

عنوان البحث

دور إدارة المخاطر في تعزيز الأمن السيبراني في الجامعات السعودية: دراسة حالة جامعة
الملك سعود بن عبدالعزيز للعلوم الصحية

إعداد:

الطالبة/ روى عبد العزيز المزيد
الرقم الأكاديمي/ ٢٥٢٠٠١١٥٦

إشراف:

الدكتور/ فايز علي جراد

الدكتور/ الفيصّل عبد الحميد محمد

العام الدراسي:

٢٠٢٦م / ١٤٤٧هـ



حقوق الطباعة

جميع حقوق الطباعة والنشر محفوظة لجامعة ميدأوشن حيث تُعدّ جميع المواد والمحتويات الواردة في هذا البحث هي ملك للجامعة، ولا يجوز استخدامها أو إعادة نشرها أو توزيعها بأي وسيلة كانت دون الحصول على إذن مسبق من جامعة ميدأوشن.

إِهْدَاء

أهدي هذا العمل إلى من كان لهم الأثر الأكبر في هذه الرحلة

إلى أُمِّي الغالية مصدر الحنان والدعاء التي كانت سندي في كل خطوة فكان لدعائها الأثر
الأكبر في توفيقِي

إلى أبي العزيز الذي غرس في نفسي قيم الجد والاجتهاد وكان قدوتي في الصبر والمثابرة

إلى إخوتي وأخواتي الذين كانوا دائماً مصدر دعمٍ وتشجيعٍ خلال هذه الرحلة

إلى كل من كان له أثر ولو بكلمة طيبة أو دعوة صادقة وأسهم في دعمي ومساندتي خلال هذه
المسيرة

إلى كل من آمن بقدرتي على الوصول وكان دافعاً لي لأحقق هذا الإنجاز

سائلةً الله أن يجعله خالصاً لوجهه الكريم وأن يكتب فيه النفع والفائدة وأن يكون بدايةً لمزيد من

النجاحات والتقدم في مسيرتي العلمية والعملية

شكر وتقدير

أتقدم بخالص الشكر وعظيم الامتنان إلى الله عز وجل، الذي وفقني وأعانني على إتمام هذا البحث، وأسأله سبحانه أن يجعله خالصاً لوجهه الكريم.

ثم أتوجه بجزيل الشكر والتقدير إلى والديّ العزيزين، اللذين كانا لي السند والداعم الأول في مسيرتي العلمية، فقد كان لتشجيعهما ودعمهما المستمر الأثر البالغ في تحفيزي ومواصلة هذا العمل. إلى والدتي الغالية، التي لم تبخل عليّ يوماً بدعائها ومحبتها وتشجيعها، وإلى والدي العزيز، الذي علّمني معنى الاجتهاد والمثابرة، فلهما مني أسمى آيات الشكر والامتنان.

كما أعبر عن عميق امتناني لجامعة ميدأوشن، لما وفرتة من بيئة أكاديمية داعمة، وما قدمته من موارد وتسهيلات كان لها دور أساسي في إنجاز هذا البحث وتحقيق أهدافه.

وأعرب عن بالغ شكري وتقديري لمشرفي البحث د. الفیصل عبد الحمید محمد ، و د. فايز علي جراد الذين قدموا لي علمهم وتوجيههم ونصحهم، وكانوا خير عون ومرشد خلال مراحل إعداد هذا البحث.

وأتوجه بالشكر لكل من قدّم لي الدعم والمساندة، سواء بالنصح أو التشجيع ، وكان لهم أثرٌ مباشر في إنجاز هذا البحث، سائلاً الله عز وجل أن يجزي الجميع خير الجزاء ، وأن يجعل هذا البحث خطوةً نحو مزيد من النجاح والتقدم.

المستخلص

هدفت هذه الدراسة إلى تحليل دور ممارسات إدارة المخاطر في تعزيز فاعلية الأمن السيبراني في الجامعات السعودية، مع تطبيق الدراسة على جامعة الملك سعود بن عبدالعزيز للعلوم الصحية كنموذج تطبيقي وركزت الدراسة على تحليل العلاقة بين ممارسات إدارة المخاطر وعدد من الأبعاد المرتبطة بفاعلية الأمن السيبراني، وهي: التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني، والتحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني، وفاعلية الإطار التنظيمي والسياسات والإجراءات، إضافة إلى تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني.

اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة أداة رئيسة لجمع البيانات من عينة الدراسة، كما تم استخدام المتوسطات الحسابية والانحرافات المعيارية لتحليل محاور الدراسة، ومعامل ارتباط بيرسون لاختبار فرضياتها.

أظهرت نتائج الدراسة أن مستوى ممارسات إدارة المخاطر وفاعلية الأمن السيبراني في الجامعة جاء بدرجة مرتفعة جداً كما بينت النتائج وجود علاقة ارتباط إيجابية ذات دلالة إحصائية بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني بالإضافة إلى وجود علاقات ارتباط إيجابية ذات دلالة إحصائية بين ممارسات إدارة المخاطر وكل من التكامل المؤسسي، والتحديات التنظيمية والتقنية، وفاعلية الإطار التنظيمي والسياسات والإجراءات، وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني.

وأشارت النتائج إلى أن تعزيز ممارسات إدارة المخاطر يساهم في دعم التكامل المؤسسي، وتحسين السياسات والإجراءات التنظيمية، وتعزيز الوعي السيبراني لدى العاملين بما يساهم في رفع مستوى الحماية الرقمية داخل المؤسسات التعليمية.

وفي ضوء النتائج، أوصت الدراسة بضرورة تعزيز التكامل المؤسسي بين إدارة المخاطر ووحدات الأمن السيبراني وتقنية المعلومات، وتطوير برامج التدريب والتوعية السيبرانية، واستقطاب الكوادر البشرية المتخصصة، إضافة إلى تحديث السياسات والإجراءات التنظيمية بما يتوافق مع المعايير الوطنية والدولية للأمن السيبراني.

الكلمات المفتاحية: إدارة المخاطر، الأمن السيبراني، التكامل المؤسسي، الحوكمة، الجامعات السعودية.

فهرس المحتويات

أ	بسم الله الرحمن الرحيم
ب	حقوق الطباعة
ت	إهداء
ث	شكر وتقدير
ج	المستخلص
ح	فهرس المحتويات
ذ	قائمة الجداول
ز	فهرس الاشكال
1	الفصل الأول : الإطار العام للبحث
2	المقدمة
4	مشكلة البحث
5	أهمية الدراسة
5	أولاً: الأهمية العلمية
5	ثانياً: الأهمية العملية
7	أهداف الدراسة
7	تساؤلات الدراسة
7	سؤال البحث الرئيسي
7	أسئلة البحث الفرعية
8	فرضيات الدراسة
8	الفرضية الرئيسية
8	الفرضيات الفرعية
9	النظرية العلمية المتبعة لإعداد البحث
9	خاتمة الفصل
10	الفصل الثاني: الدراسات السابقة والإطار النظري

11	مقدمة
11	نموذج الدراسة
13	الدراسات السابقة
21	أوجه الشبه بين الدراسات السابقة
21	أوجه الاختلاف بين الدراسات السابقة
22	الفجوة البحثية
22	أوجه الاستفادة من الدراسات السابقة
23	ما يميز هذه الدراسة عن الدراسات السابقة
24	الإطار النظري للدراسة
29	خاتمة الفصل
30	الفصل الثالث: منهجية الدراسة
31	مقدمة
31	تصميم البحث
32	مجتمع البحث
32	محددات حجم عينة الدراسة
33	خصائص العينة
40	مصادر البيانات
40	أداة جمع البيانات
42	حدود الدراسة
43	الصدق والثبات لاستبانة الدراسة (أداة الدراسة)
46	الأداة المستخدمة للتحليل الإحصائي
47	خاتمة الفصل
48	الفصل الرابع: النتائج والتوصيات
49	مقدمة
49	تحليل البيانات
50	المحور الأول: ممارسات إدارة المخاطر المؤسسية
52	المحور الثاني: فاعلية الأمن السيبراني

53.....	المحور الثالث: التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني
55.....	المحور الرابع: التحديات التنظيمية والتقنية
56.....	المحور الخامس: الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر
57.....	المحور السادس: تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني
59.....	اختبار فرضيات الدراسة
64.....	النتائج
64.....	أولاً : نتائج الدراسة
65.....	ثانياً: نتائج الدراسة ومناقشتها مع نتائج الدراسات السابقة
68.....	التوصيات
69.....	المقترحات
70.....	خاتمة الفصل
71.....	المراجع
72.....	المراجع العربية
74.....	المراجع الأجنبية
76.....	الملاحق
77.....	الاستبانة
84.....	Abstract
85.....	The Title

قائمة الجداول

رقم الصفحة	اسم الجدول
33	جدول رقم (3-1) العينة المستهدفة والخاضعة للتحليل
33	جدول رقم (3-2) خصائص العينة حسب الجنس
34	جدول رقم (3-3) خصائص عينة الدراسة حسب المستوى التعليمي
35	جدول رقم (3-4) خصائص عينة الدراسة حسب المسمى الوظيفي
37	جدول رقم (3-5) خصائص عينة الدراسة حسب عدد سنوات الخبرة
38	جدول رقم (3-6) خصائص عينة الدراسة حسب المدينة الجامعية
39	جدول رقم (3-7) خصائص عينة الدراسة حسب مدى ارتباط العمل بالأنظمة التقنية
44	الجدول رقم (3-8) صدق الاتساق الداخلي لأداة الدراسة
45	جدول رقم (3-9): معامل الثبات ألفا كرونباخ لمحاو الاستبانة ولأداة ككل
50	جدول رقم (4-1): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير ممارسات إدارة المخاطر المؤسسية
52	جدول رقم (4-2): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير فاعلية الأمن السيبراني
53	جدول رقم (4-3): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني
55	جدول رقم (4-4): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير التحديات التنظيمية والتقنية

56	جدول رقم (4-5): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر
57	جدول رقم (4-6): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني
59	جدول رقم (4-7) اختبار معامل ارتباط بيرسون للفرضية الرئيسية
60	جدول رقم (4-8): اختبار معامل ارتباط بيرسون للفرضية الفرعية الأولى
61	جدول رقم (4-9): اختبار معامل ارتباط بيرسون للفرضية الفرعية الثانية
62	جدول رقم (4-10): اختبار معامل ارتباط بيرسون للفرضية الفرعية الثالثة
63	جدول رقم (4-11): اختبار معامل ارتباط بيرسون للفرضية الفرعية الرابعة

فهرس الأشكال

رقم الصفحة	اسم الشكل
12	شكل رقم (1-1) متغيرات الدراسة
34	شكل رقم (2-3) خصائص العينة حسب الجنس
35	الشكل رقم (3-3) خصائص العينة حسب المستوى التعليمي
36	شكل رقم (4-3) خصائص العينة حسب المسمى الوظيفي
37	شكل رقم (5-3) خصائص العينة حسب عدد سنوات الخبرة
38	شكل رقم (6-3) خصائص العينة حسب المدينة الجامعية
39	شكل رقم (7-3) خصائص العينة حسب مدى ارتباط العمل بالأنظمة التقنية

الفصل الأول

الإطار العام للبحث

المقدمة:

يشهد قطاع التعليم العالي في المملكة العربية السعودية تحولاً رقمياً متسارعاً تماشياً مع مستهدفات رؤية السعودية (2030) في مختلف مجالاته الأكاديمية والإدارية، حيث تبنت الجامعات العديد من الأنظمة التقنية الحديثة شملت أنظمة القبول والتسجيل، والتعليم الإلكتروني، وإدارة البحوث، والموارد الأكاديمية. مما أسهم هذا التحول في تحسين الكفاءة التشغيلية وجودة الخدمات التعليمية ، إلا أنه في المقابل زاد من حجم التهديدات والمخاطر السيبرانية نتيجة الاعتماد المتزايد على الأنظمة التقنية وشبكات الاتصال الرقمية الحديثة (المنيع، 2022).

وتُعد الجامعات السعودية من أكثر المؤسسات تعرضاً للمخاطر الإلكترونية نظراً لاعتمادها الكبير على الأنظمة التقنية في إدارة عملياتها الأكاديمية والإدارية، مما يتطلب تطوير سياسات فعالة لحماية البيانات والمعلومات وضمان استمرارية الخدمات الرقمية (البوشي، 2022) وتشمل هذه المخاطر محاولات الاختراق الإلكتروني، وتسريب البيانات الأكاديمية والبحثية، وتعطيل الخدمات الإلكترونية الحيوية، مما يجعل الأمن السيبراني أحد أبرز أولويات مؤسسات التعليم العالي في المرحلة الراهنة.

كما أن ضعف التنسيق بين الإدارات الفنية والإدارية داخل مؤسسات التعليم العالي يُعد من أبرز التحديات التي تحدّ من كفاءة تطبيق ممارسات الأمن السيبراني والاستجابة للحوادث الرقمية، الأمر الذي يستدعي تعزيز التكامل المؤسسي بين إدارة المخاطر ووحدات الأمن السيبراني لتحقيق حماية فعالة للأصول المعلوماتية (السميري، 2022).

وفي ظل هذا الواقع، تبرز إدارة المخاطر بوصفها عملية منهجية ومنسقة تهدف إلى توجيه وضبط المنظمة فيما يتعلق بالمخاطر المحتملة، من خلال تحديدها وتحليلها وتقييمها ووضع خطط استجابة ومراقبة فعالة للحد من آثارها السلبية على تحقيق الأهداف المؤسسية . وكما يُعرّف معيار (ISO 31000) إدارة المخاطر بأنها "الأنشطة المنسقة لتوجيه المنظمة والسيطرة عليها فيما يتعلق بالمخاطر، مؤكداً على أهمية دمج إدارة المخاطر ضمن نظام الحوكمة المؤسسية وعمليات القيادة والتخطيط وصنع القرار، لما لذلك من دور في تعزيز الكفاءة المؤسسية وضمان استمرارية الأعمال وتحقيق الأهداف التنظيمية. كما تُعد إدارة المخاطر المؤسسية ركيزة أساسية في نظام الحوكمة الحديثة وفقاً لإطار (COSO,ERM) الذي يؤكد على دمج ممارسات إدارة المخاطر ضمن عملية صياغة الاستراتيجيات وتحسين الأداء المؤسسي، بما يسهم في تعزيز القدرة على اتخاذ القرارات الاستباقية وتحقيق القيمة المستدامة في مواجهة التحديات المختلفة (ISO 31000, 2018; COSO, 2017).

أما الأمن السيبراني، فيُعرّف بأنه حماية الشبكات وأنظمة تقنية المعلومات والتقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع، ويشمل مفهومه أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك. (تنظيم الهيئة الوطنية للأمن السيبراني، 2017) كما يشمل مجموعة من السياسات والإجراءات والضوابط التقنية والتنظيمية التي تهدف إلى حماية الأنظمة والشبكات والمعلومات من أي تهديد أو استخدام غير مصرح به، بما يضمن سرية البيانات وسلامتها وتوافرها. وتؤكد الأطر والسياسات الوطنية في المملكة على أهمية التكامل بين إدارة المخاطر والأمن السيبراني لتحقيق الحماية الشاملة للأصول الرقمية وضمان استدامة الخدمات.

وفي هذا السياق، أولت جامعة الملك سعود بن عبد العزيز للعلوم الصحية اهتماماً كبيراً بتطبيق مبادئ إدارة المخاطر وتعزيز الأمن السيبراني من خلال تبني سياسة إدارة مخاطر الأمن السيبراني (2025)، التي تهدف إلى وضع إطار مؤسسي متكاملًا لتحديد وتحليل المخاطر ومعالجتها بما يتوافق مع المعايير الوطنية الصادرة عن الهيئة الوطنية للأمن السيبراني (NCA) ، وتهدف هذه السياسة إلى ضمان استمرارية الأعمال وحماية البنية التحتية الرقمية للجامعة من خلال تحديد الأدوار والمسؤوليات وتوحيد منهجية تقييم المخاطر، كما تنص على ضرورة مواءمة ممارسات إدارة المخاطر السيبرانية مع إدارة المخاطر المؤسسية (ERM) بما يتوافق مع الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة عن الهيئة الوطنية للأمن السيبراني، والضوابط المكملة مثل ضوابط البيانات (DCC-1:2022) ، والضوابط الأمنية للعمل عن بُعد (TCC-1:2021) ، والضوابط الأمنية لحسابات وسائل التواصل الاجتماعي الخاصة بالمنظمات (OSMACC-1:2021) ، والضوابط الأمنية للحوسبة السحابية (CCC-1:2020) ، والضوابط الأمنية للأنظمة الحساسة (CSCC-1:2019) .

ويُعد هذا التوجّه نموذجًا تطبيقيًا يمكن الاستفادة منه في تحليل العلاقة بين إدارة المخاطر والأمن السيبراني في مؤسسات التعليم العالي السعودية، مع التركيز على تجربة جامعة الملك سعود بن عبد العزيز للعلوم الصحية كنموذج تطبيقي يهدف إلى تقييم مستوى التكامل بين إدارة المخاطر والسياسات السيبرانية، واستكشاف سبل تطويرها بما يحقق حماية فعّالة للمعلومات واستدامة العمليات الأكاديمية، والإدارية في البيئة الجامعية الرقمية.

مشكلة الدراسة :

في ظل التطورات الكبيرة التي شهدتها قطاع التعليم العالي في المملكة العربية السعودية في مجال التحول الرقمي وتطوير بنيته التقنية، وما رافق ذلك من توسع في استخدام الأنظمة التقنية في العمليات الأكاديمية والإدارية والبحثية برزت تحديات متزايدة تتعلق بالمخاطر السيبرانية نتيجة الاعتماد الكبير على الأنظمة الرقمية وتبادل البيانات عبر شبكات الاتصال والبنى التحتية المتصلة بالإنترنت وقد جعل هذا الواقع الجامعات أكثر عرضةً للتهديدات والهجمات السيبرانية التي قد تمس سلامة المعلومات واستمرارية الخدمات التعليمية.

ورغم تبني الدولة والجامعات لسياسات وطنية تُعنى بالأمن السيبراني وإدارة المخاطر فإن الواقع العملي لا يزال يشهد فجوات واضحة في مستوى التكامل بين هذين المجالين داخل مؤسسات التعليم العالي إذ تتعامل العديد من الجامعات مع إدارة المخاطر والأمن السيبراني باعتبارهما نظامين منفصلين؛ أحدهما إداري والآخر تقني مما يحد من فاعلية المنظومة المؤسسية في الوقاية من التهديدات الرقمية أو الاستجابة لها بشكل متكامل. كما يبرز قصور في تطبيق مبادئ إدارة المخاطر ضمن الإطار السيبراني سواء من حيث آليات التقييم والمتابعة أو وضوح الأدوار والمسؤوليات بين الإدارات الفنية والإدارية.

وتشير الأدبيات الحديثة إلى أن تحديات الوعي السيبراني والتدريب المهني ما زالت قائمة لدى بعض منسوبي الجامعات إلى جانب محدودية الربط بين سياسات الحوكمة العامة وضوابط الأمن السيبراني في الممارسات اليومية. وتتضاعف هذه التحديات في ظل التوسع في الخدمات الإلكترونية والتعليم عن بُعد مما يجعل البيئة الجامعية أكثر تعقيداً من الناحية التقنية والتنظيمية ويؤكد الحاجة إلى إطار تكاملي شامل لإدارة المخاطر السيبرانية يضمن استدامة العمليات الأكاديمية ويحافظ على الأصول المعلوماتية الحيوية.

من هنا، تتمثل مشكلة هذه الدراسة في تحليل دور إدارة المخاطر في تعزيز الأمن السيبراني في الجامعات السعودية من خلال تقييم مستوى التكامل بين السياسات والإجراءات التنظيمية والتقنية المطبقة ومدى فاعلية هذا الدور في حماية البنية الرقمية وضمان استمرارية الخدمات الأكاديمية مع التركيز على جامعة الملك سعود بن عبد العزيز للعلوم الصحية كنموذج تطبيقي يمكن أن يُسهم في بناء إطار مؤسسي وطني متكامل لإدارة المخاطر السيبرانية في مؤسسات التعليم العالي بما يتوافق مع الهيئة الوطنية للأمن السيبراني (NCA) .

أهمية الدراسة :

تتبع أهمية هذه الدراسة من الحاجة المتزايدة إلى فهم العلاقة بين إدارة المخاطر والأمن السيبراني داخل الجامعات السعودية، في ظل التحول الرقمي المتسارع الذي تشهده مؤسسات التعليم العالي، فمع تزايد الاعتماد على الأنظمة التقنية والمنصات الإلكترونية في إدارة العمليات الأكاديمية والإدارية أصبحت حماية المعلومات وضمان استمرارية الخدمات من أبرز التحديات التي تتطلب تكاملاً فعالاً بين الجوانب الإدارية والفنية.

أولاً: الأهمية العلمية:

تكتسب هذه الدراسة أهميتها العلمية من تناولها العلاقة التكاملية بين إدارة المخاطر والأمن السيبراني في بيئة الجامعات السعودية، وهي علاقة لم تحظَ بدرجة كافية من البحث الأكاديمي رغم أهميتها في حماية البنية التحتية الرقمية وضمان استمرارية الخدمات الأكاديمية والإدارية وتسعى الدراسة إلى توضيح دور إدارة المخاطر كمنهج استراتيجي في دعم منظومة الأمن السيبراني من خلال تحديد كيفية تطبيق مبادئ إدارة المخاطر مثل التقييم، الاستجابة، والمراقبة على التهديدات الرقمية كما تسهم الدراسة في إثراء الأدبيات العلمية بمجال إدارة المخاطر السيبرانية في قطاع التعليم العالي من خلال تحليل تجربة جامعة الملك سعود بن عبدالعزيز للعلوم الصحية كنموذج تطبيقي يُظهر كيف يمكن للحوكمة المؤسسية أن تدمج إدارة المخاطر في سياسات الأمن السيبراني لتعزيز الوقاية من التهديدات وتحسين الاستجابة لها.

