات واقعية، مما يعزز كفاءة النظام الأمني ككل. ويُعزى هذا التأثير إلى أن عملية تقييم المخاطر تساعد في تحليل درجة احتمالية وقوع الخطر وتأثيره، ما يتيح للإدارة تصميم استراتيجيات أمنية قائمة على البيانات بدلاً من الافتراضات.

تتفق هذه النتيجة مع ما أشار إليه Settembre-Blundo et al. (2021) من أن المرونة المؤسسية في اتخاذ القرار خلال فترات عدم الاستقرار ترتبط ارتباطاً مباشراً بجودة تقييم المخاطر. كما يدعمها ما أورده Aziz & Andriansyah (2023) حول دور النماذج التحليلية القائمة على الذكاء الاصطناعي في تحسين دقة التقييم وتوجيه القرارات الأمنية نحو تحقيق الكفاءة التشغيلية. ومن ثم، فإن دقة التقييم لا تُسهم فقط في الحد من الخطر، بل تُعد أيضاً أداة استراتيجية لتخصيص الموارد وتعزيز فعالية الأمن المؤسسي.

❷ الفرضية الفرعية الثالثة

“لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لمعالجات واستجابات المخاطر على تحسين حماية البنية التحتية”.

أوضحت النتائج وجود أثر إيجابي قوي لبعء معالجات واستجابات المخاطر على تطوير الأنظمة الأمنية المتكاملة ($B = 0.592$) ، $T = 13.886$ ، $\text{Sig.} = 0.000$) وتدل هذه النتيجة على أن المؤسسات التي تمتلك خططاً واضحة ومحدثة للاستجابة للمخاطر تكون أكثر قدرة على حماية البنية التحتية الحيوية من الانقطاعات الأمنية والتشغيلية. ويُفسر ذلك بأن وجود آليات استجابة سريعة ومنسقة يُسهم في تقليل زمن التأثير وتقليل الخسائر التشغيلية، ويعزز مرونة الأنظمة في التعافي بعد الأزمات.

تتفق هذه النتيجة مع ما أورده Silva & Hammad (2025) في دراستهما عن مشاريع الطاقة الكبرى، حيث أكد الباحثان أن الاستجابة الفعالة للأزمات تُعد أحد أعمدة الحماية المتكاملة للبنى التحتية. كما تتسق مع ما طرحه Habbal et al. (2024) حول أهمية التكامل بين الذكاء الاصطناعي وإدارة الاستجابة في تحقيق أمان تشغيلي متقدم.

❶ الفرضية الفرعية الرابعة

“لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لمراقبة ومتابعة المخاطر على رفع كفاءة الأنظمة الأمنية المتكاملة”.

أظهرت النتائج وجود أثر دال إحصائياً لهذا البعد ($B = 0.515$) ، $T = 12.053$ ، $\text{Sig.} = 0.000$) ، مما يشير إلى أن أنشطة المراقبة والمتابعة المستمرة تمثل عنصراً محورياً في الحفاظ على فعالية الأنظمة الأمنية. ويُفسر هذا الأثر بأن المتابعة المنتظمة للمخاطر تتيح للإدارة اكتشاف الثغرات وتقييم مدى فاعلية إجراءات الحماية القائمة، مما يؤدي إلى تحسين الأنظمة بشكل مستمر. ويُعزى ذلك أيضاً إلى الدور الذي تلعبه التكنولوجيا في تسهيل جمع وتحليل البيانات الأمنية بشكل لحظي، مما يرفع من دقة الاستجابة وسرعتها.

تتسق هذه النتيجة مع ما أوضحه Lee (2020) في دراسته حول إدارة مخاطر إنترنت الأشياء، حيث أكد أن المراقبة اللحظية تشكل أحد أعمدة الأمن الوقائي الفعال. كما تدعمها دراسة Zografopoulos et al. (2021) التي أبرزت أهمية المتابعة المستمرة في تعزيز أمن الأنظمة السيبرانية والطاقة على حد سواء.

٢٠ بُعد مراقبة ومتابعة المخاطر

جاء هذا البُعد في المرتبة الأخيرة نسبيًا بمتوسط (4.12)، وهو مستوى مرتفع لكنه أقل من بقية الأبعاد. وتُشير هذه النتيجة إلى أن عمليات المراقبة والمتابعة لا تزال تواجه بعض التحديات في جانب التكامل الزمني بين جمع البيانات وتحليلها. ويُفسر هذا التراجع النسبي بكون عملية المراقبة تتطلب تكاليف تقنية عالية ونظم إنذار مبكر دقيقة، وهو ما قد لا يتوافر في جميع المؤسسات بالقدر نفسه. ومع ذلك، فإن استمرار المؤسسات في تطوير منصات رقمية للمراقبة يعكس اهتمامًا متزايدًا بتحسين هذا البعد. كما يمكن تفسير هذه النتيجة بأن بعض الشركات تركز على المعالجة الفورية بعد وقوع الخطر أكثر من المراقبة المستمرة قبل وقوعه، وهو ما يُضعف فعالية الإنذار المبكر نسبيًا.

2.5 التوصيات

استنادًا إلى نتائج الدراسة وتحليلها الإحصائي والنظري، يُوصي الباحث بمجموعة من التوصيات العملية والعلمية التي تستهدف تعزيز كفاءة إدارة المخاطر وتطوير الأنظمة الأمنية المتكاملة في مؤسسات قطاع الطاقة بالمملكة العربية السعودية، وذلك على النحو الآتي:

1. تبني إطار مؤسسي متكامل لإدارة المخاطر يربط بين الجوانب التشغيلية والتقنية والأمنية، بحيث تصبح إدارة المخاطر جزءًا أصليًا من دورة اتخاذ القرار في جميع الإدارات والمستويات الوظيفية.
2. تعزيز أنظمة المراقبة والمتابعة الأمنية من خلال توظيف تقنيات الذكاء الاصطناعي وإنترنت الأشياء (IoT) لتوفير إنذار مبكر بالمخاطر التشغيلية والاختراقات المحتملة، مما يقلل من زمن الاستجابة ويحسن من كفاءة الحماية.
3. تطوير برامج تدريب احترافية للكوادر الأمنية والفنية لرفع الوعي بإدارة المخاطر وتعزيز القدرات الاستباقية في تحليل الأحداث الأمنية، بما يتوافق مع المعايير الدولية مثل ISO 31000 و ISO 27001.
4. تحديث خطط الطوارئ والاستجابة للأزمات بشكل دوري بما يراعي طبيعة المخاطر المتغيرة في بيئة الطاقة، مع اختبار جاهزية الفرق التشغيلية من خلال سيناريوهات محاكاة واقعية.

5. تعزيز التكامل بين الإدارات التقنية والأمنية والإدارية من خلال إنشاء لجان دائمة لإدارة المخاطر، تضمن التفاعل الفوري بين وحدات اتخاذ القرار والأنظمة التقنية.
6. إدخال مؤشرات أداء (KPIs) لقياس فاعلية إدارة المخاطر، بحيث يتم تقييم كفاءة الاستراتيجيات الأمنية والتشغيلية بانتظام، مما يتيح التحسين المستمر والتعلم التنظيمي.
7. إنشاء مركز وطني لتكامل إدارة المخاطر والأمن الصناعي خاص بقطاع الطاقة، يتولى جمع وتحليل البيانات الأمنية وتشخيص أنماط التهديدات التشغيلية على المستوى الوطني.
8. توحيد السياسات والإجراءات التنظيمية للأمن الصناعي من خلال إصدار دليل وطني لإدارة المخاطر في البنية التحتية للطاقة، بما يتسق مع المعايير الدولية وأفضل الممارسات الإقليمية.
9. دعم التحول الرقمي في إدارة المخاطر عبر تمويل مشروعات الذكاء الاصطناعي والتحليلات التنبؤية، لتمكين مؤسسات الطاقة من بناء أنظمة أمنية ذاتية التعلم.
10. إطلاق برامج وطنية للتوعية الأمنية والتدريب القطاعي تستهدف العاملين في شركات الطاقة، لتطوير ثقافة أمنية تشاركية قائمة على الوعي والمسؤولية الجماعية تجاه حماية الأصول الوطنية.
11. إجراء دراسات مستقبلية حول العلاقة بين إدارة المخاطر والأمن السيبراني في قطاع الطاقة، خصوصاً في ظل التحول إلى الأنظمة الذكية والطاقة المتجددة، بهدف بناء نماذج تنبؤية جديدة للتهديدات.
12. اقتراح تطوير نموذج عربي موحد لإدارة المخاطر في القطاعات الحيوية يستند إلى خصوصية البيئة الخليجية، ويجمع بين الأساليب الكمية والتحليل السلوكي للمخاطر التشغيلية والأمنية.