وتُعد هذه الدراسة من المحاولات الأكاديمية التي تسعى إلى تطوير إطار نظري وتطبيقي يربط بين المجالين الإداري والفني ضمن مفهوم "حوكمة المخاطر السيبرانية" بما يتوافق مع متطلبات الهيئة الوطنية للأمن السيبراني (NCA) .

ثانياً: الأهمية العملية:

❖ تحسين أداء الجامعات السعودية:

من خلال تحليل العلاقة بين إدارة المخاطر والأمن السيبراني، يمكن تقديم توصيات عملية لتطوير السياسات والإجراءات التنظيمية داخل الجامعات السعودية بما يرفع من مستوى الجاهزية السيبرانية ويقلل من احتمالية التعرض للحوادث الرقمية.

❖ تعزيز التكامل المؤسسي:

تساعد نتائج الدراسة في تحسين التنسيق بين الإدارات الفنية والإدارية داخل الجامعات (مثل إدارة المخاطر، تقنية المعلومات، والأمن السيبراني)، مما يؤدي إلى بناء منظومة موحدة لحوكمة المخاطر والسياسات الأمنية الرقمية.

❖ دعم متخذي القرار:

توفر الدراسة مؤشرات قياس أداء (KPIs) ومعايير تقييم تساعد القيادات الجامعية وصناع القرار في متابعة مدى فاعلية إدارة المخاطر السيبرانية وتوجيه الموارد نحو المجالات الأكثر تأثيراً في الوقاية والاستجابة للحوادث.

❖ تعزيز الوعي وبناء القدرات:

من خلال نتائجها وتوصياتها تسهم الدراسة في رفع مستوى الوعي السيبراني والمهارات الفنية والإدارية للعاملين في الجامعات بما يعزز ثقافة الأمن الرقمي المؤسسي ويحدّ من المخاطر البشرية (Human Factor Risks)

❖ دعم تحقيق رؤية السعودية 2030:

تأتي هذه الدراسة متوافقة مع مستهدفات رؤية (2030) في محور التحول الرقمي والحكومة الإلكترونية من خلال بناء بيئة جامعية آمنة ومتطورة تقنياً تدعم الابتكار والبحث العلمي في بيئة رقمية موثوقة ومستدامة.

❖ الاستفادة المؤسسية:

تمثل جامعة الملك سعود بن عبد العزيز للعلوم الصحية نموذجاً يمكن تعميمه على جامعات سعودية أخرى، مما يتيح تطوير إطار وطني موحد لإدارة مخاطر الأمن السيبراني مع متطلبات الهيئة الوطنية للأمن السيبراني (NCA).

أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل دور إدارة المخاطر في تعزيز الأمن السيبراني في الجامعات السعودية مع التركيز على جامعة الملك سعود بن عبد العزيز للعلوم الصحية كنموذج تطبيقي، ويمكن تلخيص أهدافها فيما يلي:

- تحديد مستوى تطبيق مبادئ إدارة المخاطر في مجال الأمن السيبراني داخل الجامعات السعودية .
- تقييم مدى التكامل بين إدارة المخاطر ووحدة الأمن السيبراني من حيث السياسات والإجراءات والتنظيم المؤسسي.
- تحليل فاعلية التكامل المؤسسي في تعزيز حماية البنية التحتية الرقمية وضمان استمرارية الخدمات الأكاديمية.
- استكشاف أهم التحديات والعوائق التي تواجه تحقيق التكامل بين إدارة المخاطر والأمن السيبراني في بيئة الجامعات السعودية.
- تقديم توصيات عملية تسهم في تطوير الأطر والسياسات الوطنية المتعلقة بإدارة المخاطر السيبرانية في مؤسسات التعليم العالي.

تساؤلات الدراسة:

سؤال البحث الرئيسي:

ما دور إدارة المخاطر في تعزيز الأمن السيبراني في الجامعات السعودية، ومدى فاعلية التكامل بينهما في حماية البنية الرقمية وضمان استمرارية الخدمات الأكاديمية؟

ويتفرع من السؤال الرئيسي مجموعة من الأسئلة الفرعية التي تتمثل فيما يلي:

-السؤال الفرعي الأول: إلى أي مدى تُطبَّق مبادئ إدارة المخاطر في مجال الأمن السيبراني داخل الجامعات السعودية؟

-السؤال الفرعي الثاني : ما مستوى إدراك منسوبي الجامعات السعودية لفئات المخاطر السيبرانية المحتملة في البيئة الجامعية؟

-السؤال الفرعي الثالث: ما مدى إسهام التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني في تعزيز الوقاية من التهديدات السيبرانية والاستجابة لها في الجامعات السعودية؟

-السؤال الفرعي الرابع: ما أهم التحديات التنظيمية والتقنية التي تعيق تحقيق التكامل الفعال بين إدارة المخاطر والأمن السيبراني في الجامعات السعودية؟

-السؤال الفرعي الخامس: ما مدى فاعلية الإطار التنظيمي والسياسات المعتمدة في دعم التكامل بين إدارة المخاطر والأمن السيبراني في الجامعات السعودية؟

-السؤال الفرعي السادس: ما مدى إسهام تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني في تعزيز فاعلية إدارة المخاطر في الجامعات السعودية؟

فرضيات الدراسة:

الفرضية الرئيسية:

لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني في جامعة الملك سعود بن عبد العزيز للعلوم الصحية.

الفرضيات الفرعية:

الفرض الأول: لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر والتكامل المؤسسي بين إدارة المخاطر والأمن السيبراني .

الفرض الثاني: لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر والتحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني.

الفرض الثالث لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر وفاعلية الإطار التنظيمي والسياسات والإجراءات المعتمدة في مجال الأمن السيبراني وإدارة المخاطر في الجامعة.

الفرض الرابع: لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر المؤسسية وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني.

النظرية العلمية المتبعة لإعداد البحث:

تعتمد هذه الدراسة على نظرية إدارة المخاطر المؤسسية (ERM) بوصفها الإطار العلمي الرئيسي الذي يستند إليها في إعداد البحث وتحليل متغيراته، وذلك لما تتميز به هذه النظرية من شمولية في تفسير كيفية تعامل المؤسسات مع المخاطر التي قد تؤثر في تحقيق أهدافها الاستراتيجية والتشغيلية وتنطلق نظرية إدارة المخاطر المؤسسية من مبدأ أساسي مفهومة أن المخاطر لا ينبغي التعامل معها بشكل منفصل أو تقني فقط، بل يجب إدارتها ضمن إطار مؤسسي متكامل يربط بين الحوكمة المؤسسية، والاستراتيجية، والعمليات، واتخاذ القرار.

وفي هذا السياق، تستند الدراسة إلى معيار (ISO 31000, 2018) الذي يؤكد أن إدارة المخاطر عملية منهجية ومنظمة تشمل تحديد المخاطر، وتحليلها، وتقييمها، ثم معالجتها ومراقبتها بشكل مستمر بما يسهم في تحسين كفاءة الأداء المؤسسي وضمان استمرارية الأعمال، كما تعتمد الدراسة على إطار (COSO ERM, 2017) الذي يربط إدارة المخاطر بصياغة الاستراتيجيات وتحسين الأداء المؤسسي ويؤكد دورها في دعم اتخاذ القرارات الاستباقية وتحقيق القيمة المستدامة.

وبناءً على ذلك، تنظر هذه الدراسة إلى الأمن السيبراني بوصفه أحد التطبيقات العملية لإدارة المخاطر في البيئة الرقمية ويتيح هذا الإطار تفسير العلاقة بين متغيرات الدراسة وتحليلها في جامعة الملك سعود بن عبد العزيز للعلوم الصحية كنموذج تطبيقي كما يسهم اعتماد هذا النموذج في اختبار فرضيات الدراسة والتوصل إلى نتائج علمية يمكن الاستفادة منها وتعميمها على مؤسسات التعليم العالي السعودية بما يتوافق مع الضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني (NCA)، ولا سيما الضوابط الأساسية للأمن السيبراني (ECC-2:2024)، وبما يدعم حماية الأصول المعلوماتية وضمان استمرارية الخدمات الأكاديمية والإدارية.

خاتمة الفصل:

في هذا الفصل تم عرض الإطار العام للدراسة المتعلقة بدور إدارة المخاطر في تعزيز الأمن السيبراني في الجامعات السعودية، حيث تم تقديم مقدمة توضح خلفية الموضوع في ظل التحول الرقمي المتسارع في قطاع التعليم العالي. كما تم تحديد مشكلة الدراسة وصياغة التساؤلات الرئيسة والفرعية التي تسعى الدراسة إلى الإجابة عنها. إضافة إلى ذلك، تم توضيح أهمية الدراسة العلمية والعملية، وتحديد الأهداف التي تسعى إلى تحقيقها، إلى جانب عرض فرضيات الدراسة التي تهدف إلى اختبار العلاقة بين ممارسات إدارة المخاطر وفعالية الأمن السيبراني في جامعة الملك سعود بن عبد العزيز للعلوم الصحية كنموذج تطبيقي.

الفصل الثاني

الدراسات السابقة والإطار النظري

مقدمة:

يهدف هذا الفصل إلى استعراض الخلفية العلمية للدراسة من خلال تناول الدراسات السابقة ذات الصلة بموضوع إدارة المخاطر والأمن السيبراني، إضافةً إلى عرض الإطار النظري الذي تستند إليه الدراسة. ويسهم هذا الفصل في بناء أساس معرفي ومنهجي يدعم تحليل متغيرات البحث، ويساعد على توضيح ما يميز هذه الدراسة عن الدراسات السابقة. كما يتناول الفصل توضيح متغيرات الدراسة حيث تتمثل في إدارة المخاطر المؤسسية بوصفها المتغير المستقل، وفاعلية الأمن السيبراني بوصفها المتغير التابع مع بيان أبعادهما والعلاقة التكاملية بينهما في سياق مؤسسات التعليم العالي السعودية بما يدعم صياغة فرضيات الدراسة وتحليل نتائجها بصورة علمية ومنهجية.

نموذج الدراسة:

يهدف هذا النموذج إلى التعرف على أثر ممارسات إدارة المخاطر المؤسسية في تعزيز فاعلية الأمن السيبراني، وذلك بالتطبيق على جامعة الملك سعود بن عبد العزيز للعلوم الصحية في المملكة العربية السعودية. ويعتمد النموذج على افتراض أن التطبيق المنهجي لإدارة المخاطر يسهم في رفع مستوى الجاهزية السيبرانية، والحد من المخاطر الرقمية، وتحسين قدرة الجامعة على حماية أصولها المعلوماتية وضمان استمرارية خدماتها الأكاديمية والإدارية.

❖ المتغير المستقل:

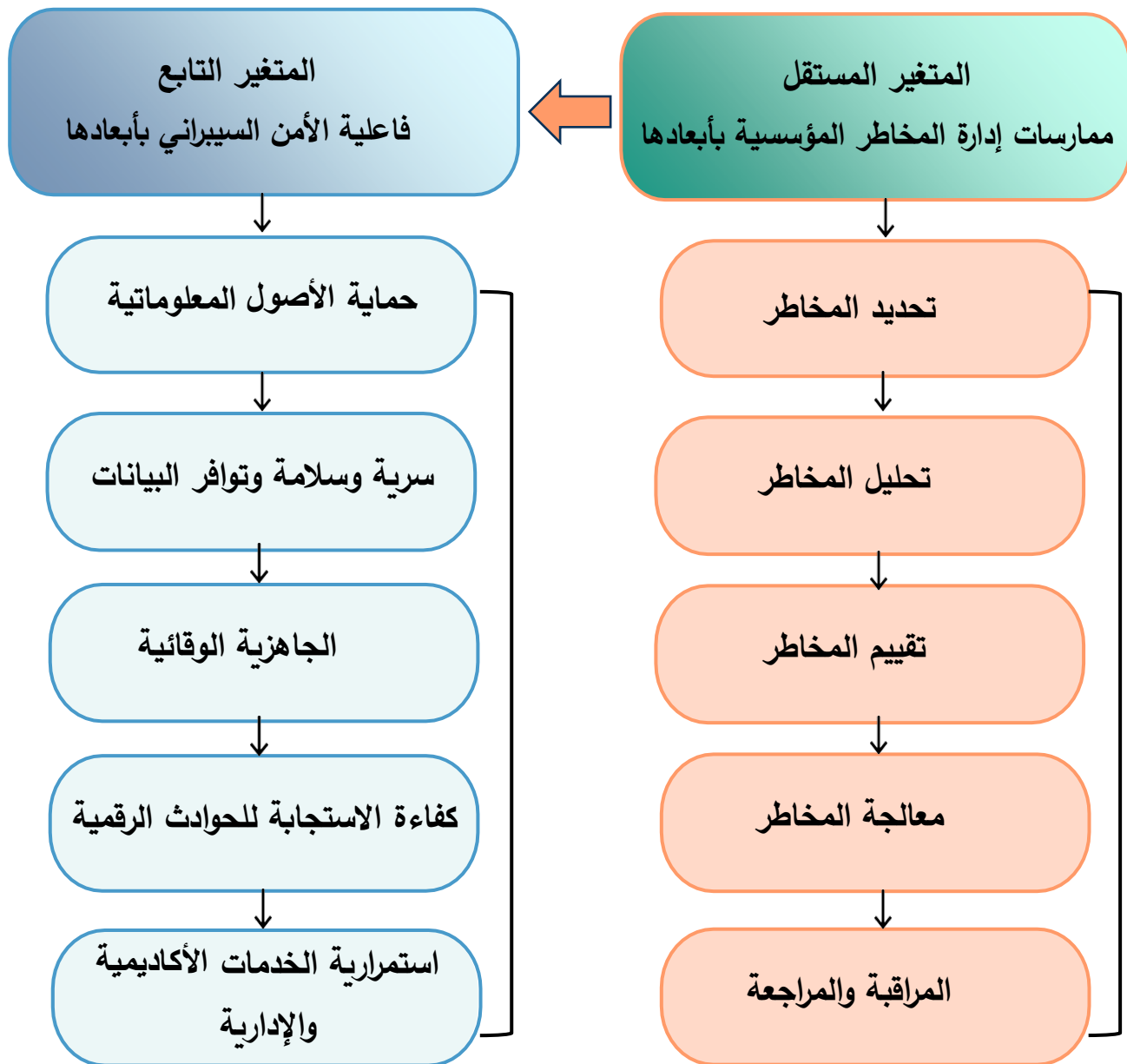
ممارسات إدارة المخاطر المؤسسية بأبعادها، وتشمل:

(تحديد المخاطر - تحليل المخاطر - تقييم المخاطر - معالجة المخاطر - المراقبة والمراجعة).

❖ المتغير التابع:

فاعلية الأمن السيبراني بأبعادها، وتشمل:

(حماية الأصول المعلوماتية - سرية وسلامة وتوافر البيانات - الجاهزية الوقائية - كفاءة الاستجابة للحوادث الرقمية - استمرارية الخدمات الأكاديمية والإدارية).



شكل رقم (1-1) متغيرات الدراسة

من إعداد الباحث

الدراسات السابقة:

من خلال هذا القسم يتم استعراض وتحليل الدراسات السابقة ذات الصلة بموضوع إدارة المخاطر والأمن السيبراني ، وذلك من خلال استعراض أبرز الاتجاهات البحثية، والمفاهيم والنماذج النظرية، والمنهجيات المستخدمة، إضافةً إلى النتائج التي توصلت إليها تلك الدراسات ويسهم هذا العرض في تكوين فهم متكامل للإطار المعرفي الذي تناولته الأدبيات العلمية وتحديد أوجه الاتفاق والاختلاف بين الدراسات، والكشف عن الفجوات البحثية التي لم تحظَ بالمعالجة الكافية.

كما يركّز هذا القسم على إبراز موقع الدراسة الحالية وتمييزها مقارنةً بالدراسات السابقة، من حيث نطاق البحث، والسياق التطبيقي، والمتغيرات محل الدراسة، والمنهجية المستخدمة. إذ تسعى هذه الدراسة إلى تقديم إضافة علمية من خلال التركيز على التكامل بين إدارة المخاطر والأمن السيبراني في مؤسسات التعليم العالي السعودية، في ظل التحول الرقمي، وهو ما يُعد مجالاً بحثياً لا يزال بحاجة إلى مزيد من الدراسة المتعمقة في البيئة المحلية.

1-دراسة (القحطاني، 2019) بعنوان مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات

الجامعات السعودية من منظور اجتماعي: دراسة ميدانية

- هدفت الدراسة إلى التعرف على مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي، من خلال دراسة ميدانية تناولت مستوى إدراك الطلبة لمفهوم الأمن السيبراني وأبرز الجرائم المرتبطة به ووسائل الوقاية منها.
- اعتمدت الدراسة على المنهج الوصفي المسحي، حيث تم استخدام الاستبانة أداةً لجمع البيانات من عينة مكونة من (486) طالباً وطالبة من الجامعات السعودية. وأظهرت نتائج الدراسة أن مفهوم الأمن السيبراني لدى الطلبة يتمثل في استخدام وسائل تقنية وتنظيمية تهدف إلى حماية الأنظمة المعلوماتية من الاختراق وسوء الاستخدام.
- أظهرت نتائج الدراسة أن الاحتيال الإلكتروني يعد من أكثر الجرائم السيبرانية شيوعاً، وأن التوعية الإعلامية والمجتمعية تمثل من أهم وسائل الوقاية من الجرائم السيبرانية.
- وأوصت الدراسة بضرورة تعزيز برامج التوعية بالأمن السيبراني في المجتمع والجامعات، وتطوير البنية التحتية للأمن السيبراني، وإدراج مفاهيم الأمن السيبراني في المناهج التعليمية، إضافة إلى تعزيز دور الأسرة في توجيه استخدام الأبناء للتقنيات الرقمية.

2-دراسة (الخضري وآخرون ،2020) بعنوان: الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة.

- هدفت الدراسة إلى تحليل واقع الأمن السيبراني في الجامعات السعودية وإلى قياس مدى اعتماد هذه الجامعات على تقنيات الذكاء الاصطناعي لتحسين القدرات الدفاعية الرقمية.
- اعتمدت الدراسة على المنهج الوصفي التحليلي المقارن، وشملت الدراسة عدة جامعات حكومية.
- أظهرت نتائج الدراسة وجود تفاوت واضح في مستوى جاهزية الأمن السيبراني بين الجامعات، بالإضافة إلى ضعف في الوعي الأمني وقصور في التكامل المؤسسي بين الجهات الفنية والتنظيمية.
- وأوصت الدراسة بضرورة تعزيز الحوكمة السيبرانية، وتطوير سياسات موحدة، وبناء قدرات بشرية قادرة على مواجهة التهديدات الرقمية.

3-دراسة (البيشي، 2021) بعنوان: الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس دراسة على جامعة بيشة.

- هدفت الدراسة قياس أثر تطبيق الأمن السيبراني على مستوى الثقة الرقمية لدى منسوبي جامعة بيشة.
- ولتحقيق أهداف الدراسة استخدم الباحث المنهج الوصفي التحليلي والاستبانة كأداة لجمع البيانات.
- وأظهرت نتائج الدراسة وجود علاقة إيجابية قوية بين مستوى تطبيق الأمن السيبراني والثقة الرقمية لدى أعضاء هيئة التدريس في جامعة بيشة، مما يؤكد أهمية الإجراءات والسياسات الأمنية في تعزيز الاطمئنان نحو الخدمات الإلكترونية في البيئة الجامعية.
- وأوصت الدراسة على بضرورة تعزيز الوعي السيبراني وتخصيص ميزانيات لتطوير وحدات الأمن السيبراني داخل الجامعات وبرامج التوعية الرقمية ، نظرًا لدور هذه الممارسات في تحسين الحماية الرقمية ودعم استمرارية الخدمات الأكاديمية.

4-دراسة بعنوان: (2021, Almomani, I., Ahmed, M., & Maglaras, L.)

Cybersecurity Maturity Assessment Framework for Higher Education

.Institutions in Saudi Arabia (SCMAF)

- قدّم الباحثون إطارًا لقياس نضج الأمن السيبراني في مؤسسات التعليم العالي، اعتمادًا على معايير NIS و ISO وقد استخدم الإطار لتقييم جاهزية الجامعات السعودية في حماية أصولها الرقمية وتطوير استراتيجيات أمنية فعّالة.

- هدفت الدراسة إلى تصميم إطار معياري لتقييم نضج الأمن السيبراني في الجامعات بما يدعم عمليات التطوير المؤسسي.
- استخدم الباحثون المنهج الوصفي الكمي، من خلال تحليل بيانات من جامعات سعودية متعددة لتحديد مستوى الجاهزية الأمنية.
- أظهرت نتائج الدراسة عن وجود فجوات معتبرة في مستوى النضج السيبراني داخل مؤسسات التعليم العالي خصوصاً في مجالات إدارة المخاطر، تدريب العاملين، وتطوير السياسات، وكذلك بينت النتائج أن غياب نموذج معياري يحد من قدرة الجامعات على قياس جاهزيتها بدقة، وأن ربط التقييمات بممارسات الحوكمة وإدارة المخاطر يسهم في تحسين الفاعلية السيبرانية.
- أوصت الدراسة بضرورة تبني إطار قياس معياري لتقييم مستوى النضج السيبراني في مؤسسات التعليم العالي، وربطه على نحو مباشر بممارسات إدارة المخاطر المؤسسية لضمان تحسين الحوكمة الرقمية. كما شددت الدراسة على أهمية تطوير استراتيجية سيبرانية شاملة تتوافق مع احتياجات الجامعات التقنية والتنظيمية، وتعزيز التدريب والوعي الأمني لجميع العاملين والطلاب، إلى جانب ضرورة توحيد السياسات والإجراءات الأمنية داخل المؤسسة لضمان تطبيق متسق وفعال لضوابط الأمن السيبراني، إضافةً إلى تحسين قدرات الاستجابة للحوادث عبر تفعيل خطط طوارئ سيبرانية قائمة على تقييم المخاطر المستمر ودعم عمليات اتخاذ القرار المبني على البيانات.