Abstract

This study aimed to analyze the impact of risk management, with its four dimensions (risk identification, risk assessment, risk treatment and response, and risk monitoring and follow-up), on the development of integrated security systems for protecting the energy sector's infrastructure in the Kingdom of Saudi Arabia. The study adopted the descriptive-analytical method as it is appropriate for the nature of the topic, and employed a questionnaire to collect data from a sample of 320 employees working in security and technical departments within Saudi energy institutions. Data were analyzed using the SPSS statistical software package.

The results revealed that the level of risk management practices in energy institutions was high, with an average mean score of (4.23). Furthermore, the findings indicated a statistically significant impact of the four risk management dimensions on the development of integrated security systems ($R^2 = 0.717$, $F = 132.546$, $\text{Sig.} = 0.000$). Among these dimensions, risk treatment and response showed the strongest effect, followed by risk assessment, risk identification, and finally risk monitoring and follow-up.

The study recommended establishing a National Center for Risk Management and Industrial Security Integration within the energy sector, and adopting a unified institutional framework that combines risk management and technological security. It also emphasized the importance of enhancing the use of artificial intelligence and predictive monitoring technologies in risk analysis and follow-up, in addition to supporting continuous training programs for personnel in security and technical fields to ensure preparedness and effective response to future crises.

Keywords: Risk Management, Integrated Security Systems, Infrastructure Protection, Energy Sector, Kingdom of Saudi Arabia.

قائمة المراجع

المراجع باللغة العربية

1. إبراهيم، ابراهيم اسماعيل، و خليل، فرقد زهير. (2021). إدارة مخاطر منح الائتمان المصرفي. مجلة المحقق الحلي للعلوم القانونية والسياسية، مج13، ع3 ، 9 - 71. مسترجع من <http://search.mandumah.com/Record/1176200>
2. البابلي، عمار ياسر محمد زهير. (2021). دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة. مجلة الأمن والقانون، مج29، ع1 ، 124 - 213. مسترجع من <http://search.mandumah.com/Record/1131190>
3. باقر، وفاء جاسم علي عباس، ارتيمة، هاني جزاع عبدالكريم، و الهواري، سامر فواز. (2020). أثر إدارة المخاطر في إدارة المشاريع الهندسية: الدور الوسيط للثقافة المنظمة في الهيئة العامة للطرق والنقل البري في دولة الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من <http://search.mandumah.com/Record/1219633>
4. البقي، سعد، و شرقي، فاطنة. (2025). دور اليقظة الاستراتيجية في إدارة المخاطر: دراسة حالة أزمة كوفيد بالمملكة العربية السعودية. مجلة الرسالة للدراسات والبحوث الإنسانية، مج10، ع1 ، 927 - 936. مسترجع من <http://search.mandumah.com/Record/1567945>
5. بوزيان، فتيحة، و سلماني، هناء. (2024). إشكالية تطوير أنظمة الدفع الإلكتروني في الجزائر كمدخل للتجارة الإلكترونية. مجلة البحوث في العلوم المالية والمحاسبية، مج9، ع1 ، 19 - 33. مسترجع من <http://search.mandumah.com/Record/1519581>
6. ثوبي، عائدة، و غجاني، إبتسام. (2022). دور التدقيق الداخلي في إدارة المخاطر: دراسة ميدانية في المؤسسة المينائية لولاية سكيكدة. مجلة أرصاد للدراسات الاقتصادية والإدارية، مج5، ع1 ، 115 - 130. مسترجع من <http://search.mandumah.com/Record/1313032>

7. الجازي، مرام صالح محمد. (2022). تطوير أنظمة حماية الكمبيوتر في المؤسسات الحكومية. مجلة

رماج للبحوث والدراسات، ع73 ، 167 - 180. مسترجع من

<http://search.mandumah.com/Record/1329284>

8. حجاج، مراد، و بن عياش، سمير. (2024). الحد من مخاطر الكوارث: مواكبة التجارب الدولية. المجلة

الجزائرية للحقوق والعلوم السياسية، مج9، ع1 ، 1157 - 1178. مسترجع من

<http://search.mandumah.com/Record/1484113>

9. الحسني، عبدالله بن حمود بن محمد، و الخشالي، شاكِر جَار الله محمود. (2022). أثر التفكير

الاستراتيجي في إدارة المخاطر: الدور المعدل للدعم المنظمي في شركات المقاولات العمانية (رسالة

دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من

<http://search.mandumah.com/Record/1264921>

10. الرواشدة، ينال عاطف سلام، و الشورة، عبدالله أحمد سليمان. (2022). أثر إدارة المخاطر في مرونة

سلسلة التوريد: الدور المعدل للتمكين في شركة البوتاس العربية (رسالة دكتوراه غير منشورة).