5-دراسة (Ulven, J. B., & Wangen, G) (2021) بعنوان:

A Systematic Review of Cybersecurity Risks in Higher Education

- هدفت الدراسة إلى تحديد أبرز مخاطر الأمن السيبراني التي تواجه مؤسسات التعليم العالي، وتحليل الاتجاهات البحثية المتعلقة بالأمن السيبراني في الجامعات، إضافة إلى تقديم تصور شامل حول طبيعة التهديدات السيبرانية التي قد تؤثر في البنية التحتية الرقمية للمؤسسات التعليمية.
- اعتمدت الدراسة على المنهج التحليلي القائم على المراجعة المنهجية للأدبيات العلمية (Systematic Literature Review)، حيث قام الباحثان بتحليل مجموعة من الدراسات العلمية المنشورة في مجال الأمن السيبراني في التعليم العالي، بهدف تصنيف أنواع المخاطر السيبرانية وتحليل أسبابها وتأثيراتها.
- أظهرت نتائج الدراسة أن الجامعات تُعد من أكثر المؤسسات عرضة للهجمات السيبرانية بسبب الطبيعة المفتوحة للبيئة الأكاديمية وتعدد المستخدمين والأنظمة الرقمية. كما بينت النتائج أن أبرز المخاطر السيبرانية تشمل هجمات التصيد الإلكتروني، والبرمجيات الخبيثة، وسرقة البيانات، وضعف إدارة الوصول إلى الأنظمة. وأشارت الدراسة إلى أن ضعف الوعي الأمني لدى المستخدمين

ونقص السياسات التنظيمية يعدان من أهم العوامل التي تزيد من احتمالية حدوث الهجمات السيبرانية.

- أوصت الدراسة بضرورة تعزيز ممارسات إدارة المخاطر السيبرانية في مؤسسات التعليم العالي، وتطوير سياسات أمن المعلومات، وتطبيق استراتيجيات متكاملة تشمل الجوانب التقنية والتنظيمية والبشرية. كما أكدت على أهمية نشر الوعي بالأمن السيبراني وتوفير برامج تدريبية مستمرة للعاملين والطلاب، إضافة إلى تبني أطر حوكمة فعالة لإدارة الأمن السيبراني في الجامعات.

6-دراسة (المنيع، 2022) بعنوان: متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030.

- هدفت الدراسة إلى تحديد متطلبات تحقيق الأمن السيبراني في الجامعات السعودية، وتحليل مدى توافقها مع مستهدفات رؤية المملكة 2030، من خلال استعراض الممارسات والسياسات المطبقة داخل مؤسسات التعليم العالي.
- ولتحقيق أهداف الدراسة اعتمدت الباحثة المنهج الوصفي التحليلي، واستخدمت تحليل الوثائق والمقابلات لجمع البيانات من عدد من الجامعات السعودية.
- توصلت نتائج الدراسة إلى وجود قصور في التكامل بين الإدارات الفنية والإدارية فيما يتعلق بتنفيذ سياسات الأمن السيبراني، مما يؤثر على كفاءة الحماية الرقمية في الجامعات.
- وأوصت الدراسة بزيادة برامج التوعية للموظفين حول مخاطر استخدام الأجهزة الشخصية لنقل البيانات السرية، ومنح حوافز مادية ومعنوية للموظفين المتميزين في مجال الأمن السيبراني.

7-دراسة (السميري، 2022) بعنوان: واقع الأمن السيبراني وتحدياته في السعودية

- هدفت الدراسة إلى التعرف على أبرز التحديات التي تواجه المؤسسات السعودية في تطبيق ممارسات الأمن السيبراني، ومدى استعدادها للتعامل مع التهديدات الرقمية المتزايدة.
- ولتحقيق أهداف الدراسة استخدم الباحث المنهج الوصفي التحليلي، وجمع البيانات من خلال استبانة موجهة إلى موظفي القطاعين العام والخاص.
- وأظهرت نتائج الدراسة وجود ضعف في التنسيق بين الإدارات المختلفة وغياب التكامل بين الإجراءات الفنية والتنظيمية، بالإضافة إلى نقص برامج التدريب والوعي السيبراني.
- وأوصت الدراسة على ضرورة دمج إدارة المخاطر في السياسات الأمنية وتكثيف برامج التدريب الوطني للموظفين في القطاعين العام والخاص.

8-دراسة (الحربي، 2022) بعنوان: أثر التحول الرقمي على كفاءة الأداء الأكاديمي - حالة دراسية لهيئة أعضاء التدريس بجامعة الملك عبد العزيز.

- هدفت الدراسة إلى تحليل مدى تأثير التحول الرقمي على كفاءة الأداء الأكاديمي، وتحديد متطلبات التحول الرقمي اللازمة لرفع كفاءة أعضاء هيئة التدريس، إضافة إلى تحليل المعوقات التي قد تحد من فاعلية تطبيق التحول الرقمي داخل الجامعة.
- ولتحقيق أهداف الدراسة اعتمد الباحث المنهج الوصفي التحليلي واستبانة وُزعت على عينة من أعضاء هيئة التدريس.
- وتوصلت نتائج الدراسة إلى وجود أثر دال للتحول الرقمي على تحسين الأداء الأكاديمي، كما بيّنت أن توفر البنية التحتية التقنية، والدعم الفني، ومعايير التحول الرقمي يعدّ من العوامل الأساسية المؤثرة في نجاح العملية التعليمية. وكشفت الدراسة كذلك عن وجود معوقات تحد من فاعلية التحول الرقمي أبرزها ضعف الدعم الفني وصعوبة التعامل مع بعض البرمجيات.
- كما أوصت الدراسة بتعزيز متطلبات التحول الرقمي داخل الجامعة لضمان رفع كفاءة الأداء الأكاديمي، وضرورة إزالة المعوقات التي تحد من فاعلية التحول الرقمي، والالتزام بالمعايير الأكاديمية والتقنية المطلوبة، وتعزيز استخدام الأنظمة الرقمية مثل نظام البلاك بورد لتسهيل تقديم الخدمات الأكاديمية. كما شددت على أهمية توفير بنية تحتية تقنية متطورة، وتشكيل فرق عمل مختصة بالتخطيط للتعليم الرقمي، وإنشاء رؤية رقمية مشتركة يلتزم بها أعضاء هيئة التدريس والطلاب. وأوصت كذلك بتوفير محتوى تفاعلي يدعم العملية التعليمية، واستقطاب كوادر بشرية مؤهلة، وتعزيز مهارات التعامل مع البرمجيات والدعم الفني، إلى جانب توفير الأجهزة والمعدات اللازمة للتحول الرقمي، وأخيرًا التأكيد على أهمية التقييم المستمر للأنظمة الرقمية ومقارنتها بالمعايير العالمية لضمان تحسين جودة الأداء الأكاديمي.

9-دراسة (2022,Cheng, E. C. K., & Wang, T.) بعنوان:

Institutional Strategies for Cybersecurity in Higher Education Institution.

- تطرق الباحثان في هذه الدراسة إلى استراتيجيات الأمن السيبراني المؤسسية في الجامعات العالمية، وتم مناقشة أهمية الحوكمة والتكامل بين الإدارة التقنية والإدارية لضمان استمرارية الأعمال الأكاديمية.
- هدفت الدراسة إلى تحديد الاستراتيجيات المؤسسية التي تعزز الأمن السيبراني في مؤسسات التعليم العالي، مع التركيز على الحوكمة والتكامل التنظيمي بين الإدارات.

- استخدم الباحثان المنهج الوصفي التحليلي لعدد من الجامعات الأوروبية والآسيوية.
- أظهرت نتائج الدراسة أن فاعلية الأمن السيبراني في مؤسسات التعليم العالي تعتمد بدرجة كبيرة على تبني نهج مؤسسي تكاملي يشمل الأبعاد التقنية والتنظيمية والبشرية. وبيّنت أن الجامعات التي تمتلك حوكمة رقمية واضحة وتدمج الأمن السيبراني ضمن استراتيجياتها الإدارية والتعليمية تُظهر مستوى أعلى من النضج السيبراني والجاهزية في مواجهة الهجمات والاختراقات الإلكترونية. كما أشارت النتائج إلى أن ضعف التنسيق بين الإدارات الأكاديمية والفنية وغياب آليات إدارة المخاطر ضمن منظومة الأمن السيبراني يُعدّ من أبرز التحديات التي تحدّ من كفاءة الاستجابة للحوادث الرقمية.
- أوصى الباحثان بضرورة دمج إدارة المخاطر ضمن إطار الحوكمة المؤسسية للأمن السيبراني، وإنشاء سياسات موحدة واستراتيجيات مؤسسية تضمن استدامة الأمن الرقمي عبر التعاون بين الإدارات التقنية والإدارية. كما أكّدت التوصيات على أهمية رفع الوعي السيبراني والتدريب المستمر للعاملين والطلاب، ووضع مؤشرات أداء رئيسية (KPIs) لقياس فعالية برامج الأمن السيبراني، وتعزيز ثقافة أمنية قائمة على المسؤولية المشتركة داخل الجامعات.

10-دراسة (2022, Alharbi, T.) بعنوان: Developing a Cost-effective

Cybersecurity Management System for Academic Institutions in Saudi Arabia.

- هدفت الدراسة إلى اقتراح نظام إدارة الأمن السيبراني (CMS) مصمم خصيصاً لمؤسسات التعليم العالي في المملكة العربية السعودية، مع مراعاة التكلفة والموارد المحدودة في هذه المؤسسات.
- استخدم الباحث المنهج التطبيقي، وقام بتصميم نموذج إداري وتقني يمكن تكييفه وفق متطلبات كل مؤسسة تعليمية.
- أظهرت نتائج الدراسة أن غالبية الجامعات السعودية تتبنى بعض المعايير الدولية للأمن السيبراني لكنها تفتقر إلى إطار مخصص للمؤسسات الأكاديمية من حيث التكلفة والمواءمة، وأن تحديات مثل نقص الدعم الإداري والموارد، وضعف الخبرة تُعقّد تطبيق الحلول الشاملة.
- أوصى الباحث بضرورة توفير التزام قيادي من مستوى الإدارة العليا، ودمج إدارة المخاطر ضمن منظومة الأمن السيبراني، وتبسيط الأطر لتتناسب الجامعات، بالإضافة إلى رفع وعي العاملين والتدريب المستمر واستحداث مؤشرات أداء واضحة للحماية السيبرانية في البيئة الجامعية السعودية.

11-دراسة (2022, Ganesen, R., Abu Bakar, A., Ramli, R., Rahim, F., & Ahmad

cybersecurity Risk Assessment: Modeling Factors بعنوان: (Zawawi, M.)

Associated with Higher Education Institutions

- تناول الباحثون في هذه الدراسة موضوع تقييم مخاطر الأمن السيبراني في مؤسسات التعليم العالي، مع التركيز على العوامل المؤثرة في مستوى المخاطر السيبرانية داخل الجامعات، وكيفية نمذجة هذه العوامل وتحليلها بهدف دعم عملية اتخاذ القرار في إدارة المخاطر الرقمية.
- هدفت الدراسة إلى تحديد العوامل الرئيسية المرتبطة بمخاطر الأمن السيبراني في مؤسسات التعليم العالي، وتطوير نموذج يساعد على تقييم هذه المخاطر وتحليل تأثيرها في البيئة التعليمية الرقمية، بما يساهم في تعزيز قدرة الجامعات على مواجهة التهديدات السيبرانية.
- اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال تحليل مجموعة من العوامل التنظيمية والتقنية المرتبطة بالأمن السيبراني في الجامعات، إضافة إلى استخدام نماذج تحليلية لتقييم مستوى المخاطر السيبرانية المرتبطة بالأنظمة التعليمية الرقمية.
- أظهرت نتائج الدراسة أن مستوى المخاطر السيبرانية في مؤسسات التعليم العالي يتأثر بعدة عوامل رئيسية، من أبرزها ضعف سياسات أمن المعلومات، ونقص الوعي السيبراني لدى المستخدمين، وقصور آليات إدارة المخاطر داخل المؤسسات التعليمية. كما بينت النتائج أن وجود إطار واضح لإدارة المخاطر وتكامل السياسات الأمنية يساهم في تقليل احتمالية وقوع الهجمات السيبرانية وتحسين مستوى الحماية الرقمية للأنظمة التعليمية.
- أوصت الدراسة بضرورة تطوير نماذج متقدمة لتقييم مخاطر الأمن السيبراني في الجامعات، وتعزيز تطبيق سياسات أمن المعلومات وإدارة المخاطر، إضافة إلى زيادة برامج التدريب والتوعية بالأمن السيبراني للعاملين والطلاب. كما أكدت التوصيات أهمية دمج إدارة المخاطر السيبرانية ضمن الاستراتيجيات المؤسسية للجامعات لضمان حماية البنية التحتية الرقمية واستمرارية الخدمات التعليمية.

12-دراسة (الهزاني، 2023) بعنوان: ضوابط ومتطلبات تطبيق الأمن السيبراني في جامعة

الأميرة نورة بنت عبد الرحمن.

- هدفت الدراسة إلى تقييم مدى التزام جامعة الأميرة نورة بتطبيق الضوابط الوطنية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، وتحليل التحديات المرتبطة بالتنفيذ.

- ولتحقيق أهداف الدراسة استخدمت الباحثة المنهج الوصفي التحليلي، وجمعت البيانات من خلال استبانة موجهة للعاملين في الإدارة التقنية والإدارية بالجامعة.
- وأظهرت نتائج الدراسة أن الجامعة حققت تقدماً ملحوظاً في تبني السياسات التقنية، إلا أن مستوى التنسيق بين الإدارات الإدارية والفنية يحتاج إلى مزيد من التطوير.
- وأوصت الدراسة على ضرورة دمج إدارة المخاطر في السياسات الأمنية وتكثيف برامج التدريب الوطني للموظفين في القطاعين العام والخاص.

13-دراسة (2025, Armas, R., & Taherdoost, H) بعنوان:

Building a cybersecurity culture in higher Education: Proposing a cybersecurity awareness paradigm. MDPI

- هدفت الدراسة إلى تحليل دور الثقافة المؤسسية في تعزيز الأمن السيبراني داخل مؤسسات التعليم العالي، من خلال فهم تأثير الوعي السيبراني والقيم والسلوكيات المهنية على قدرة الجامعات في مواجهة التهديدات الرقمية.
- استخدمت الدراسة منهج الاستدلال الاستنباطي (Deductive Approach) من خلال الاعتماد على نماذج ونظريات مسبقة حول الثقافة السيبرانية، ثم اختبارها وتحليلها في سياق جامعات أمريكية وأوروبية، مع توظيف أدوات تحليل نوعية لتفسير الأنماط السلوكية الرقمية لدى منسوبي تلك المؤسسات.
- توصلت نتائج الدراسة إلى أن الثقافة السيبرانية المستدامة تُعد عاملاً رئيسياً في خفض الحوادث الأمنية، وأن الوعي السيبراني والتدريب المستمر يسهمان بشكل مباشر في تحسين الامتثال للسياسات الأمنية وتقليل الأخطاء التشغيلية. كما أشارت الدراسة إلى وجود فجوات في التكامل بين الإدارات التقنية والإدارية، مما يُضعف فعالية جهود الأمن السيبراني. وأكدت النتائج أن دعم القيادات الجامعية يمثل عنصراً جوهرياً في تعزيز السلوك الأمني لدى الموظفين.
- وأوصت الدراسة بضرورة تطوير برامج تدريب متقدمة ومستمرة، وتعزيز التكامل المؤسسي بين إدارات الجامعة المختلفة، وتفعيل سياسات تشجع على الممارسات الأمنية اليومية، إضافةً إلى ضرورة تبني القيادة دوراً أكثر فعالية في نشر الوعي الأمني.

أوجه الشبه بين الدراسات السابقة:

من خلال تحليل الدراسات السابقة، يتضح وجود اتفاق عام بينها حول أهمية الأمن السيبراني في مؤسسات التعليم العالي، خاصة في ظل التوسع في استخدام الأنظمة الرقمية والخدمات الإلكترونية، كما أجمعت الدراسات على أن فاعلية الأمن السيبراني لا تعتمد فقط على الحلول التقنية، بل ترتبط بعوامل تنظيمية وإدارية وبشرية، مثل وضوح السياسات، ودعم الإدارة العليا، ومستوى الوعي السيبراني، والتنسيق بين الإدارات المختلفة.

كذلك تشابهت معظم الدراسات أن التحديات السيبرانية في البيئة الجامعية في انها تتسم بطابع مركب تتداخل فيه الأبعاد التقنية مع الجوانب المؤسسية والسلوكية، الأمر الذي يستلزم تبني نهج مؤسسي تكاملي يربط بين الحوكمة، والسياسات، وبناء القدرات البشرية، وإدارة المخاطر. ومن الناحية المنهجية، اعتمدت غالبية الدراسات على المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة رئيسة لجمع البيانات مع التركيز على قياس مستوى الجاهزية أو النضج السيبراني أو درجة الالتزام بالضوابط الوطنية والدولية. وفي المقابل، اتجهت بعض الدراسات الأجنبية إلى توظيف المراجعة المنهجية للأدبيات أو بناء الأطر والنماذج التحليلية، إلا أنها انتهت إلى نتائج مقارنة تؤكد أهمية الحوكمة والتوعية ودمج إدارة المخاطر ضمن الأطر التنظيمية للأمن السيبراني في مؤسسات التعليم العالي.

أوجه الاختلاف بين الدراسات السابقة:

رغم هذا الاتفاق إلا أن الدراسات اختلفت في نطاقها وأهدافها وزاوية المعالجة. فقد ركزت بعض الدراسات على قياس مستوى الوعي والثقافة السيبرانية لدى المستخدمين داخل الجامعات، في حين تناولت دراسات أخرى تقييم مستوى الجاهزية أو النضج السيبراني ودرجة الالتزام بالضوابط والمعايير الوطنية والدولية. كما اتجهت بعض الدراسات إلى تطوير أطر ونماذج لتقييم الأمن السيبراني أو إدارة مخاطره، بينما ركزت دراسات أخرى على تحليل أثر الأمن السيبراني في متغيرات مختلفة مثل الثقة الرقمية أو كفاءة الأداء الأكاديمي.

كما اختلفت الدراسات من حيث السياق التطبيقي إذ تناولت بعض الدراسات جامعات سعودية محددة، في حين ركزت دراسات أخرى على تجارب دولية أو عينات متعددة من المؤسسات التعليمية. كذلك تباينت الدراسات من حيث المنهجية المستخدمة حيث اعتمدت كثير من الدراسات على المنهج الوصفي التحليلي والاستبانة أداة رئيسة لجمع البيانات، بينما استخدمت بعض الدراسات الأخرى أساليب مختلفة،

مثل المراجعة المنهجية للأدبيات أو تطوير الأطر والنماذج التحليلية لتقييم مخاطر الأمن السيبراني ومستوى النضج السيبراني.

وعلى الرغم من أن العديد من الدراسات أشارت إلى أهمية إدارة المخاطر في دعم الأمن السيبراني، إلا أن معظمها تناول هذا الجانب بصورة عامة أو ضمن التوصيات، دون تحليل العلاقة المباشرة بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني داخل المؤسسات التعليمية، أو اختبارها بوصفها متغيرًا مستقلًا يمكن قياس أثره في تعزيز فاعلية الأمن السيبراني داخل البيئة الجامعية، وهو ما تسعى الدراسة الحالية إلى معالجته بصورة أكثر عمقًا.

الفجوة البحثية:

على الرغم من تعدد الدراسات التي تناولت موضوع الأمن السيبراني في الجامعات، إلا أن معظمها ركز على تقييم مستوى الوعي السيبراني أو قياس درجة الالتزام بالضوابط والسياسات الأمنية، أو تحليل مستوى الجاهزية والنضج السيبراني داخل المؤسسات التعليمية، ومع ذلك لا تزال هناك فجوة بحثية واضحة تتمثل في قلة الدراسات التي تناولت العلاقة التكاملية بين إدارة المخاطر المؤسسية وفاعلية الأمن السيبراني بصورة منهجية داخل البيئة الجامعية السعودية.

كما أن غالبية الدراسات لم تتناول بصورة تفصيلية كيفية توظيف مراحل إدارة المخاطر (التحديد، التحليل، التقييم، المعالجة، والمراقبة) في دعم السياسات والإجراءات السيبرانية داخل الجامعات بالإضافة إلى ذلك، لم تحظ مسألة الربط بين الأطر الوطنية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني والأطر الدولية لإدارة المخاطر باختبار ميداني كافٍ داخل مؤسسات التعليم العالي، مما يبرز الحاجة إلى إجراء دراسات تطبيقية تعالج هذا التكامل بصورة أعمق.

أوجه الاستفادة من الدراسات السابقة:

استفادت هذه الدراسة من الدراسات السابقة في بناء إطارها النظري وتحديد متغيراتها وصياغة أسئلتها وفرضياتها، حيث أسهمت الدراسات السابقة في توضيح واقع الأمن السيبراني في الجامعات السعودية، وإبراز التحديات التنظيمية والتقنية المرتبطة بضعف التكامل المؤسسي وغياب إدارة المخاطر ضمن المنظومة السيبرانية. كما وفّرت الدراسات السابقة أساسًا علميًا لفهم أهمية الحوكمة السيبرانية، ودور الوعي والتدريب، وأهمية دمج إدارة المخاطر في السياسات الأمنية.

وساعدت نتائج تلك الدراسات في تحديد الفجوات البحثية التي لم تحظَ بالمعالجة الكافية، خصوصًا ما يتعلق بدراسة العلاقة التكاملية بين إدارة المخاطر والأمن السيبراني في مؤسسات التعليم العالي السعودية، وربطها بالمعايير الوطنية والدولية ذات الصلة، وقد أسهم ذلك في توجيه الدراسة الحالية نحو معالجة هذه الفجوة البحثية وتحليلها بصورة أكثر عمقًا في سياق جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

ما يميز هذه الدراسة عن الدراسات السابقة:

على الرغم من إسهام الدراسات السابقة في توضيح واقع الأمن السيبراني في الجامعات وتبسيط الضوء على بعض التحديات التقنية والتنظيمية المرتبطة به، إلا أن معظمها ركّز على الأمن السيبراني بوصفه وظيفة تقنية مستقلة، أو تناول إدارة المخاطر بشكل عام دون الربط المنهجي والتكاملي بين المجالين. كما أن عددًا من هذه الدراسات اكتفى بوصف مستوى الجاهزية أو قياس الالتزام بالضوابط والمعايير، دون تحليل عميق لدور إدارة المخاطر المؤسسية في تعزيز فاعلية الأمن السيبراني ضمن إطار الحوكمة الجامعية.

لذا تتميز الدراسة الحالية عن تلك الدراسات بأنها تتناول العلاقة بين إدارة المخاطر والأمن السيبراني بوصفها علاقة تكاملية وليست علاقة موازية أو منفصلة، حيث تسعى إلى تحليل كيفية توظيف مبادئ إدارة المخاطر (التحديد، التقييم، المعالجة، والمراقبة) في دعم السياسات والإجراءات السيبرانية داخل الجامعات كما تتجاوز الدراسة الطرح الوصفي الشائع في الأدبيات السابقة، من خلال التركيز على تحليل مستوى التكامل المؤسسي بين الإدارات الإدارية والفنية وأثره في حماية الأصول المعلوماتية وضمان استمرارية الخدمات الأكاديمية.

ومن الناحية التطبيقية نلاحظ أن غالبية الدراسات السابقة إما تناولت عينات متعددة من الجامعات دون تعمق في السياق التنظيمي لكل جامعة، أو ركزت على تجارب دولية قد لا تتسجم كليًا مع البيئة التنظيمية والتشريعية في المملكة العربية السعودية في المقابل تنفرد هذه الدراسة بتركيزها على جامعة الملك سعود بن عبد العزيز للعلوم الصحية كنموذج تطبيقي مما يتيح تحليلًا أكثر دقة وواقعية لآليات التكامل بين إدارة المخاطر والأمن السيبراني في ضوء السياسات الوطنية والضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني.

كما أن هذه الدراسة أتت في توقيت يتزامن مع التحول الرقمي المتسارع ضمن إطار رؤية السعودية 2030، في حين أن عددًا من الدراسات السابقة أُجري في مراحل مبكرة من هذا التحول، ولم يعكس

بشكل كافٍ التوسع الحالي في الخدمات الرقمية والتعليم الإلكتروني والعمل عن بُعد وبذلك تسهم الدراسة الحالية في سد فجوة بحثية زمنية وتنظيمية، وتقدّم نتائج وتوصيات أكثر ملاءمة للواقع الراهن واحتياجات صنّاع القرار في مؤسسات التعليم العالي.

وبناءً على ما سبق، فإن القيمة المضافة لهذه الدراسة لا تقتصر على إعادة تناول موضوع الأمن السيبراني أو إدارة المخاطر، بل تتمثل في إعادة صياغة العلاقة بينهما ضمن إطار مؤسسي تكاملي يربط بين الحوكمة، والسياسات، والممارسات الإدارية والتقنية، بما يعزز من فاعلية الأمن السيبراني ويواكب متطلبات البيئة الجامعية السعودية الحديثة.

الإطار النظري للدراسة :

تقوم هذه الدراسة على إطار نظري يهدف إلى عرض المفاهيم والمتغيرات الرئيسة المرتبطة بإدارة المخاطر والأمن السيبراني في مؤسسات التعليم العالي، وذلك في ظل التحول الرقمي المتسارع الذي تشهده الجامعات السعودية وقد أسهم هذا التحول في التوسع في استخدام الأنظمة التقنية والاعتماد المتزايد على البيانات الرقمية في العمليات الأكاديمية والإدارية مما أدى إلى بروز المخاطر ولا سيما المخاطر السيبرانية بوصفها أحد التحديات الرئيسة التي تواجه استمرارية الأعمال وحماية الأصول المعلوماتية.

وانطلاقاً من ذلك تعتمد الدراسة على مجموعة من المحاور النظرية التي تبدأ بتوضيح مفهوم المخاطر وأنواعها ومصادرها ثم تنتقل إلى شرح إدارة المخاطر بوصفها عملية منهجية، قبل التطرق إلى مفهوم الأمن السيبراني وإبراز العلاقة التكاملية بينه وبين إدارة المخاطر، وصولاً إلى استعراض الأطر الوطنية والدولية الداعمة لهذا التكامل.

أولاً: مفهوم المخاطر (Risk Concept)

تُعرّف المخاطر بأنها احتمال وقوع حدث غير مؤكد قد يكون له تأثير إيجابي أو سلبي على تحقيق أهداف المؤسسة، نتيجة لعوامل داخلية أو خارجية. وتُعد المخاطر عنصراً ملازماً لكافة الأنشطة المؤسسية، إذ تختلف في طبيعتها وحدّتها باختلاف نوع المؤسسة ونشاطها وبيئتها التشغيلية، مما يستلزم التعامل معها بأسلوب علمي ومنهجي (ISO 31000, 2018) .

وتُعد إدارة المخاطر المؤسسية من الركائز الأساسية التي تعتمد عليها المؤسسات الحديثة في مواجهة التحديات المتزايدة الناتجة عن التطورات التقنية والاقتصادية والتنظيمية. إذ تساعد هذه الممارسات المؤسسات على التعرف المبكر على مصادر التهديد المحتملة، وتحليل آثارها المحتملة على الأهداف

الاستراتيجية والتشغيلية للمؤسسة، ومن ثم وضع الإجراءات المناسبة للحد من آثارها أو تجنبها كما تسهم إدارة المخاطر في تعزيز قدرة المؤسسات على اتخاذ القرارات الاستراتيجية المبنية على تحليل منهجي للمخاطر والفرص، الأمر الذي يعزز من كفاءة الأداء المؤسسي ويزيد من قدرة المؤسسات على تحقيق الاستدامة والاستمرارية في بيئة عمل تتسم بالتغير المستمر.

ثانيًا: أنواع المخاطر في مؤسسات التعليم العالي

تتعدد أنواع المخاطر التي تواجه المؤسسات، ويمكن تصنيفها إلى عدة فئات رئيسية، من أبرزها:

- **المخاطر الاستراتيجية:** المرتبطة بالقرارات طويلة الأجل وتحقيق الأهداف الاستراتيجية.
- **المخاطر التشغيلية:** الناتجة عن العمليات اليومية والإجراءات الداخلية.
- **المخاطر المالية:** المتعلقة بالموارد المالية والاستثمارات.
- **المخاطر التقنية والسيبرانية:** المرتبطة باستخدام الأنظمة الرقمية وحماية المعلومات.

وتُعد المخاطر السيبرانية من أبرز المخاطر التي تواجه مؤسسات التعليم العالي، نظرًا للاعتماد المتزايد على الأنظمة الرقمية في التعليم والإدارة والبحث العلمي (COSO ERM, 2017).

ثالثًا: تصنيف المخاطر حسب نوع المؤسسة

تختلف طبيعة المخاطر باختلاف نوع المؤسسة ونشاطها، ففي الجامعات تتركز المخاطر بشكل خاص حول:

- أمن المعلومات والبيانات الأكاديمية والبحثية.
- استمرارية الأنظمة التعليمية والإدارية.
- الامتثال للأنظمة والتشريعات ذات العلاقة.
- المخاطر البشرية المرتبطة بسلوك المستخدمين ومستوى الوعي السيبراني.

رابعًا: مصادر الخطر

تنشأ المخاطر من مصادر متعددة، يمكن تصنيفها إلى:

- **مصادر داخلية:** مثل ضعف السياسات والإجراءات، نقص التدريب، أو أخطاء المستخدمين.
- **مصادر خارجية:** مثل الهجمات السيبرانية، التطور التقني السريع، أو التهديدات التنظيمية.

خامسًا: خطوات إدارة المخاطر

تُعد إدارة المخاطر عملية منهجية منظمة تهدف إلى التعامل مع المخاطر بصورة استباقية، وتشمل الخطوات التالية:

- **تحديد المخاطر:** حصر المخاطر المحتملة التي قد تؤثر على أهداف المؤسسة.
- **تحليل المخاطر:** دراسة احتمالية وقوع المخاطر وتأثيرها.
- **تقييم المخاطر:** تحديد مستوى المخاطر وترتيب أولوياتها.
- **معالجة المخاطر:** اختيار الاستراتيجيات المناسبة، مثل التجنب أو التقليل أو النقل أو القبول.
- **المراقبة والمراجعة:** المتابعة المستمرة لفعالية الضوابط والإجراءات.

سادسًا: مفهوم الأمن السيبراني

يُقصد بالأمن السيبراني حماية الشبكات وأنظمة تقنية المعلومات والتقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع (تنظيم الهيئة الوطنية للأمن السيبراني، 2017).

ويهدف الأمن السيبراني إلى ضمان سرية البيانات وسلامتها وتوافرها، وهي المبادئ الأساسية المعروفة في مجال حماية المعلومات، حيث تشير السرية إلى حماية البيانات من الوصول غير المصرح به بينما تعني السلامة الحفاظ على دقة البيانات وعدم التلاعب بها، في حين يشير التوافر إلى ضمان إمكانية الوصول إلى الأنظمة والمعلومات عند الحاجة إليها من قبل المستخدمين المصرح لهم.

كما يشمل مفهوم الأمن السيبراني مجموعة من المجالات المرتبطة بحماية البيئة الرقمية مثل أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي، والتي تتكامل فيما بينها لتوفير منظومة شاملة لحماية الأنظمة التقنية والبنية التحتية المعلوماتية، وفي ظل التحول الرقمي المتسارع الذي تشهده المؤسسات الحديثة أصبحت الحاجة إلى تعزيز الأمن السيبراني أمرًا ضروريًا لضمان استمرارية الأعمال وحماية البيانات الحساسة من التهديدات الإلكترونية المتزايدة.

وقد أكدت الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني على أن تحقيق مستوى عالٍ من الأمن السيبراني يتطلب تكامل الأدوار والمسؤوليات بين الإدارات الفنية والإدارية داخل المؤسسة، إضافة إلى تبني نهج إداري متكامل يجمع بين تطبيق الضوابط التقنية وتعزيز ممارسات

الحوكمة المؤسسية وإدارة المخاطر بما يسهم في رفع مستوى الجاهزية السيبرانية للمؤسسات وتقليل احتمالية التعرض للهجمات الإلكترونية أو الاختراقات الرقمية (ECC-2:2024).

وفي المؤسسات التعليمية على وجه الخصوص تزداد أهمية الأمن السيبراني نتيجة الاعتماد المتزايد على الأنظمة الإلكترونية في إدارة العمليات الأكاديمية والبحثية مثل أنظمة إدارة التعلم وقواعد البيانات الأكاديمية ومنصات الخدمات الإلكترونية ويستلزم ذلك تبني سياسات وإجراءات فعّالة تسهم في حماية المعلومات الحساسة وضمان استقرار الخدمات الرقمية المقدمة للطلاب وأعضاء هيئة التدريس.

سابعاً: العلاقة التكاملية بين إدارة المخاطر والأمن السيبراني

يُعد الأمن السيبراني أحد التطبيقات العملية لإدارة المخاطر في البيئة الرقمية، حيث يسهم تبني منهجية إدارة المخاطر المؤسسية (ERM) في تعزيز الجاهزية السيبرانية، وتقليل احتمالية وقوع الحوادث الرقمية، وتحسين كفاءة الاستجابة لها عند حدوثها وفي هذا الإطار لم يعد الأمن السيبراني مقتصرًا على الجوانب التقنية فحسب، بل أصبح جزءًا لا يتجزأ من المنظومة الإدارية والتنظيمية التي تهدف إلى حماية الأصول المعلوماتية ودعم استمرارية الأعمال خصوصاً في مؤسسات التعليم التي تعتمد بشكل متزايد على الأنظمة الرقمية في عملياتها الأكاديمية والإدارية.

ويُعد التكامل بين إدارة المخاطر والأمن السيبراني ضرورة استراتيجية في المؤسسات الحديثة، إذ يُسهم هذا التكامل في بناء نظام شامل يتيح تحديد التهديدات التقنية وتحليلها وتقييم آثارها المحتملة، ووضع خطط استجابة استباقية للتعامل معها، كما يعزز هذا التكامل الحوكمة المؤسسية من خلال وضوح الأدوار والمسؤوليات وتكامل الإجراءات بين الإدارات المعنية، مثل إدارة المخاطر، ووحدة الأمن السيبراني، وإدارة تقنية المعلومات، بما يدعم الحوكمة الرقمية داخل الجامعات ويضمن حماية الأصول المعلوماتية الحساسة واستمرارية الخدمات الأكاديمية والإدارية.

كما يساعد هذا التكامل في تطوير إطار مؤسسي لإدارة المخاطر السيبرانية يربط بين السياسات التنظيمية والضوابط التقنية، الأمر الذي يسهم في رفع مستوى النضج المؤسسي في التعامل مع المخاطر الرقمية. كما يعزز ثقة المستخدمين في البيئة الرقمية التي تعتمد عليها المؤسسات التعليمية في تقديم خدماتها المختلفة.

ثامناً: الإطار الوطني والدولي الداعم للتكامل

تستند هذه الدراسة إلى مجموعة من الأطر المرجعية الوطنية والدولية التي تؤكد على أهمية التكامل بين إدارة المخاطر والأمن السيبراني، من أبرزها:

1. المعيار الدولي ISO 31000:2018

- يوفر إطاراً عالمياً لإدارة المخاطر يمكن تطبيقه في مختلف القطاعات.
- يؤكد على دمج إدارة المخاطر ضمن أنشطة القيادة والتخطيط وصنع القرار المؤسسي.

2. إطار COSO ERM (2017)

- يربط إدارة المخاطر بالأداء المؤسسي والاستراتيجية .
- يُشجع على اتخاذ القرارات المبنية على تحليل المخاطر وتعزيز القيمة التنظيمية.

3. ضوابط الهيئة الوطنية للأمن السيبراني وعلى رأسها: (NCA)

- الضوابط الأساسية للأمن السيبراني (ECC-2:2024)
- ضوابط البيانات (DCC-1:2022)
- ضوابط العمل عن بُعد (TCC-1:2021)
- ضوابط الحوسبة السحابية (CCC-1:2020)
- ضوابط الأنظمة الحساسة (CSCC-1:2019)

وتشكل هذه الضوابط الأساس التنظيمي لتطوير ممارسات الأمن السيبراني داخل الجامعات السعودية بما ينسجم مع إدارة المخاطر المؤسسية.

وبالاستناد إلى ما تم عرضه من أطر نظرية، وعلى رأسها معيار ISO 31000 وإطار COSO ERM وضوابط الهيئة الوطنية للأمن السيبراني (ECC-2:2024) ، يتضح أن إدارة المخاطر تمثل الأساس المنهجي لتعزيز فاعلية الأمن السيبراني داخل المؤسسات الحديثة. كما تشير الأدبيات إلى أن مستوى التكامل المؤسسي والوضوح التنظيمي وتطوير القدرات البشرية عوامل حاسمة في رفع مستوى الحماية الرقمية. ومن هذا المنطلق جاءت فرضيات الدراسة الواردة في الفصل الأول لاختبار هذه العلاقات ميدانياً داخل جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

خاتمة الفصل:

تناول هذا الفصل الإطار النظري للدراسة حيث تم استعراض متغيرات الدراسة وبيان مفاهيمها الرئيسية وأبعادها المختلفة، كما تم استعراض الدراسات السابقة ذات الصلة بموضوع الدراسة مع تحليل أبرز ما توصلت إليه من نتائج، وبيان أوجه الشبه والاختلاف بينها، إضافة إلى تحديد الفجوة البحثية وأوجه الاستفادة منها في بناء الدراسة الحالية ، وتم توضيح ما يميز هذه الدراسة عن الدراسات السابقة من حيث موضوعها، ومتغيراتها، وسياقها التطبيقي في الجامعات السعودية بما يسهم في تقديم إضافة علمية في مجال التكامل بين إدارة المخاطر المؤسسية وفاعلية الأمن السيبراني في مؤسسات التعليم العالي.

الفصل الثالث

منهجية الدراسة

مقدمة:

يعرض هذا الفصل الإطار المنهجي والإجراءات البحثية التي تم اتباعها في تنفيذ هذه الدراسة، بدءًا من تحديد تصميم البحث المناسب، وصولًا إلى توضيح آليات جمع البيانات وتحليلها إحصائيًا، وذلك بما يضمن تحقيق أهداف الدراسة والوصول إلى نتائج علمية دقيقة وموثوقة. ويُعد اختيار المنهج البحثي خطوة محورية في تصميم الدراسة، إذ يساهم في توجيه مسار البحث وتحديد الأساليب الملائمة لتحليل الظاهرة محل الدراسة في سياقها الواقعي.

وانطلاقًا من طبيعة موضوع الدراسة الذي يتناول واقع ممارسات إدارة المخاطر وعلاقتها بفاعلية الأمن السيبراني في البيئة الجامعية، فقد تم تصميم المنهجية بما يتيح فهم هذه الظاهرة من منظور مؤسسي شامل، يراعي الأبعاد التنظيمية والإدارية إلى جانب المتغيرات ذات الصلة بحماية المعلومات واستمرارية الأعمال. كما يركز هذا الفصل على بيان الأسس العلمية التي استندت إليها الدراسة في اختيار أدواتها البحثية، وتحديد مجتمعها، وتحليل بياناتها، بما يدعم موثوقية النتائج.

تصميم البحث:

نظرًا لطبيعة هذه الدراسة التي تهدف إلى التعرف على دور تطبيق ممارسات إدارة المخاطر في تعزيز فاعلية الأمن السيبراني داخل البيئة الجامعية، وبما يشمل أبعادها المرتبطة بحماية الأنظمة التقنية والمعلوماتية، والتكامل المؤسسي، واستمرارية الخدمات الأكاديمية والإدارية، فقد اعتمدت الدراسة على المنهج الوصفي التحليلي نظرًا لملاءمته لطبيعة الدراسة وأهدافها حيث يقوم هذا المنهج على جمع البيانات من عينة ممثلة لمجتمع الدراسة، ثم تنظيمها وتحليلها وعرضها إحصائيًا بهدف وصف الظاهرة محل البحث وقياس العلاقات بين متغيراتها.

وقد تم استخدام المنهج الوصفي في الجانب النظري من الدراسة، حيث يعمل هذا المنهج على وصف مفاهيم إدارة المخاطر والأمن السيبراني، وتوضيح أبعادهما، وبيان العلاقة بينهما، إضافة إلى توضيح متغيرات الدراسة والاطلاع على الأدبيات العلمية والدراسات السابقة ذات الصلة، بما يساهم في بناء الإطار النظري للدراسة.

كما تم استخدام المنهج التحليلي في الجانب الميداني من الدراسة، لكونه يعمل على تحليل بيانات الاستبانة لقياس العلاقات بين متغيرات الدراسة واختبار الفرضيات وتفسير النتائج تفسيرًا علميًا دقيقًا، ومن ثم إصدار الأحكام المناسبة المتعلقة بواقع تطبيق إدارة المخاطر ومستوى فاعلية الأمن السيبراني والتكامل المؤسسي بين الجهات ذات العلاقة في جامعة الملك سعود بن عبد العزيز للعلوم الصحية.

مجتمع البحث:

يتشمل مجتمع البحث في جميع منسوبي جامعة الملك سعود بن عبدالعزيز للعلوم الصحية في المملكة العربية السعودية ، والبالغ عددهم (6096) منسوباً ممن يرتبط عملهم بموضوع الدراسة ارتباطاً مباشراً أو غير مباشر. ولتحقيق الدقة المنهجية، تضمنت أداة الدراسة سؤالاً يحدد مدى ارتباط عمل المبحوث بالأنظمة التقنية (ارتباط مباشر / ارتباط غير مباشر)، بما يتيح تصنيف المشاركين وفق درجة علاقتهم الفنية أو التنظيمية بمجالي إدارة المخاطر والأمن السيبراني.

ويأتي اختيار مجتمع البحث على هذا النحو نظراً لدور منسوبي الجامعة باختلاف مواقعهم الوظيفية في دعم تطبيق سياسات إدارة المخاطر، والمساهمة في حماية الأصول المعلوماتية، وتعزيز ممارسات الأمن السيبراني داخل الجامعة.

كما يتيح إشراك هذه الفئات توفير بيانات دقيقة وشاملة تعكس واقع مستوى التكامل المؤسسي بين الجهات ذات العلاقة داخل الجامعة، من حيث تنسيق الأدوار وتكامل الإجراءات وتبادل المعلومات ويسهم ذلك في فهم أعمق لكيفية تأثير هذا التكامل على فاعلية الأمن السيبراني، سواء من حيث تعزيز القدرة على الوقاية من المخاطر السيبرانية أو تحسين آليات الاستجابة للحوادث بما يدعم بناء بيئة رقمية أكثر أماناً واستقراراً داخل الجامعة.

محددات حجم عينة الدراسة:

تكون مجتمع الدراسة من جميع منسوبي جامعة الملك سعود بن عبدالعزيز للعلوم الصحية في المملكة العربية السعودية، والبالغ عددهم (6096) منسوباً ممن يرتبط عملهم بموضوع الدراسة ارتباطاً مباشراً أو غير مباشر.

واعتمدت الدراسة على استخدام أسلوب العينة العشوائية البسيطة (Simple Random Sampling) لضمان تمثيل مناسب لمجتمع الدراسة، حيث تم اختيار عينة بلغ حجمها (300) مبحوثاً، وبلغ عدد الاستبيانات الموزعة إلكترونياً على أفراد العينة (300) استبيان حيث تم تحويل الاستبيان إلى استمارة إلكترونية عبر موقع (Google Forms) ، ومن ثم إرسال الرابط الإلكتروني إلى العينة المستهدفة عبر البريد الإلكتروني الرسمي، مع التأكيد على سرية المعلومات واستخدامها لأغراض البحث العلمي فقط و تم استرجاع (250) استبيان من إجمالي الاستبيانات الموزعة واستُبعد منها (25) استبيان لعدم صلاحيتها للتحليل الإحصائي وعليه بلغ عدد الاستبيانات الصالحة والمستخدم في التحليل الإحصائي (225) استبيان و يبين الجدول رقم (3-1) العينة المستهدفة والعينة الخاضعة للتحليل.