جامعة العلوم الإسلامية العالمية، عمان. مسترجع من

<http://search.mandumah.com/Record/1329066>

11. الطبال، غيث المبروك. (2025). دور المحاسب الإداري في إدارة المخاطر. مجلة العلوم الاقتصادية

والسياسية، مج22، ع1 ، 88 - 115. مسترجع من

<http://search.mandumah.com/Record/1560663>

12. علوان، حميد جاسم. (2021). دور إدارة المخاطر في تقليل الخسائر في المنظمات. مجلة كلية الإدارة

والاقتصاد للدراسات الاقتصادية والإدارية والمالية، مج13، ع2 ، 300 - 318. مسترجع من

<http://search.mandumah.com/Record/1263556>

13. الغراوي، حيدر جبوري شمخي، و الشريدة، ندى عبدالقادر عبدالستار. (2025). دور إدارة المخاطر

في تحقيق الجودة الشاملة: دراسة استطلاعية في شركة نفط البصرة. مجلة الأقتصادي الخليجي،

ع65 ، 144 - 190. مسترجع من <http://search.mandumah.com/Record/1616289>

14. المناور، فيصل، و العليان، منى. (2021). إدارة المخاطر الإجتماعية: التخطيط وسبل المواجهة. جسر

التنمية، ع154 ، 1 - 23. مسترجع من <http://search.mandumah.com/Record/1142784>

15. النحاس، أحمد حمدي، و دبا، ندى طارق. (2022). إدارة مخاطر التحول الرقمي. المجلة العلمية

للدراستات والبحوث المالية والإدارية، مج13، ملحق ، 1501 - 1513. مسترجع من

<http://search.mandumah.com/Record/1292003>

16. نصر الدين، قارة عشيرة، و حبار، عبدالرزاق. (2020). إدارة مخاطر الائتمان باستخدام: الحوكمة،

معيار كفاية رأس المال، التوريق، المشتقات الائتمانية. مجلة الريادة لاقتصاديات الأعمال، مج6، ع2

، 344 - 362. مسترجع من <http://search.mandumah.com/Record/1035401>

المراجع باللغة الإنجليزية

1. Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110-132
2. Chen, Y., Zheng, W., Li, W., & Huang, Y. (2021). Large group activity security risk assessment and risk early warning based on random forest algorithm. *Pattern Recognition Letters*, 144, 1-5.
3. Ezzat, A. M. (2025). Extending and Improving Current Frameworks for Risk Management and Decision Making: Incorporating Dynamic Aspects of Risk and Uncertainty in Saudi Arabia. *International Journal of Research and Innovation in Social Science*, IX(XIV), 1844–1851. <https://doi.org/10.47772/ijriss.2025.914mg00139>

4. Gbabo, E. Y., Okenwa, O. K., & Chima, P. E. (2022). *Framework for Integrating Cybersecurity Risk Controls into Energy System Implementation Lifecycles*. 3(1), 365–371. <https://doi.org/10.54660/.jfmr.2022.3.1.365-371>
5. Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, 240, 122442.
6. Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, 240, 122442.
7. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 24(2), 393-414
8. Ispas, L., Mironeasa, C., & Silvestri, A. (2023). Risk-based approach in the implementation of integrated management systems: a systematic literature review. *Sustainability*, 15(13), 10251
9. Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future internet*, 12(9), 157.
10. Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. *Global Journal of Flexible Systems Management*, 22(Suppl 2), 107-132.
11. Silva, P., & Hammad, A. (2025). *Integrated Risk Management Framework for Large-Scale Energy Projects: A Case Study from the Middle East*. <https://doi.org/10.2118/226888-ms>

12. Wei, L., Lv, Z., Peng, D., & Qi, E. (n.d.). *Integrated Energy Systems Security Assessment Based on Belief Rule Base Model*. <https://doi.org/10.1109/icpre52634.2021.9635568>
13. Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEe Access*, 9, 29775-29818.