جدول رقم (3-1) العينة المستهدفة والخاضعة للتحليل

النسبة من العينة الموزعة	الاستبانات	
% 100	300	الاستبانات الموزعة
% 83.3	250	الاستبانات المسترجعة
% 8.3	25	الاستبانات المستبعدة
% 75	225	الاستبانات الخاضعة للتحليل

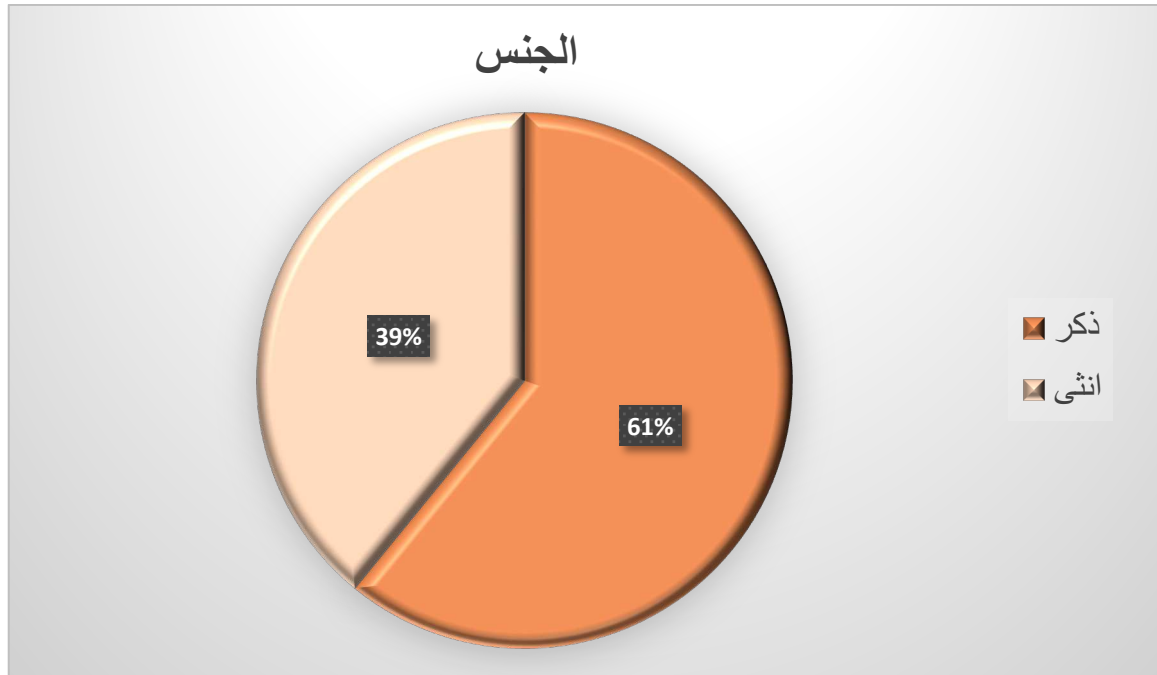
خصائص العينة:

يتناول هذا الجزء عرض الخصائص الشخصية والوظيفية لأفراد عينة الدراسة ، وذلك بهدف التعرف على السمات العامة للمبحوثين ومدى تنوعهم الوظيفي داخل الجامعة ، وقد اشتملت هذه الخصائص على عددًا من المتغيرات الديموغرافية ذات الصلة بموضوع البحث، مثل الجنس، والمستوى التعليمي، والمسمى الوظيفي، وعدد سنوات الخبرة، المدينة الجامعية ، ومدى الارتباط بالأنظمة التقنية (ارتباط مباشر / ارتباط غير مباشر) وذلك بهدف تقديم وصف إحصائي واضح لخصائص أفراد العينة، وبيان مدى تمثيلها لمجتمع الدراسة ، إلى جانب مقارنة الفروق بين الفئات المختلفة عند تحليل متغيرات الدراسة، بما يساعد على تفسير النتائج بشكل أدق.

♦ خصائص عينة الدراسة حسب الجنس

جدول رقم (3-2) خصائص العينة حسب الجنس

المتغير	فئات المتغير	العدد	النسبة المئوية %
الجنس	ذكر	137	% 60.9
	انثى	88	% 39.1
المجموع		225	% 100



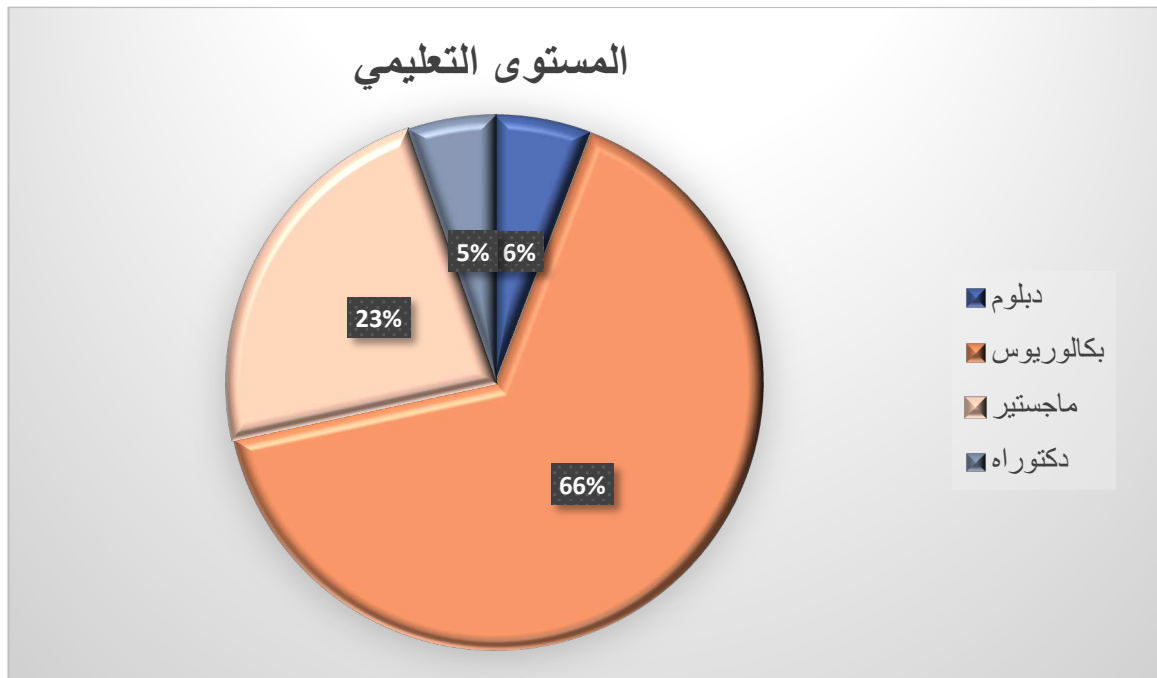
شكل رقم (2-3) خصائص العينة حسب الجنس

وبالنظر إلى الجدول (2-3) والشكل (2-3)، يتضح أن نسبة الذكور في عينة الدراسة كانت أعلى من نسبة الإناث، ويمكن تفسير ذلك بطبيعة بعض المهام الوظيفية المرتبطة بمجالات إدارة المخاطر والأمن السيبراني داخل البيئة الجامعية، والتي قد تتطلب خبرات تقنية متخصصة أو أدوارًا إشرافية يشغلها الذكور بنسبة أكبر في الوقت الحالي.

♦ خصائص عينة الدراسة حسب المستوى التعليمي

جدول رقم (3-3) خصائص عينة الدراسة حسب المستوى التعليمي

المتغير	فئات المتغير	العدد	النسبة المئوية %
المستوى التعليمي	دبلوم	13	5.8 %
	بكالوريوس	148	65.8 %
	ماجستير	52	23.1 %
	دكتوراه	12	5.3 %
المجموع		225	100 %



الشكل رقم (3-3) خصائص العينة حسب المستوى التعليمي

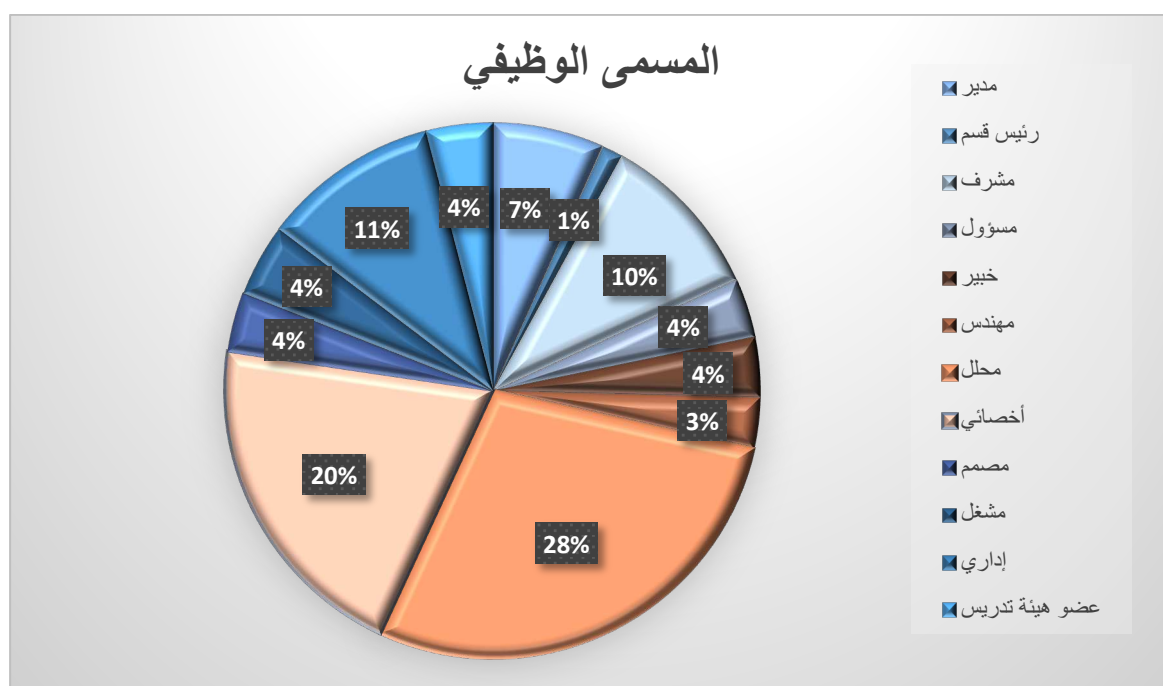
وبالنظر إلى الجدول (3-3) والشكل (3-3) ، يتضح أن غالبية أفراد عينة الدراسة يحملون درجة البكالوريوس بنسبة (65.8%)، تليها درجة الماجستير بنسبة (23.1%)، في حين بلغت نسبة الحاصلين على الدبلوم (5.8%)، والدكتوراه (5.3%). ويعكس ذلك أن معظم المشاركين يتمتعون بمستوى تعليمي جامعي، مما يعزز من موثوقية البيانات، نظرًا لقدرتهم على فهم مفاهيم إدارة المخاطر والأمن السيبراني والإجابة عن فقرات الاستبانة بدرجة عالية من الوعي والإدراك.

♦ خصائص عينة الدراسة حسب المسمى الوظيفي

جدول رقم (4-3) خصائص عينة الدراسة حسب المسمى الوظيفي

المتغير	فئات المتغير	العدد	النسبة المئوية %
المسمى الوظيفي	مدير	15	6.7 %
	رئيس قسم	3	1.3 %
	مشرف	23	10.2 %
	مسؤول	8	3.6 %
	خبير	8	3.6 %
	مهندس	7	3.1 %
	محلل	64	28.4 %

20.4%	46	اخصائي	
3.6%	8	مصمم	
4.4%	10	مشغل	
10.7%	24	إداري	
4.0%	9	عضو هيئة تدريس	
% 100	225	المجموع	



شكل رقم (4-3) خصائص العينة حسب المسمى الوظيفي

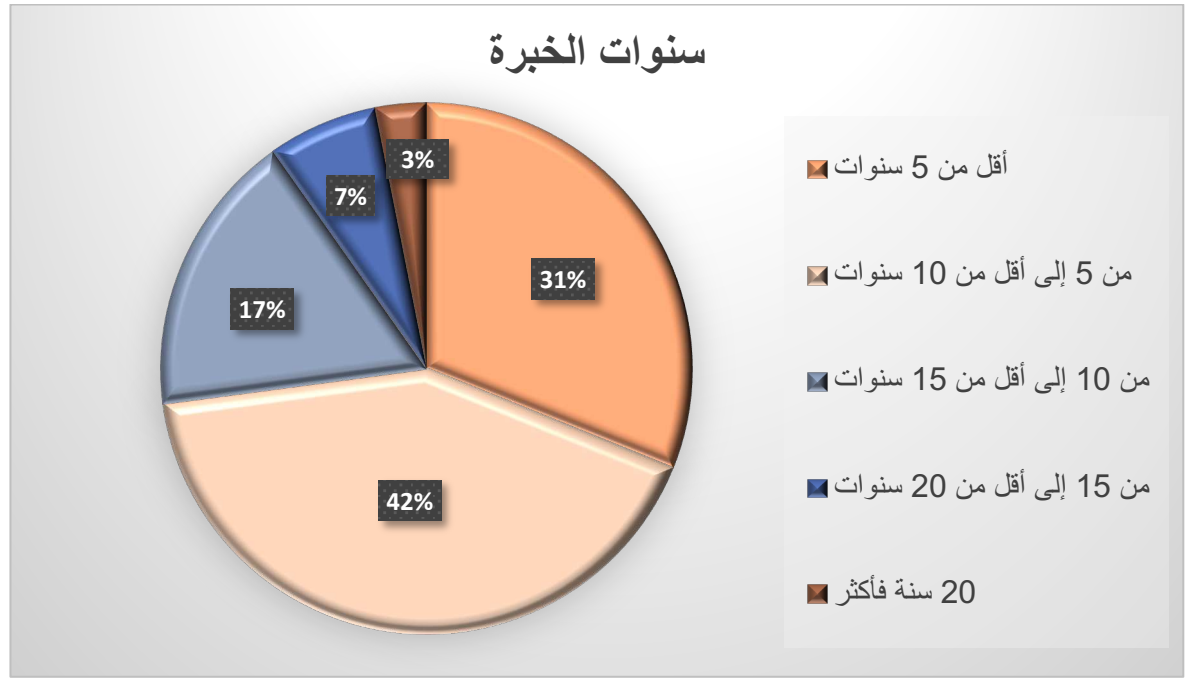
وبالنظر إلى الجدول (4-3) والشكل (4-3) أن أعلى نسبة من أفراد العينة كانت من فئة المحللين بنسبة (28.4%)، تليها فئة الأخصائيين بنسبة (20.4%)، ثم فئة الإداريين بنسبة (10.7%)، والمشرفين بنسبة (10.2%). بينما توزعت بقية النسب على مسميات وظيفية أخرى مثل المديرين، والمهندسين، والخبراء، وأعضاء هيئة التدريس بنسب متفاوتة.

ويشير هذا التوزيع إلى أن غالبية المشاركين يشغلون وظائف فنية وإدارية ذات ارتباط مباشر أو غير مباشر بالأنظمة التقنية وإجراءات الحوكمة، مما يعزز ملاءمة العينة لطبيعة الدراسة المتعلقة بإدارة المخاطر والأمن السيبراني داخل البيئة الجامعية، ويسهم في توفير بيانات تعكس الواقع المؤسسي بدرجة عالية من الدقة.

♦ خصائص عينة الدراسة حسب عدد سنوات الخبرة

جدول رقم (3-5) خصائص عينة الدراسة حسب عدد سنوات الخبرة

المتغير	فئات المتغير	العدد	النسبة المئوية %
سنوات الخبرة	أقل من 5 سنوات	70	31.1 %
	من 5 إلى أقل من 10 سنوات	94	41.8 %
	من 10 إلى أقل من 15 سنوات	39	17.3 %
	من 15 إلى أقل من 20 سنة	15	6.7 %
	20 سنة فأكثر	7	3.1 %
المجموع		225	100 %



شكل رقم (3-5) خصائص العينة حسب عدد سنوات الخبرة

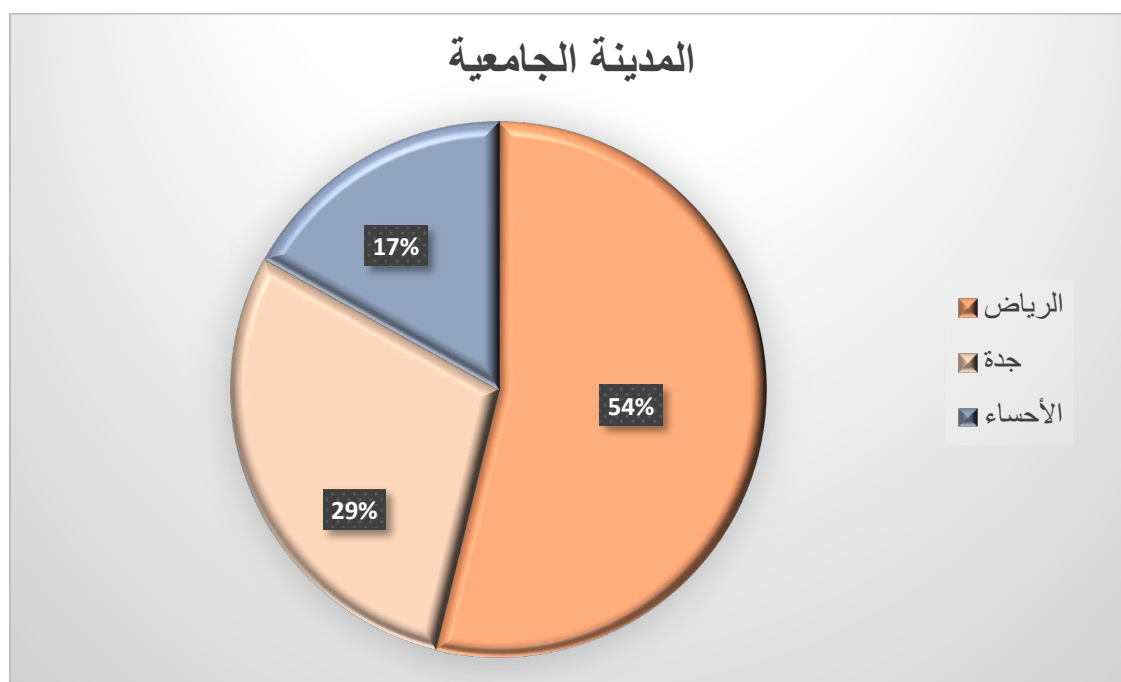
بالنظر إلى جدول رقم (3-5) وشكل (3-5) يلاحظ أن النسبة الأكبر من أفراد العينة تقع ضمن فئة من 5 إلى أقل من 10 سنوات خبرة بنسبة (41.8%)، تليها فئة أقل من 5 سنوات بنسبة (31.1%) ثم فئة من 10 إلى أقل من 15 سنة بنسبة (17.3%) في حين بلغت نسبة من لديهم خبرة من 15 إلى أقل من 20 سنة (6.7%)، ومن لديهم 20 سنة فأكثر (3.1%) ويشير هذا التوزيع إلى أن غالبية أفراد

العينة يتمتعون بخبرة مهنية متوسطة، مما يعكس مستوى جيداً من المعرفة بالأنظمة والإجراءات المؤسسية، ويعزز من مصداقية آرائهم فيما يتعلق بتطبيق ممارسات إدارة المخاطر وفاعلية الأمن السيبراني داخل الجامعة.

♦ خصائص عينة الدراسة حسب المدينة الجامعية

جدول رقم (3-6) خصائص عينة الدراسة حسب المدينة الجامعية

المتغير	فئات المتغير	العدد	النسبة المئوية %
المدينة الجامعية	الرياض	121	53.8%
	جدة	66	29.3%
	الأحساء	38	16.9%
المجموع		225	100 %



شكل رقم (3-6) خصائص العينة حسب المدينة الجامعية

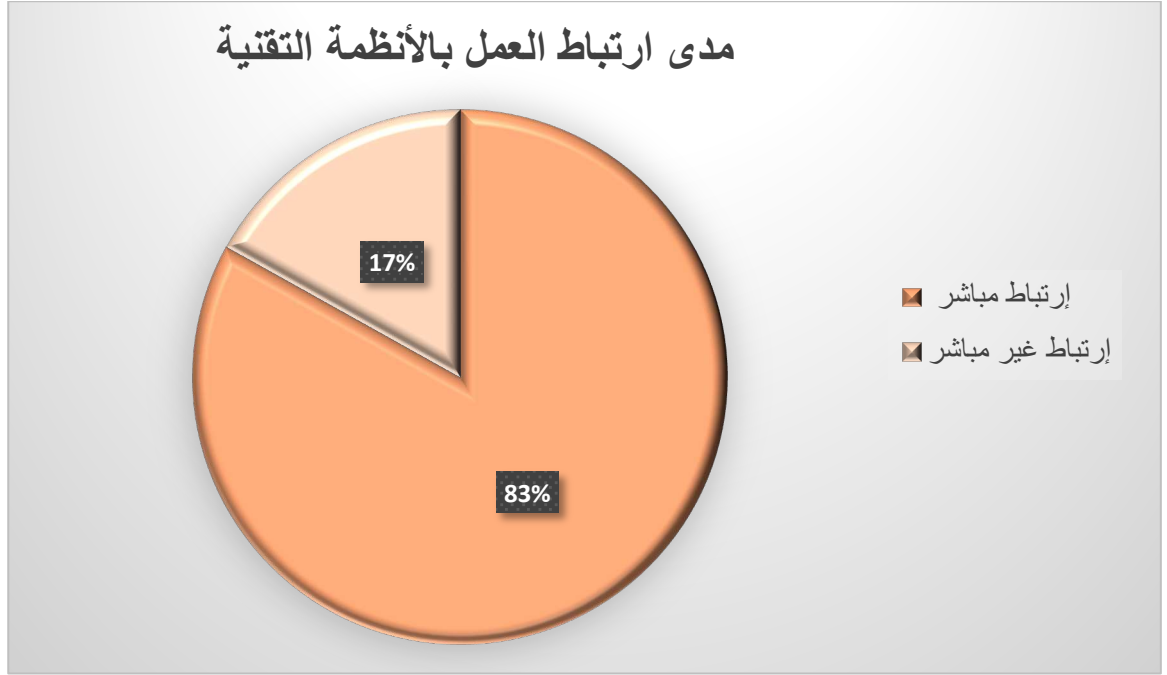
بالنظر إلى جدول رقم (3-6) وشكل (3-6) يلاحظ أن النسبة الأكبر من أفراد العينة كانت من المدينة الجامعية بالرياض بنسبة (53.8%)، تليها جدة بنسبة (29.3%)، ثم الأحساء بنسبة (16.9%) ويعكس هذا التوزيع التمثيل النسبي للفروع الجامعية المختلفة، كما يمكن تفسير ارتفاع نسبة المشاركين

من فرع الرياض بكونه المقر الرئيسي للجامعة والأكبر من حيث عدد الموظفين والإدارات، مما يؤدي بطبيعة الحال إلى زيادة عدد المستجيبين مقارنة ببقية الفروع ويجعل تمثيله في العينة أعلى من غيره.

♦ خصائص عينة الدراسة حسب مدى ارتباط العمل بالأنظمة التقنية

جدول رقم (3-7) خصائص عينة الدراسة حسب مدى ارتباط العمل بالأنظمة التقنية

المتغير	فئات المتغير	العدد	النسبة المئوية %
ارتباط العمل بالأنظمة التقنية	ارتباط مباشر	187	83.1 %
	ارتباط غير مباشر	38	16.9 %
المجموع		225	100 %



شكل رقم (3-7) خصائص العينة حسب مدى ارتباط العمل بالأنظمة التقنية

بالنظر إلى جدول رقم (3-7) وشكل (3-7) يلاحظ أن الغالبية العظمى من أفراد العينة يرتبط عملهم بالأنظمة التقنية ارتباطاً مباشراً بنسبة (83.1%)، في حين بلغت نسبة من يرتبط عملهم بالأنظمة التقنية ارتباطاً غير مباشر (16.9%) ويشير ذلك إلى أن معظم المشاركين يتعاملون بشكل مباشر مع الأنظمة التقنية أو الإجراءات ذات العلاقة، مما يعزز من ملاءمة آرائهم لطبيعة الدراسة المتعلقة بإدارة المخاطر والأمن السيبراني، ويزيد من موثوقية النتائج المستخلصة.

مصادر البيانات:

اعتمدت هذه الدراسة في جمع البيانات والمعلومات على مصدرين رئيسين:

أولاً: المصادر الثانوية:

قام الباحث بالرجوع إلى الكتب والمراجع العربية والأجنبية ذات العلاقة بموضوع الدراسة، إضافة الدراسات السابقة، والأبحاث والتقارير العلمية التي تناولت إدارة المخاطر والأمن السيبراني في المؤسسات التعليمية. كما تم الاستعانة بالأدبيات والمعايير واللوائح التنظيمية الوطنية والدولية، إضافة إلى المصادر العلمية المتاحة عبر مواقع الإنترنت المختلفة، وذلك بهدف تقديم الإطار النظري المتعلق بهذه الدراسة ودعم تفسير نتائجها

ثانياً: المصادر الأولية:

قام الباحث بإعداد استبانة كأداة رئيسة لجمع البيانات الأولية من أفراد عينة الدراسة من منسوبي جامعة الملك سعود بن عبد العزيز للعلوم الصحية، بهدف قياس مستوى تطبيق إدارة المخاطر وفاعلية الأمن السيبراني ومستوى التكامل المؤسسي بين الجهات ذات العلاقة، بما يسهم في اختبار فروض الدراسة والإجابة عن تساؤلاتها.

أداة جمع البيانات:

لجمع البيانات وتحقيق أهداف الدراسة، تم اعتماد أسلوب الاستبانة كأداة رئيسة للبحث، نظراً لملاءمتها لطبيعة الدراسة، وسهولة التطبيق على عدد كبير من المبحوثين، وانخفاض التكلفة، وإمكانية الحصول على بيانات كمية قابلة للتحليل الإحصائي بدقة وموضوعية.

وانطلاقاً من أهمية بناء أداة قياس تتسم بالصدق والثبات، فقد تم إعداد الاستبانة وفق خطوات علمية منهجية مع الحرص على أن تكون فقراتها واضحة ومحددة وخالية من الغموض، وتعكس المتغيرات الرئيسة للدراسة بصورة دقيقة، وذلك على النحو الآتي:

- خطوات إعداد أداة الدراسة

الخطوة الأولى: تحديد هدف الدراسة

تم تحديد الهدف الرئيسي للدراسة، والمتمثل في التعرف على دور ممارسات إدارة المخاطر المؤسسية في تعزيز فاعلية الأمن السيبراني داخل جامعة الملك سعود بن عبدالعزيز للعلوم الصحية، وقياس مستوى التكامل المؤسسي بين إدارة المخاطر ووحدة الأمن السيبراني.

الخطوة الثانية: تحديد مجالات القياس

تم تحديد مجالات القياس في جزأين رئيسين:

أولاً: البيانات الديموغرافية

وشملت: (الجنس، والمستوى التعليمي، والمسمى الوظيفي، وعدد سنوات الخبرة، المدينة الجامعية ، ومدى الارتباط بالأنظمة التقنية).

ثانياً: محاور الدراسة الرئيسة

وتضمنت ستة محاور هي:

- المحور الأول: ممارسات إدارة المخاطر المؤسسية. ويتكون من (8) فقرات.
- المحور الثاني: فاعلية الأمن السيبراني ويتكون من (6) فقرات.
- المحور الثالث: التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني ويتكون من (3) فقرات.
- المحور الرابع: التحديات التنظيمية والتقنية ويتكون من (3) فقرات.
- المحور الخامس: الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر ويتكون من (3) فقرات.
- المحور السادس: تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني ويتكون من (3) فقرات.

الخطوة الثالثة: صياغة فقرات الأداة في صورتها الأولية

تمت صياغة فقرات الاستبانة بالاستناد إلى الإطار النظري والدراسات السابقة ذات الصلة بمجالي إدارة المخاطر والأمن السيبراني، مع مراعاة ملاءمة الفقرات لبيئة الجامعة، وارتباطها بالتعريفات الإجرائية لمتغيرات الدراسة.

الخطوة الرابعة: تحديد مقياس الاستجابة

تم اعتماد مقياس ليكرت الخماسي لتدرج الاستجابات على فقرات الدراسة وفق الترتيب الآتي:

❖ لا أوافق بشدة = (1)

❖ لا أوافق = (2)

❖ محايد = (3)

❖ أوافق = (4)

❖ أوافق بشدة = (5)

الخطوة الخامسة: إعداد تعليمات الاستبانة

تم إعداد تعليمات واضحة في مقدمة الاستبانة، تضمنت توضيح هدف الدراسة، والتأكيد على سرية المعلومات، واستخدام البيانات لأغراض البحث العلمي فقط، إضافة إلى شرح طريقة الإجابة على الفقرات.

الخطوة السادسة: إخراج الاستبانة في صورتها النهائية وتطبيقها

بعد اعتماد الاستبانة بصورتها النهائية، تم تحويلها إلى استمارة إلكترونية عبر (Google Forms)، ومن ثم إرسال الرابط الإلكتروني إلى أفراد العينة المستهدفة عبر البريد الإلكتروني، مع متابعة عملية الاستجابة لضمان تحقيق العدد المطلوب من المشاركات.

حدود الدراسة:

1-الحدود الموضوعية:

تركز هذه الدراسة على تحليل العلاقة بين إدارة المخاطر والأمن السيبراني في بيئة الجامعات السعودية، من خلال تقييم مستوى التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني، ودراسة أثر هذا التكامل في دعم الحوكمة المؤسسية وحماية الأصول المعلوماتية. وتستبعد الدراسة الجوانب التقنية البحتة التي لا ترتبط بالإدارة أو السياسات والإجراءات التنظيمية.

2-الحدود المكانية:

تقتصر هذه الدراسة على جامعة الملك سعود بن عبد العزيز للعلوم الصحية في المملكة العربية السعودية، بوصفها نموذجًا تطبيقيًا يمثل إحدى الجامعات السعودية التي تبنت سياسات رسمية في مجال إدارة المخاطر والأمن السيبراني.

3-الحدود الزمانية:

تشمل الدراسة الفترة الزمنية للعام الأكاديمي 2024-2025م، وهي المدة التي يتم خلالها جمع البيانات الميدانية وتحليل السياسات والوثائق التنظيمية ذات العلاقة بموضوع الدراسة.

4-الحدود البشرية:

تم تطبيق الدراسة على جميع منسوبي جامعة الملك سعود بن عبد العزيز للعلوم الصحية العاملين في الإدارات ذات العلاقة بموضوع الدراسة ارتباطًا مباشرًا أو غير مباشر، وتشمل الموظفين، وأعضاء هيئة التدريس.

الصدق والثبات لاستبانة الدراسة (أداة الدراسة)

أولاً: اختبار صدق أداة الدراسة (Validity)

1. الصدق الظاهري (صدق المحكمين)

تم التحقق من صدق أداة الدراسة (الاستبانة) للتأكد من صلاحيتها لقياس المتغيرات التي أُعدت من أجلها، ومدى تمثيلها لكافة أبعاد الدراسة بصورة دقيقة وشاملة. كما تم التأكد من وضوح صياغة الفقرات وسلامتها اللغوية، ومدى ملاءمتها لطبيعة مجتمع الدراسة، بحيث تكون مفهومة للمستجيبين وخالية من الغموض أو الالتباس وقد تم ذلك من خلال الإجراءات التالية:

- عرض الأداة على عدد من المحكمين المتخصصين مجال إدارة المخاطر والأمن السيبراني.
- الأخذ بملاحظاتهم فيما يتعلق بإعادة الصياغة أو الحذف أو الإضافة.
- اعتماد النسخة النهائية بعد إجراء التعديلات المقترحة.

وبذلك أصبحت الأداة صالحة للتطبيق الميداني.

2. صدق الاتساق الداخلي لأداة الدراسة (Internal Consistency)

تم التحقق من صدق الاتساق الداخلي لأداة الدراسة باستخدام معامل ارتباط بيرسون (Pearson Correlation Coefficient)، وذلك من خلال تطبيقها على عينة استطلاعية مكونة من (50) موظفًا في جامعة الملك سعود بن عبد العزيز للعلوم الصحية في المملكة العربية السعودية تم اختيارهم عشوائيًا من مجتمع الدراسة وقد تم حساب معامل الارتباط بين كل عبارة من عبارات الاستبانة والدرجة الكلية للمحور الذي تنتمي إليه بعد استبعادها منه، بهدف التأكد من مدى اتساق العبارات داخليًا وارتباطها بالبُعد الذي نقيسه.

ويعد هذا الإجراء من الأساليب الإحصائية المعتمدة للتحقق من تجانس فقرات المحور الواحد ومدى تمثيلها للمفهوم المراد قياسه ويعرض الجدول أدناه النتائج:

الجدول رقم (3-8) صدق الاتساق الداخلي لأداة الدراسة

المحاور	رقم العبارة	معامل الارتباط
المحور الأول	1	0.858
	2	0.748
	3	0.637
	4	0.532
	5	0.846
	6	0.886
	7	0.843
	8	0.464
المحور الثاني	1	0.406
	2	0.568
	3	0.847
	4	0.715
	5	0.500
	6	0.421
المحور الثالث	1	0.551
	2	0.355
	3	0.389
المحور الرابع	1	0.770
	2	0.846
	3	0.822
المحور الخامس	1	0.776
	2	0.872
	3	0.559
المحور السادس	1	0.908
	2	0.918
	3	0.724

بالنظر إلى الجدول أعلاه يتضح أن معاملات ارتباط بيرسون بين عبارات كل محور والدرجة الكلية له جاءت جميعها موجبة ودالة إحصائية، مما يعكس تحقق صدق الاتساق الداخلي لأداة الدراسة بدرجة عالية. فقد تراوحت معاملات الارتباط في المحور الأول بين (0.464 – 0.886)، وفي المحور الثاني بين (0.406 – 0.847)، وفي المحور الثالث بين (0.355 – 0.551)، كما تراوحت في المحور الرابع بين (0.770 – 0.846)، وفي المحور الخامس بين (0.559 – 0.872)، وفي المحور السادس بين (0.724 – 0.918). وتشير هذه النتائج إلى وجود ارتباط إيجابي واضح بين العبارات ومحاورها، ويُستدل منها أن جميع قيم المحاور جاءت موجبة ودالة عند مستوى دلالة إحصائية (0.01)، مما يدل على قوة العلاقة بين فقرات الاستبيان وأبعادها. وبناءً على ذلك، يتبين أن أداة الدراسة تتمتع بدرجة قوية من صدق الاتساق الداخلي، وأن عباراتها تقيس المتغيرات التي صُممت من أجلها بدقة وموضوعية، بما يعزز من موثوقية نتائج الدراسة.

ثانياً: اختبار ثبات أداة الدراسة (Reliability)

تم قياس ثبات أداة الدراسة باستخدام معامل ألفا كرونباخ (Cronbach's Alpha) وذلك من خلال تطبيقها على العينة الاستطلاعية المكونة من (50) موظفًا في جامعة الملك سعود بن عبد العزيز للعلوم الصحية في المملكة العربية السعودية وجاءت النتائج كما في الجدول التالي:

جدول رقم (3-9): معامل الثبات ألفا كرونباخ لمحاور الاستبانة ولأداة ككل

م.	المحاور	عدد العبارة	معامل ألفا كرونباخ
1	ممارسات إدارة المخاطر المؤسسية	8	0.969
2	فاعلية الأمن السيبراني	6	0.961
3	التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني	3	0.852
4	التحديات التنظيمية والتقنية	3	0.927
5	الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر	3	0.947
6	تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني	3	0.998
	الثبات الكلي للأداة	26	0.984

وقد أظهرت النتائج أن معاملات ألفا كرونباخ لجميع المحاور جاءت مرتفعة، حيث بلغ معامل الثبات للمحور الأول (0.969)، وللمحور الثاني (0.961)، وللمحور الثالث (0.852)، وللمحور الرابع (0.927)، وللمحور الخامس (0.947)، وللمحور السادس (0.998) الداخلي كما بلغ معامل الثبات الكلي لفقرات الاستبانة (0.984)، وهي قيمة مرتفعة جدًا وفق المعايير الإحصائية المعتمدة إذ تتجاوز الحد المقبول إحصائيًا (0.70) مما يدل على تمتع أداة الدراسة بدرجة عالية من الثبات والاتساق الداخلي وأنها صالحة للغرض الذي صممت من أجله الأمر الذي يعزز الثقة في النتائج المستخلصة منها وإمكانية الاعتماد عليها عند تطبيقها على العينة النهائية للدراسة.

الأداة المستخدمة للتحليل الإحصائي:

بغرض الإجابة عن أسئلة الدراسة واختبار صحة فرضياتها تم استخدام برنامج **الحزمة الإحصائية للعلوم الاجتماعية (IBM SPSS Statistics)** ، وذلك لما يتميز به من دقة وموثوقية في تحليل البيانات الكمية واختبار الفرضيات في الدراسات الاجتماعية والإدارية وقد تم استخدام مجموعة من الأساليب الإحصائية التي تتناسب مع طبيعة الدراسة وأهدافها، وذلك على النحو الآتي:

1. **الإحصاء الوصفي (Descriptive Statistics) :** تم استخدام التكرارات والنسب المئوية لوصف الخصائص الديموغرافية لعينة الدراسة (الجنس-المستوى التعليمي- المسمى الوظيفي- عدد سنوات الخبرة - المدينة الجامعية -مدى ارتباط عملك بالأنظمة التقنية)، كما تم حساب المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لتحديد مستوى استجابات أفراد العينة على محاور الدراسة وفق مقياس ليكرت الخماسي.
2. **معامل ألفا كرونباخ (Cronbach's Alpha) :** تم استخدامه للتحقق من درجة الاتساق الداخلي لفقرات الاستبانة وقياس ثبات الأداة وذلك للتأكد من مدى اتساق فقرات كل محور مع بعضها البعض وقياس مدى موثوقية الأداة المستخدمة في جمع البيانات.
3. **معامل ارتباط بيرسون (Pearson Correlation Coefficient) :** تم استخدامه لقياس قوة واتجاه العلاقة بين متغيرات الدراسة واختبار فرضياتها المتعلقة بوجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر ومحاور فاعلية الأمن السيبراني المختلفة.

خاتمة الفصل:

تناول هذا الفصل منهجية الدراسة والإجراءات العلمية التي تم اتباعها لتنفيذ البحث حيث تم توضيح تصميم البحث والمنهج المستخدم، والمتمثل في المنهج الوصفي التحليلي لملاءمته لطبيعة الدراسة وأهدافها كما تم تحديد مجتمع البحث المتمثل في منسوبي جامعة الملك سعود بن عبدالعزيز للعلوم الصحية، إضافة إلى تحديد عينة الدراسة وطريقة اختبارها وعرض أداة الدراسة المتمثلة في الاستبانة، وبيان خطوات إعدادها وآلية توزيعها وجمع البيانات إلى جانب عرض الخصائص الديموغرافية لعينة الدراسة مثل الجنس، والمستوى التعليمي، والمسمى الوظيفي، وعدد سنوات الخبرة، كما تم توضيح الأساليب الإحصائية التي تم استخدامها في تحليل البيانات واختبار فرضيات الدراسة .

الفصل الرابع النتائج والتوصيات

مقدمة:

يهدف هذا الفصل إلى عرض وتحليل البيانات التي تم جمعها من خلال أداة الدراسة (الاستبانة) وذلك بهدف الوصول إلى فهم علمي دقيق لطبيعة العلاقة بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني في الجامعات السعودية. ويأتي هذا الفصل استكمالاً للإطار النظري والدراسات السابقة التي تناولت موضوع الدراسة، حيث يسعى إلى توظيف البيانات الميدانية للتحقق من فرضيات الدراسة والإجابة عن تساؤلاتها، بما يسهم في تقديم نتائج علمية يمكن الاستفادة منها في تعزيز ممارسات إدارة المخاطر ودعم فاعلية الأمن السيبراني في المؤسسات التعليمية، وقد تم تحليل البيانات باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) من خلال توظيف الأساليب الإحصائية الوصفية والاستدلالية المناسبة لطبيعة متغيرات الدراسة، وذلك للتحقق من مدى ملاءمة البيانات وإجراء الاختبارات الإحصائية اللازمة للوصول إلى نتائج علمية دقيقة.

ويتضمن هذا الفصل عرض نتائج التحليل الوصفي لمحاور الدراسة بهدف التعرف على مستوى استجابات أفراد العينة لكل محور من محاور الدراسة، يلي ذلك اختبار فرضيات الدراسة باستخدام الأساليب الإحصائية المناسبة مع تقديم تفسير علمي للنتائج التي تم التوصل إليها، كما يتم في نهاية الفصل مناقشة النتائج وتحليلها في ضوء الإطار النظري والدراسات السابقة بما يسهم في إبراز أوجه الاتفاق أو الاختلاف بين نتائج الدراسة الحالية وما توصلت إليه الدراسات السابقة، ويساعد في تقديم فهم أكثر شمولاً لموضوع الدراسة.

تحليل البيانات

يعرض تحليل البيانات نتائج التحليل الإحصائي لمتغيرات الدراسة وأبعادها، وذلك من خلال حساب المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية ومستوى الاستجابة لكل عبارة من عبارات محاور الدراسة إضافة إلى حساب الدرجة الكلية لكل محور تمهيداً لاختبار فرضيات الدراسة.

وفيما يلي عرض تفصيلي لنتائج التحليل الإحصائي لمحاور الدراسة، بما يسهم في تفسير البيانات بشكل علمي دقيق يدعم الوصول إلى استنتاجات موضوعية.

المحور الأول: ممارسات إدارة المخاطر المؤسسية

جدول رقم (4-1): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير ممارسات إدارة المخاطر المؤسسية

م.	العبارات	المتوسط الحسابي	الانحراف المعياري	النتيجة	الوزن النسبي	المستوى	الرتبة
1	تقوم جامعة الملك سعود بن عبد العزيز للعلوم الصحية بتحديد المخاطر السيبرانية المرتبطة بالأنظمة الأكاديمية والإدارية بشكل واضح	4.63	0.85	موافق بشدة	92.6 %	مرتفع جداً	1
2	يتم توثيق المخاطر السيبرانية داخل الجامعة ضمن سجلات رسمية معتمدة	4.61	0.88	موافق بشدة	92.2 %	مرتفع جداً	2
3	يتم تحليل احتمالية حدوث المخاطر السيبرانية وتأثيرها قبل اتخاذ القرارات	3.97	0.81	موافق	79.4 %	مرتفع	7
4	تعتمد جامعة الملك سعود بن عبد العزيز للعلوم الصحية على معايير واضحة لتصنيف المخاطر السيبرانية حسب درجة الخطورة	3.97	0.77	موافق	79.4 %	مرتفع	8
5	يتم تقييم المخاطر السيبرانية وفق منهجية موحدة داخل جامعة الملك سعود بن عبد العزيز للعلوم الصحية	4.50	0.96	موافق بشدة	90.0 %	مرتفع جداً	4
6	يتم ربط نتائج تقييم المخاطر بالأهداف الاستراتيجية للجامعة	4.55	0.88	موافق بشدة	91.0 %	مرتفع جداً	3
7	تتوفر خطط استجابة معتمدة للتعامل مع الحوادث السيبرانية بدرجة كافية	4.50	0.89	موافق بشدة	90.0 %	مرتفع جداً	5
8	يتم تحديث سياسات الأمن السيبراني وإدارة المخاطر في الجامعة بناءً على نتائج المراجعة والتقييم الدوري	4.09	0.77	موافق	81.8 %	مرتفع	6
الدرجة الكلية للمحور الأول		4.35	0.85	موافق بشدة	87.1 %	مرتفع جداً	

يتضح من خلال نتائج الجدول رقم (4-1) اعلاه لمحور ممارسات إدارة المخاطر المؤسسية أن المتوسط الحسابي الكلي للمحور بلغ (4.35) بانحراف معياري قدره (0.85)، وبوزن نسبي بلغ (87.1%)، وجاءت النتيجة بدرجة (موافق بشدة) وبمستوى (مرتفع جداً) وتشير هذه النتيجة إلى أن مستوى تطبيق ممارسات إدارة المخاطر المؤسسية في جامعة الملك سعود بن عبد العزيز للعلوم الصحية يُعد مرتفعاً جداً من وجهة نظر أفراد العينة مما يعكس وجود إطار مؤسسي منظم لإدارة المخاطر السيبرانية داخل الجامعة، ويتوافق مع متطلبات الحوكمة المؤسسية ومعايير تعزيز الأمن السيبراني في مؤسسات التعليم العالي.