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس دور إدارة المخاطر في تطوير الأنظمة الأمنية المتكاملة

لحماية البنية التحتية لقطاع الطاقة بالمملكة العربية السعودية

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول

منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم

بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن

جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا

البحث، وسوف أزدكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

1- النوع الاجتماعي ☐ ذكر ☐ أنثى

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

☐ من 40 – 50 سنة ☐ من 50 سنة فأكثر

3- المؤهل العلمي ☐ بكالوريوس ☐ دراسات عليا

☐ دبلوم فأقل

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

☐ من 10 – 15 سنة ☐ أكثر من 15 سنة

5- المسمى الوظيفي ☐ مدير إدارة أو رئيس قسم ☐ مهندس تشغيل وتحكم

☐ مختص أمن معلومات/سيبراني ☐ محلل مخاطر أو باحث أمني

☐ موظف إشرافي آخر

ثانيا محاور الاستبيان

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

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
تحديد المخاطر					
					تعمل المؤسسة على تحديد مصادر الخطر بشكل دوري قبل تنفيذ الأنشطة التشغيلية.
					تعتمد المؤسسة على أساليب تحليلية ومنهجية في تحديد المخاطر المحتملة.
					يتم إشراك الإدارات المختلفة في عملية تحديد المخاطر.
					تمتلك المؤسسة قاعدة بيانات محدثة لتوثيق أنواع المخاطر السابقة.
تقييم المخاطر					
					تُجري المؤسسة تقييمًا منتظمًا لاحتمالية حدوث المخاطر وتأثيرها.
					تستخدم المؤسسة أدوات كمية ونوعية لتقدير شدة المخاطر.
					يتم ترتيب المخاطر حسب أولويتها وتأثيرها المحتمل على العمليات.
					تعتمد المؤسسة على فرق عمل مختصة لتقييم المخاطر.

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
معالجة واستجابة المخاطر					
					تمتلك المؤسسة خطط استجابة واضحة ومكتوبة لمختلف أنواع المخاطر.
					يتم تفعيل إجراءات الطوارئ فور رصد أي خطر يهدد سلامة الأنظمة.
					تُجرى تدريبات ومحاكاة دورية للتعامل مع الحالات الطارئة.
					تُراجع خطط المعالجة بصفة دورية لتحديثها وتحسينها.
مراقبة ومتابعة المخاطر					
					تُجرى عمليات مراقبة دورية لرصد مؤشرات المخاطر المحتملة.
					يتم إعداد تقارير دورية لتوثيق مستوى المخاطر والإجراءات المتخذة.
					تعتمد المؤسسة على نظم إنذار مبكر للكشف عن المخاطر المستجدة.
					تُستخدم نتائج المتابعة لتطوير خطط إدارة المخاطر.

✿ المحور الثاني: تطوير الأنظمة الأمنية المتكاملة، ضع إشارة (✓) في المربع المناسب

لاختيارك:

المعارض بشدة	معارض	محايد	أو وافق بشدة	البعد
				تعتمد المؤسسة على بنية تقنية متطورة تدعم الأنظمة الأمنية التشغيلية.
				يوجد تكامل فعال بين الأنظمة الأمنية المختلفة داخل المؤسسة.
				الأنظمة الأمنية جاهزة للتعامل مع الحوادث والأزمات الأمنية المفاجئة.
				تستجيب الأنظمة بسرعة لأي تهديدات أو محاولات اختراق.
				تستخدم المؤسسة تقنيات الذكاء الاصطناعي لتحليل البيانات الأمنية.
				يتم تكامل البيانات الأمنية بين الأقسام المختلفة لتحسين الاستجابة.
				تُحدَّث الإجراءات الأمنية بشكل دوري بما يتلاءم مع المتغيرات.
				تمتلك المؤسسة كوادر بشرية مؤهلة لإدارة وتشغيل الأنظمة الأمنية.
				تلتزم المؤسسة بالمعايير الأمنية الدولية ومتطلبات الحوكمة.

معارض بشدة	معارض	محايد	أوافق	أوافق بشدة	البعد
					تحظى عمليات تطوير الأنظمة الأمنية بدعم مباشر من الإدارة العليا.

مع خالص التقدير والاحترام

Mid Ocean University

College of Management

Master of Risk Management



**Risk Management's Role in Developing Integrated Security
Systems to Protect the Energy Sector Infrastructure in the
Kingdom of Saudi Arabia**

Prepared by:

Abdulsalam Amer Almisfer

251002791

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

Dr. Fayez Jarad

1447-2025