فيما يتعلق بالعبارات الفردية، فقد جاءت العبارة الأولى في المرتبة الأولى بمتوسط حسابي بلغ (4.63) ووزن نسبي (92.6%)، وبمستوى (مرتفع جداً) مما يدل على وضوح عملية تحديد المخاطر السيبرانية المرتبطة بالأنظمة الأكاديمية والإدارية. كما جاءت العبارة الثانية في المرتبة الثانية بمتوسط حسابي (4.61) ووزن نسبي (92.2%)، وهو ما يعكس انتظام عملية توثيق المخاطر السيبرانية ضمن سجلات رسمية معتمدة، بما يعزز من كفاءة عمليات المتابعة والمراجعة، وجاءت العبارة السادسة في المرتبة الثالثة بمتوسط حسابي (4.55)، تليها العبارة الخامسة و العبارة السابعة بمتوسط (4.50) لكل منهما، مما يشير إلى قوة الربط بين نتائج تقييم المخاطر والأهداف الاستراتيجية للجامعة، ووجود منهجية موحدة لتقييم المخاطر، إضافة إلى توافر خطط استجابة معتمدة للحوادث السيبرانية أما العبارة الثامنة فقد بلغ متوسطها الحسابي (4.09) وبوزن نسبي (81.8%)، وجاءت بمستوى (مرتفع) مما يدل على وجود تحديث دوري لسياسات الأمن السيبراني وإدارة المخاطر بناءً على نتائج المراجعة والتقييم، في حين سجلت العبارتان الثالثة والرابعة أدنى متوسط حسابي بلغ (3.97) لكل منهما، وبوزن نسبي (79.4%)، إلا أنهما بقيتا ضمن مستوى (مرتفع) مما يشير إلى أن تحليل احتمالية المخاطر وتصنيفها وفق معايير واضحة يتم تطبيقهما بدرجة جيدة وإن كانا يمثلان جانباً فنياً يتطلب مستوى أعلى من التحليل والتقدير مقارنة بالممارسات الإجرائية الأخرى.

وبوجه عام، تؤكد نتائج هذا المحور أن الجامعة تطبق ممارسات إدارة المخاطر المؤسسية بدرجة عالية من التنظيم والاتساق، مع تركيز واضح على التحديد والتوثيق والربط الاستراتيجي، وهو ما يعزز من فاعلية منظومة إدارة المخاطر السيبرانية داخل المؤسسة

المحور الثاني: فاعلية الأمن السيبراني

جدول رقم (4-2): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير فاعلية الأمن السيبراني

م.م	العبارات	المتوسط الحسابي	الانحراف المعياري	النتيجة	الوزن النسبي	المستوى	الرتبة
1	تحتل البيانات الأكاديمية والبحثية بحماية كافية داخل جامعة الملك سعود بن عبد العزيز للعلوم الصحية	4.67	0.78	موافق بشدة	93.4 %	مرتفع جداً	2
2	يتم تحديد وتنظيم صلاحيات دخول المستخدمين إلى الأنظمة التقنية بما يتناسب مع مهامهم الوظيفية	4.67	0.75	موافق بشدة	93.4 %	مرتفع جداً	3
3	تُطبق جامعة الملك سعود بن عبد العزيز للعلوم الصحية ضوابط واضحة لضمان سرية وسلامة البيانات	4.60	0.82	موافق بشدة	92.0 %	مرتفع جداً	4
4	توجد آلية واضحة للإبلاغ عن الحوادث السيبرانية داخل الجامعة	4.44	0.95	موافق بشدة	88.8 %	مرتفع جداً	5
5	تُطبق جامعة الملك سعود بن عبد العزيز للعلوم الصحية إجراءات وقائية للحد من المخاطر السيبرانية قبل وقوعها	4.15	0.79	موافق	83.0 %	مرتفع	6
6	تسهم سياسات الأمن السيبراني في ضمان استمرارية الخدمات الأكاديمية والإدارية	4.67	0.80	موافق بشدة	93.4 %	مرتفع جداً	1
	الدرجة الكلية للمحور الثاني	4.53	0.81	موافق بشدة	90.6 %	مرتفع جداً	

يتضح من خلال نتائج الجدول رقم (4-2) اعلاه لمحور فاعلية الأمن السيبراني أن المتوسط الحسابي الكلي للمحور بلغ (4.53) بانحراف معياري قدره (0.81)، وبوزن نسبي بلغ (90.6%)، وجاءت النتيجة بدرجة (موافق بشدة) وبمستوى (مرتفع جداً) وتشير هذه النتيجة إلى أن مستوى فاعلية الأمن السيبراني في جامعة الملك سعود بن عبد العزيز للعلوم الصحية يُعد مرتفعاً جداً من وجهة نظر أفراد العينة، مما يعكس وجود منظومة أمنية متكاملة تسهم في حماية البيانات والأنظمة الرقمية وضمان استمرارية الخدمات الأكاديمية والإدارية.

فيما يتعلق بالعبارات الفردية، جاءت العبارة السادسة في المرتبة الأولى بمتوسط حسابي بلغ (4.67) ووزن نسبي (93.4%)، وبمستوى (مرتفع جداً) مما يدل على أن سياسات الأمن السيبراني تسهم بدرجة كبيرة في ضمان استمرارية الخدمات الأكاديمية والإدارية داخل الجامعة، كما جاءت العبارة الأولى في المرتبة الثانية بمتوسط حسابي (4.67) ووزن نسبي (93.4%)، وهو ما يعكس ارتفاع مستوى حماية البيانات الأكاديمية والبحثية داخل الجامعة، وجاءت العبارة الثانية في المرتبة الثالثة بمتوسط حسابي (4.67) ووزن نسبي (93.4%)، مما يشير إلى وجود تنظيم دقيق لصلاحيات دخول المستخدمين إلى الأنظمة التقنية بما يتناسب مع مهامهم الوظيفية، أما العبارة الثالثة فقد بلغ متوسطها الحسابي (4.60) وبوزن نسبي (92.0%)، وجاءت بمستوى (مرتفع جداً) مما يدل على تطبيق ضوابط واضحة لضمان سرية وسلامة البيانات، وجاءت العبارة الرابعة بمتوسط حسابي (4.44) ووزن نسبي (88.8%)، مما يشير إلى وجود آلية واضحة للإبلاغ عن الحوادث السيبرانية داخل الجامعة، في حين سجلت العبارة الخامسة أدنى متوسط حسابي بلغ (4.15) وبوزن نسبي (83.0%)، وجاءت بمستوى (مرتفع) مما يدل على تطبيق إجراءات وقائية للحد من المخاطر السيبرانية قبل وقوعها، وإن كانت بدرجة أقل نسبياً مقارنة ببقية الممارسات، وتدل نتائج هذا المحور أن فاعلية الأمن السيبراني في الجامعة تتميز بدرجة عالية من الكفاءة والاتساق مع تركيز واضح على حماية البيانات، تنظيم الصلاحيات، ضمان الاستمرارية، وتطبيق الضوابط الوقائية، مما يعزز من جاهزية المؤسسة للتعامل مع التحديات السيبرانية.

المحور الثالث: التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني

جدول رقم (4-3): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني

م.	العبارات	المتوسط الحسابي	الانحراف المعياري	النتيجة	الوزن النسبي	المستوى	الرتبة
1	يوجد تنسيق واضح بين إدارة المخاطر ووحدة الأمن السيبراني داخل الجامعة	3.49	0.81	موافق	89.8 %	مرتفع	2
2	يتم تبادل المعلومات المتعلقة بالمخاطر السيبرانية بين إدارة المخاطر، ووحدة الأمن السيبراني، وإدارة تقنية المعلومات بشكل منتظم	3.37	0.79	محايد	67.4 %	متوسط	3

3	يساعد التعاون بين إدارة المخاطر ووحدة الأمن السيبراني في سرعة وكفاءة الاستجابة للحوادث الرقمية	4.52	0.87	موافق بشدة	90.4 %	مرتفع جداً	1
الدرجة الكلية للمحور الثالث		3.79	0.82	موافق	75.8 %	مرتفع	

يتضح من خلال نتائج الجدول رقم (4-3) اعلاه لمحور التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني أن المتوسط الحسابي الكلي للمحور بلغ (3.79) بانحراف معياري قدره (0.82)، ووزن نسبي بلغ (75.8%)، وجاءت النتيجة بدرجة (موافق) وبمستوى (مرتفع) وتشير هذه النتيجة إلى أن مستوى التكامل المؤسسي بين إدارة المخاطر ووحدة الأمن السيبراني داخل الجامعة يُعد مرتفعاً بشكل عام، إلا أنه أقل نسبياً مقارنة بالمحورين السابقين، مما يدل على وجود ممارسات تكاملية قائمة لكنها قد تحتاج إلى مزيد من التعزيز والتطوير.

فيما يتعلق بالعبارات الفردية جاءت العبارة الثالثة في المرتبة الأولى بمتوسط حسابي بلغ (4.52) ووزن نسبي (90.4%)، وبمستوى (مرتفع جداً) مما يدل على إدراك أفراد العينة لأهمية التعاون بين إدارة المخاطر ووحدة الأمن السيبراني في تعزيز سرعة وكفاءة الاستجابة للحوادث الرقمية داخل الجامعة، أما العبارة الأولى في المرتبة الثانية بمتوسط حسابي (3.49) ووزن نسبي (89.8%)، وبمستوى (مرتفع) مما يشير إلى وجود تنسيق واضح بين إدارة المخاطر ووحدة الأمن السيبراني داخل الجامعة، وإن كان بدرجة أقل من مستوى الإدراك المرتبط بالمعوقات التنظيمية و العبارة الثانية فقد جاءت في المرتبة الثالثة بمتوسط حسابي (3.37) ووزن نسبي (67.4%)، وجاءت بدرجة (محايد) وبمستوى (متوسط) مما يشير إلى أن تبادل المعلومات المتعلقة بالمخاطر السيبرانية بين إدارة المخاطر ووحدة الأمن السيبراني وإدارة تقنية المعلومات لا يتم بشكل منتظم أو بالدرجة المأمولة من وجهة نظر أفراد العينة وتعكس هذه النتائج وجود مستوى جيد من التنسيق المؤسسي، إلا أن جانب تبادل المعلومات يمثل نقطة تحتاج إلى مزيد من التنظيم والوضوح، لما له من دور محوري في تعزيز التكامل بين الجهات المعنية بالأمن السيبراني وإدارة المخاطر.

المحور الرابع: التحديات التنظيمية والتقنية

جدول رقم (4-4): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير التحديات التنظيمية والتقنية

م.	العبارات	المتوسط الحسابي	الانحراف المعياري	النتيجة	الوزن النسبي	المستوى	الرتبة
1	تشكل قلة الوعي السيبراني لدى بعض الموظفين تحدياً مؤثراً على فاعلية الأمن السيبراني في الجامعة	4.76	0.71	موافق بشدة	95.2 %	مرتفع جداً	1
2	تشكل محدودية الكوادر البشرية المتخصصة عائقاً أمام تطبيق الأمن السيبراني بدرجة ملحوظة	4.73	0.73	موافق بشدة	94.6 %	مرتفع جداً	2
3	تؤثر التعقيدات التنظيمية والإجرائية على فاعلية تطبيق سياسات الأمن السيبراني في الجامعة	4.65	0.84	موافق بشدة	93.0 %	مرتفع جداً	3
	الدرجة الكلية للمحور الرابع	4.71	0.76	موافق بشدة	94.2 %	مرتفع جداً	

يتضح من خلال نتائج الجدول رقم (4-4) اعلاه لمحور التحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني أن المتوسط الحسابي الكلي للمحور بلغ (4.71) بانحراف معياري قدره (0.76)، وبوزن نسبي بلغ (94.2%)، وجاءت النتيجة بدرجة (موافق بشدة) وبمستوى (مرتفع جداً) وتشير هذه النتيجة إلى أن أفراد العينة يدركون بدرجة كبيرة وجود مجموعة من التحديات التنظيمية والتقنية التي قد تؤثر على فاعلية تطبيق الأمن السيبراني داخل جامعة الملك سعود بن عبد العزيز للعلوم الصحية، مما يعكس أهمية معالجة هذه التحديات لتعزيز مستوى الحماية السيبرانية داخل الجامعة.

وفيما يتعلق بالعبارات الفردية جاءت العبارة الأولى في المرتبة الأولى بمتوسط حسابي بلغ (4.76) ووزن نسبي (95.2%)، وبمستوى (مرتفع جداً) مما يدل على أن قلة الوعي السيبراني لدى بعض الموظفين تُعد من أبرز التحديات التي قد تؤثر على فاعلية الأمن السيبراني داخل الجامعة وجاءت العبارة الثانية في المرتبة الثانية بمتوسط حسابي (4.73) ووزن نسبي (94.6%)، وبمستوى (مرتفع جداً) مما يشير إلى أن محدودية الكوادر البشرية المتخصصة في مجال الأمن السيبراني تشكل عائقاً ملحوظاً أمام تطبيق متطلبات الأمن السيبراني بكفاءة، أما العبارة الثالثة فقد جاءت في المرتبة الثالثة بمتوسط حسابي (4.65) ووزن نسبي (93.0%)، وبمستوى (مرتفع جداً) مما يدل على أن التعقيدات التنظيمية والإجرائية

قد تؤثر على فاعلية تطبيق سياسات الأمن السيبراني داخل الجامعة، وتعكس هذه النتائج إدراكاً مرتفعاً لدى أفراد العينة لوجود تحديات متعددة قد تؤثر على فاعلية تطبيق الأمن السيبراني، ويأتي في مقدمتها ضعف الوعي السيبراني لدى بعض الموظفين، إلى جانب محدودية الكوادر المتخصصة، والتعقيدات التنظيمية والإجرائية، الأمر الذي يؤكد أهمية تعزيز برامج التوعية والتدريب، وتطوير الكفاءات البشرية، وتبسيط الإجراءات التنظيمية بما يساهم في رفع مستوى فاعلية الأمن السيبراني داخل الجامعة.

المحور الخامس: الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر

جدول رقم (4-5): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر

م.م	العبارات	المتوسط الحسابي	الانحراف المعياري	النتيجة	الوزن النسبي	المستوى	الرتبة
1	تتسم سياسات الأمن السيبراني وإدارة المخاطر في الجامعة بالوضوح والشمول الكافي لتنظيم العمل المؤسسي	4.65	0.85	موافق بشدة	% 93.0	مرتفع جداً	2
2	يتم تطبيق سياسات الأمن السيبراني وإدارة المخاطر في الجامعة بدرجة عالية من الالتزام عبر الإدارات المعنية	4.61	0.87	موافق بشدة	% 92.2	مرتفع جداً	3
3	تساهم سياسات الأمن السيبراني وإدارة المخاطر في توحيد الإجراءات وتحديد الأدوار والمسؤوليات داخل الجامعة بشكل فعال	4.72	0.77	موافق بشدة	% 94.4	مرتفع جداً	1
الدرجة الكلية للمحور الخامس		4.66	0.83	موافق بشدة	% 93.2	مرتفع جداً	

يتضح من خلال نتائج الجدول رقم (4-5) اعلاه لمحور فاعلية الإطار التنظيمي والسياسات والإجراءات المعتمدة في الأمن السيبراني أن المتوسط الحسابي الكلي للمحور بلغ (4.66) بانحراف معياري قدره (0.83)، وبوزن نسبي بلغ (%93.2)، وجاءت النتيجة بدرجة (موافق بشدة) وبمستوى (مرتفع جداً) وتشير هذه النتيجة إلى أن سياسات الأمن السيبراني وإدارة المخاطر في جامعة الملك سعود

بن عبد العزيز للعلوم الصحية تتسم بدرجة عالية من الفاعلية والوضوح والتنظيم، مما يعكس وجود إطار تنظيمي متكامل يسهم في تنظيم العمل المؤسسي وتعزيز مستوى الحوكمة في مجال الأمن السيبراني.

وفيما يتعلق بالعبارات الفردية جاءت العبارة الثالثة في المرتبة الأولى بمتوسط حسابي بلغ (4.72) ووزن نسبي (94.4%)، وبمستوى (مرتفع جداً) مما يدل على أن سياسات الأمن السيبراني وإدارة المخاطر تسهم بدرجة كبيرة في توحيد الإجراءات وتحديد الأدوار والمسؤوليات داخل الجامعة بشكل فعال الأمر الذي يعزز من وضوح المهام التنظيمية ويحد من التداخل في المسؤوليات، وجاءت العبارة الأولى في المرتبة الثانية بمتوسط حسابي (4.65) ووزن نسبي (93.0%)، وبمستوى (مرتفع جداً) مما يشير إلى أن سياسات الأمن السيبراني وإدارة المخاطر تتسم بالوضوح والشمول الكافي لتنظيم العمل المؤسسي داخل الجامعة أما العبارة الثانية فقد جاءت في المرتبة الثالثة بمتوسط حسابي (4.61) ووزن نسبي (92.2%)، وبمستوى (مرتفع جداً) مما يدل على وجود مستوى عالٍ من الالتزام بتطبيق سياسات الأمن السيبراني وإدارة المخاطر عبر الإدارات المعنية داخل الجامعة، وتعكس هذه النتائج مستوى مرتفعاً من فاعلية الإطار التنظيمي والسياسات والإجراءات المعتمدة في مجال الأمن السيبراني داخل الجامعة حيث تسهم هذه السياسات في تعزيز وضوح الإجراءات التنظيمية وتحديد المسؤوليات المؤسسية، إضافة إلى دعم الالتزام المؤسسي بتطبيق متطلبات الأمن السيبراني بما يسهم في رفع مستوى الحماية الرقمية داخل المؤسسة.

المحور السادس: : تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني

جدول رقم (4-6): المتوسطات الحسابية، الانحرافات المعيارية، النتيجة، الوزن النسبي، المستوى والرتبة لعبارات متغير تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني

م.	العبارات	المتوسط الحسابي	الانحراف المعياري	النتيجة	الوزن النسبي	المستوى	الرتبة
1	تحرص الجامعة على تنفيذ برامج تدريبية منتظمة لتنمية قدرات الموظفين في مجال الأمن السيبراني	4.75	0.81	موافق بشدة	95.0 %	مرتفع جداً	3
2	يتم نشر الوعي بمخاطر الأمن السيبراني وسبل الوقاية منها بين منسوبي الجامعة بدرجة كافية	4.76	0.83	موافق بشدة	95.2 %	مرتفع جداً	2

3	يسهم مستوى الوعي السيبراني لدى الموظفين في الحد من المخاطر السيبرانية داخل الجامعة بدرجة ملحوظة	4.80	0.74	موافق بشدة	96.0 %	مرتفع جداً	1
	الدرجة الكلية للمحور السادس	4.77	0.79	موافق بشدة	95.4 %	مرتفع جداً	

يتضح من خلال نتائج الجدول رقم (4-6) اعلاه لمحور تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني أن المتوسط الحسابي الكلي للمحور بلغ (4.77) بانحراف معياري قدره (0.79)، وبوزن نسبي بلغ (95.4%)، وجاءت النتيجة بدرجة (موافق بشدة) وبمستوى (مرتفع جداً) وتشير هذه النتيجة إلى أن جامعة الملك سعود بن عبد العزيز للعلوم الصحية تولي اهتماماً كبيراً بتنمية القدرات البشرية وتعزيز مستوى الوعي بالأمن السيبراني لدى منسوبيها، مما يعكس إدراكاً مؤسسياً لأهمية العامل البشري في الحد من المخاطر السيبرانية وتعزيز منظومة الحماية الرقمية داخل الجامعة.

وفيما يتعلق بالعبارات الفردية جاءت العبارة الثالثة في المرتبة الأولى بمتوسط حسابي بلغ (4.80) ووزن نسبي (96.0%)، وبمستوى (مرتفع جداً) مما يدل على أن ارتفاع مستوى الوعي السيبراني لدى الموظفين يسهم بدرجة كبيرة في الحد من المخاطر السيبرانية داخل الجامعة، وجاءت العبارة الثانية في المرتبة الثانية بمتوسط حسابي (4.76) ووزن نسبي (95.2%)، وبمستوى (مرتفع جداً) مما يشير إلى أن الجامعة تعمل على نشر الوعي بمخاطر الأمن السيبراني وسبل الوقاية منها بين منسوبيها بدرجة كافية، أما العبارة الأولى فقد جاءت في المرتبة الثالثة بمتوسط حسابي (4.75) ووزن نسبي (95.0%)، وبمستوى (مرتفع جداً) مما يدل على حرص الجامعة على تنفيذ برامج تدريبية منتظمة لتنمية قدرات الموظفين في مجال الأمن السيبراني، وتعكس هذه النتائج مستوى مرتفعاً جداً من الاهتمام بتنمية القدرات البشرية وتعزيز الوعي السيبراني داخل الجامعة، حيث تسهم برامج التدريب والتوعية في رفع مستوى الإدراك بالمخاطر السيبرانية وتعزيز السلوكيات الآمنة في استخدام الأنظمة الرقمية، الأمر الذي يدعم فاعلية منظومة الأمن السيبراني داخل الجامعة.

اختبار فرضيات الدراسة

يتم في هذا الجزء اختبار فرضيات الدراسة للتحقق من وجود علاقات ذات دلالة إحصائية بين متغيرات الدراسة. وقد تم استخدام معامل ارتباط بيرسون (Pearson Correlation) لقياس قوة واتجاه العلاقة بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني ومحاورها المختلفة. ويُعد معامل ارتباط بيرسون من الأساليب الإحصائية الشائعة في الدراسات التي تهدف إلى قياس العلاقة بين المتغيرات الكمية، حيث يوضح درجة وقوة الارتباط بينها عند مستوى دلالة إحصائية محدد وقد تم اعتماد مستوى الدلالة الإحصائية ($\alpha \leq 0.05$) للحكم على النتائج بحيث يتم رفض الفرضية الصفرية في حال كانت قيمة مستوى الدلالة أقل من (0.05)، وقبولها في حال كانت أكبر من ذلك.

1. الفرضية الرئيسية:

H01: لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني في جامعة الملك سعود بن عبد العزيز للعلوم الصحية.

جدول رقم (4-7) اختبار معامل ارتباط بيرسون للفرضية الرئيسية

Correlation Pearson			
		Risk Managemnet Practices	Cybersecurity Effectiveness
Managemnet Risk Practices ممارسات إدارة المخاطر	Pearson Correlation	1	.828***
	Sig. (2-tailed)		<.001
	N	225	225
Cybersecurity Effectiveness فاعلية الأمن السيبراني	Pearson Correlation	.828***	1
	Sig. (2-tailed)	<.001	
	N	225	225
***. Correlation at 0.001(2-tailed)			

من خلال الجدول رقم (4-7) أعلاه، يتضح من نتائج التحليل الإحصائي أن قيمة معامل الارتباط بلغت (0.828) وهي قيمة موجبة تشير إلى وجود علاقة ارتباط إيجابية قوية بين ممارسات إدارة المخاطر

وفاعلية الأمن السيبراني، وبلغت قيمة مستوى الدلالة الإحصائية ($\text{Sig} < 0.001$) وهي أقل من مستوى الدلالة المعتمد في الدراسة (0.05) وبناءً على ذلك يتم رفض الفرضية الصفرية (H_0) التي تنص على عدم وجود علاقة ذات دلالة إحصائية بين المتغيرين، ويتم قبول الفرضية البديلة (H_a) التي تنص على وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

2. الفرضية الفرعية الأولى:

H_0 : لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر والتكامل المؤسسي بين إدارة المخاطر والأمن السيبراني .

جدول رقم (4-8): اختبار معامل ارتباط بيرسون للفرضية الفرعية الأولى

Correlation Pearson			
		Risk Managemnet Practices	Institutional Integration
Practices Managemnet Risk ممارسات إدارة المخاطر	Pearson Correlation	1	.623***
	Sig. (2-tailed)		<.001
	N	225	225
Institutional Integration التكامل المؤسسي	Pearson Correlation	.623***	1
	Sig. (2-tailed)	<.001	
	N	225	225
***. Correlation at 0.001(2-tailed)			

من خلال الجدول رقم (4-8) أعلاه، يتضح من نتائج التحليل الإحصائي أن قيمة معامل الارتباط بلغت (0.623) وهي قيمة موجبة تشير إلى وجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر والتكامل المؤسسي بين إدارة المخاطر والأمن السيبراني، وبلغت قيمة مستوى الدلالة الإحصائية ($\text{Sig} < 0.001$) وهي أقل من مستوى الدلالة المعتمد في الدراسة (0.05) وبناءً على ذلك يتم رفض الفرضية الصفرية (H_0) التي تنص على عدم وجود علاقة ذات دلالة إحصائية بين المتغيرين، ويتم قبول الفرضية البديلة (H_a) التي تنص على وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر

والتكامل المؤسسي بين إدارة المخاطر والأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

3. الفرضية الفرعية الثانية:

H03: لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر والتحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني.

جدول رقم (4-9): اختبار معامل ارتباط بيرسون للفرضية الفرعية الثانية

Correlation Pearson			
		Risk Managemnet Practices	Organizational and Technical Challenges
Managemnet Risk Practices ممارسات إدارة المخاطر	Pearson Correlation	1	.677***
	Sig. (2-tailed)		<.001
	N	225	225
Organizational and Technical Challenges التحديات التنظيمية والتقنية	Pearson Correlation	.677***	1
	Sig. (2-tailed)	<.001	
	N	225	225
***. Correlation at 0.001(2-tailed)			

من خلال الجدول رقم (4-9) أعلاه، يتضح من نتائج التحليل الإحصائي أن قيمة معامل الارتباط بلغت (0.677) وهي قيمة موجبة تشير إلى وجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر والتحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني، وبلغت قيمة مستوى الدلالة الإحصائية ($\text{Sig} < 0.001$) وهي أقل من مستوى الدلالة المعتمد في الدراسة (0.05) وبناءً على ذلك يتم رفض الفرضية الصفرية (H03) التي تنص على عدم وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر والتحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني، ويتم قبول الفرضية البديلة (Ha3) التي تنص على وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر والتحديات التنظيمية والتقنية المرتبطة بتطبيق الأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

4. الفرضية الفرعية الثالثة:

H04: لا توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر وفاعلية الإطار التنظيمي والسياسات والإجراءات المعتمدة في مجال الأمن السيبراني وإدارة المخاطر في الجامعة.

جدول رقم (4-10): اختبار معامل ارتباط بيرسون للفرضية الفرعية الثالثة

Correlation Pearson			
		Risk Managemnet Practices	Effectiveness of the Regulatory Policies, and Procedures
Practices Managemnet Risk ممارسات إدارة المخاطر	Pearson Correlation	1	.719***
	Sig. (2-tailed)		<.001
	N	225	225
Effectiveness of the Regulatory Policies, and Procedures فاعلية الإطار التنظيمي والسياسات والإجراءات	Pearson Correlation	.719***	1
	Sig. (2-tailed)	<.001	
	N	225	225
***. Correlation at 0.001(2-tailed)			

من خلال الجدول رقم (4-10) أعلاه، يتضح من نتائج التحليل الإحصائي أن قيمة معامل الارتباط بلغت (0.719) وهي قيمة موجبة تشير إلى وجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر وفاعلية الإطار التنظيمي والسياسات والإجراءات، كما بلغت قيمة مستوى الدلالة الإحصائية ($\text{Sig} < 0.001$) وهي أقل من مستوى الدلالة المعتمد في الدراسة (0.05) وبناءً على ذلك يتم رفض الفرضية الصفرية (H04) التي تنص على عدم وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر وفاعلية الإطار التنظيمي والسياسات والإجراءات، ويتم قبول الفرضية البديلة (Ha4) التي تنص على وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر وفاعلية الإطار التنظيمي والسياسات والإجراءات في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

5. الفرضية الفرعية الرابعة:

H05: لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين ممارسات إدارة المخاطر المؤسسية وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني.

جدول رقم (4-11): اختبار معامل ارتباط بيرسون للفرضية الفرعية الرابعة

Correlation Pearson			
		Risk Managemnet Practices	Human Capacity Development and Cybersecurity Awareness
Practices Managemnet Risk ممارسات إدارة المخاطر	Pearson Correlation	1	.556***
	Sig. (2-tailed)		<.001
	N	225	225
Human Capacity Development and Cybersecurity Awareness تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني	Pearson Correlation	.556***	1
	Sig. (2-tailed)	<.001	
	N	225	225
***. Correlation at 0.001(2-tailed)			

من خلال الجدول رقم (4-11) أعلاه، يتضح من نتائج التحليل الإحصائي أن قيمة معامل الارتباط بلغت (0.556) موجبة تشير إلى وجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني، كما بلغت قيمة مستوى الدلالة الإحصائية ($\text{Sig} < 0.001$) وهي أقل من مستوى الدلالة المعتمد في الدراسة (0.05) وبناءً على ذلك يتم رفض الفرضية الصفرية (H05) التي تنص على عدم وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني، ويتم قبول الفرضية البديلة (Ha5) التي تنص على وجود علاقة ذات دلالة إحصائية بين ممارسات إدارة المخاطر وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

النتائج:

أولاً: نتائج الدراسة

في ضوء تحليل بيانات الدراسة واختبار فرضياتها، توصلت الدراسة إلى مجموعة من النتائج الرئيسية يمكن عرضها على النحو الآتي:

- أظهرت نتائج التحليل الوصفي أن مستوى ممارسات إدارة المخاطر المؤسسية جاء بدرجة مرتفعة جداً إذ بلغ المتوسط الحسابي الكلي للمحور (4.35) وبوزن نسبي (87.1%) وهو ما يشير إلى وجود مستوى متقدم من تطبيق ممارسات إدارة المخاطر داخل الجامعة، لا سيما فيما يتعلق بتحديد المخاطر السيبرانية، وتوثيقها، وربط نتائج تقييمها بالأهداف الاستراتيجية، وتوافر خطط استجابة معتمدة للحوادث السيبرانية. وتعكس هذه النتيجة وجود إطار مؤسسي منظم لإدارة المخاطر يتسق مع متطلبات الحوكمة المؤسسية ومعايير تعزيز الأمن السيبراني في مؤسسات التعليم العالي.
- بينت النتائج أن فاعلية الأمن السيبراني جاءت كذلك بدرجة مرتفعة جداً حيث بلغ المتوسط الحسابي الكلي لهذا المحور (4.53) وبوزن نسبي (90.6%) مما يدل على أن الجامعة تتمتع بمستوى عالٍ من الكفاءة في حماية البيانات الأكاديمية والبحثية وتنظيم صلاحيات الدخول إلى الأنظمة التقنية وتطبيق الضوابط المرتبطة بسرية البيانات وسلامتها إضافة إلى الإسهام الفعال لسياسات الأمن السيبراني في ضمان استمرارية الخدمات الأكاديمية والإدارية.
- فيما يخص التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني فقد أظهرت النتائج أن هذا المحور جاء بدرجة مرتفعة بمتوسط حسابي كلي بلغ (3.79) وبوزن نسبي (75.8%) وتشير هذه النتيجة إلى وجود مستوى جيد من التنسيق المؤسسي بين الجهات ذات العلاقة إلا أن هذا المستوى لا يزال أقل نسبياً مقارنة بمحوري ممارسات إدارة المخاطر وفاعلية الأمن السيبراني وقد برزت بصفة خاصة ملاحظة تتعلق بضعف انتظام تبادل المعلومات الخاصة بالمخاطر السيبرانية بين إدارة المخاطر ووحدته الأمن السيبراني وإدارة تقنية المعلومات وهو ما يشير إلى وجود حاجة إلى مزيد من التنظيم والوضوح في هذا الجانب.
- أظهرت النتائج أن محور التحديات التنظيمية والتقنية، فقد جاء بدرجة مرتفعة جداً بمتوسط حسابي بلغ (4.71) وبوزن نسبي (94.2%) مما يدل على وجود إدراك مرتفع لدى أفراد عينة الدراسة بأن هناك تحديات تنظيمية وتقنية مؤثرة في فاعلية تطبيق الأمن السيبراني داخل جامعة الملك سعود بن عبدالعزيز للعلوم الصحية الأمر الذي يعكس أن تعزيز الأمن السيبراني لا يرتبط فقط بتوافر السياسات والإجراءات، بل يتطلب أيضاً معالجة المعوقات البشرية والتنظيمية المصاحبة لعملية التطبيق.

- فيما يتعلق بفاعلية الإطار التنظيمي والسياسات والإجراءات المعتمدة في مجال الأمن السيبراني وإدارة المخاطر فقد أظهرت النتائج أن هذا المحور جاء بدرجة مرتفعة جداً بمتوسط حسابي كلي بلغ (4.66) وبوزن نسبي (93.2%) مما يشير إلى أن السياسات المعتمدة داخل الجامعة تتسم بدرجة عالية من الوضوح والشمول، وتسهم في توحيد الإجراءات وتحديد الأدوار والمسؤوليات داخل المؤسسة بشكل فعال، وهو ما يعكس نضجاً تنظيمياً في إدارة الأمن السيبراني والمخاطر المرتبطة به.
- أظهرت النتائج أن تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني جاءت بدرجة مرتفعة جداً وبمتوسط حسابي بلغ (4.77) وبوزن نسبي (95.4%) وهي أعلى قيمة بين محاور الدراسة الفرعية مما يدل على إدراك مؤسسي واضح لأهمية العامل البشري في دعم فاعلية الأمن السيبراني، وقد أظهرت العبارات المرتبطة بهذا المحور أن الجامعة تحرص على تنفيذ برامج تدريبية منتظمة، ونشر الوعي بالمخاطر السيبرانية، وأن ارتفاع مستوى الوعي لدى الموظفين يسهم بوضوح في الحد من المخاطر السيبرانية داخل الجامعة.
- وعلى مستوى اختبار الفرضيات، فقد كشفت نتائج معامل ارتباط بيرسون عن وجود علاقة ارتباط إيجابية قوية ذات دلالة إحصائية بين ممارسات إدارة المخاطر وفاعلية الأمن السيبراني حيث بلغ معامل الارتباط (0.828) عند مستوى دلالة ($\text{Sig} < 0.001$) وبذلك تم رفض الفرضية الصفرية الرئيسة وقبول الفرضية البديلة. كما أظهرت النتائج وجود علاقة ارتباط إيجابية ذات دلالة إحصائية بين ممارسات إدارة المخاطر والتكامل المؤسسي بمعامل ارتباط بلغ (0.623)، ووجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر والتحديات التنظيمية والتقنية بمعامل ارتباط بلغ (0.677)، ووجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر وفاعلية الإطار التنظيمي والسياسات والإجراءات بمعامل ارتباط بلغ (0.719)، إضافة إلى وجود علاقة ارتباط إيجابية بين ممارسات إدارة المخاطر وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني بمعامل ارتباط بلغ (0.556) وجميعها عند مستوى دلالة ($\text{Sig} < 0.001$) وتؤكد هذه النتائج مجتمعة أن ممارسات إدارة المخاطر تمثل أحد المحددات الجوهرية لرفع فاعلية الأمن السيبراني داخل الجامعة.

ثانياً: نتائج الدراسة ومناقشتها مع نتائج الدراسات السابقة

- أظهرت نتائج الدراسة الحالية أن ممارسات إدارة المخاطر المؤسسية ترتبط ارتباطاً إيجابياً قوياً بفاعلية الأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية وهو ما يؤكد أن تعزيز عمليات تحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراجعتها يسهم بصورة مباشرة في رفع مستوى الحماية الرقمية داخل البيئة الجامعية وتنسجم هذه النتيجة مع التوجه العام في الدراسات السابقة الذي أكد أن فاعلية الأمن السيبراني في مؤسسات التعليم العالي لا تعتمد فقط على الحلول التقنية بل تتأثر كذلك

بعوامل تنظيمية وإدارية وبشرية مثل الحوكمة، والتنسيق المؤسسي، ووضوح السياسات، ومستوى الوعي، والتدريب.

- أظهرت نتائج الدراسة ارتفاع مستوى ممارسات إدارة المخاطر المؤسسية داخل الجامعة وهو ما يتفق مع ما أشارت إليه الدراسات السابقة من أن دمج إدارة المخاطر ضمن المنظومة المؤسسية يساهم في تحسين جاهزية المؤسسات التعليمية لمواجهة التهديدات الرقمية وقد دعمت دراسة (2021, Almomani, I., Ahmed, M., & Maglaras, L.) هذا الاتجاه حيث أكدت أن ربط تقييم النضج السيبراني بممارسات إدارة المخاطر والحوكمة يساهم في تحسين الفاعلية السيبرانية في مؤسسات التعليم العالي، مع الإشارة إلى وجود فجوات في تدريب العاملين وتطوير السياسات.
- بينت نتائج الدراسة أن فاعلية الأمن السيبراني جاءت بدرجة مرتفعة جداً وهي نتيجة تتفق مع دراسة (البوشي، 2022) التي توصلت إلى وجود علاقة إيجابية قوية بين تطبيق الأمن السيبراني ومستوى الثقة الرقمية لدى منسوبي الجامعات، كما تتفق مع دراسة (الهزاني، 2023) التي أوضحت أن الالتزام بالضوابط الوطنية والسياسات التقنية يساهم في رفع مستوى الحماية الرقمية داخل المؤسسات التعليمية.
- أظهرت النتائج أن مستوى التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني جاء بدرجة مرتفعة لكنه أقل نسبياً من بقية المحاور مما يدل على وجود تنسيق جيد بين الجهات المعنية، إلا أنه لا يزال بحاجة إلى مزيد من التطوير خصوصاً في جانب تبادل المعلومات المتعلقة بالمخاطر السيبرانية وتتفق هذه النتيجة مع دراسة (الخصري وآخرون، 2020) ودراسة (المنيع، 2022) اللتين أشارتا إلى وجود قصور في التكامل المؤسسي بين الإدارات الفنية والإدارية في الجامعات السعودية، وكذلك مع دراسة (السميري، 2022) التي أكدت ضعف التنسيق بين الإجراءات الفنية والتنظيمية.
- أظهرت نتائج الدراسة أن التحديات التنظيمية والتقنية جاءت بدرجة مرتفعة جداً مما يعكس إدراكاً واضحاً لدى أفراد العينة لوجود معوقات تؤثر في فاعلية تطبيق الأمن السيبراني ومن أبرزها قلة الوعي السيبراني لدى بعض الموظفين ومحدودية الكوادر البشرية المتخصصة إضافة إلى التعقيدات التنظيمية والإجرائية وتتفق هذه النتيجة مع دراسة (السميري، 2022) ودراسة (Alharbi, T., 2022) اللتين أشارتا إلى أن نقص التدريب والكوادر المتخصصة وضعف الدعم المؤسسي يمثلان من أبرز التحديات التي تواجه تطبيق الأمن السيبراني في المؤسسات.
- أظهرت النتائج أن فاعلية الإطار التنظيمي والسياسات والإجراءات جاءت بدرجة مرتفعة جداً مما يدل على وجود سياسات واضحة وشاملة تساهم في تنظيم العمل المؤسسي وتحديد الأدوار والمسؤوليات وتتفق هذه النتيجة مع دراسة (Cheng, E. C. K., & Wang, T., 2022) التي أكدت أن الجامعات

التي تمتلك حوكمة رقمية واضحة وتدمج الأمن السيبراني ضمن استراتيجياتها المؤسسية تحقق مستويات أعلى من النضج السيبراني.

- أظهرت نتائج الدراسة أن تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني جاءت في المرتبة الأعلى بين محاور الدراسة وهو ما يؤكد الدور المحوري للعامل البشري في تعزيز الأمن السيبراني داخل المؤسسات التعليمية. وتتفق هذه النتيجة مع دراسة (2025, Armas, R., & Taherdoost, H) التي أكدت أن التدريب المستمر ونشر الثقافة السيبرانية يساهمان في تحسين الالتزام بالسياسات الأمنية وتقليل الأخطاء التشغيلية.

- وتتفق نتائج الدراسة الحالية مع دراسة (القحطاني , 2019) التي أشارت إلى أهمية رفع مستوى الوعي بالأمن السيبراني لدى طلبة الجامعات السعودية، مؤكدة أن التوعية السيبرانية تمثل أحد أهم الوسائل الوقائية للحد من الجرائم الإلكترونية وتعزيز الاستخدام الآمن للتقنيات الرقمية.

- كما أظهرت نتائج الدراسة الحالية توافقاً مع ما توصلت إليه دراسة (Ulven & Wangen, 2021) التي بينت أن مؤسسات التعليم العالي تعد من أكثر المؤسسات عرضة للهجمات السيبرانية بسبب طبيعة البيئة الأكاديمية المفتوحة وتعدد المستخدمين والأنظمة الرقمية، مما يستدعي تبني ممارسات فعالة لإدارة المخاطر السيبرانية وتعزيز السياسات الأمنية داخل الجامعات.

- كما تتفق نتائج الدراسة الحالية مع دراسة (Ganesen et al, 2022) التي أكدت أن مستوى المخاطر السيبرانية في مؤسسات التعليم العالي يتأثر بعدة عوامل تنظيمية وتقنية، من أبرزها ضعف سياسات أمن المعلومات وقصور آليات إدارة المخاطر داخل المؤسسات التعليمية، كما أشارت إلى أن وجود إطار واضح لإدارة المخاطر وتكامل السياسات الأمنية يساهم في تقليل احتمالية وقوع الهجمات السيبرانية.

- تتفق نتائج الدراسة الحالية مع دراسة (الحربي , 2022) التي تناولت أثر التحول الرقمي في الجامعات، حيث أشارت إلى أن التوسع في استخدام الأنظمة الرقمية يتطلب توفير بنية تقنية آمنة وسياسات تنظيمية واضحة لضمان استمرارية الخدمات الأكاديمية الرقمية، وهو ما يعزز أهمية إدارة المخاطر المصاحبة للتحول الرقمي في المؤسسات التعليمية.

- وعلى مستوى اختبار الفرضيات أظهرت النتائج وجود علاقة ارتباط إيجابية ذات دلالة إحصائية بين ممارسات إدارة المخاطر وجميع أبعاد فاعلية الأمن السيبراني وهو ما يساهم في سد الفجوة البحثية التي أشارت إليها الدراسة في باب الدراسات السابقة حيث إن معظم الدراسات ركزت على تقييم الجاهزية السيبرانية أو الالتزام بالضوابط دون تحليل العلاقة المباشرة بين إدارة المخاطر المؤسسية وفاعلية الأمن السيبراني.

- وبوجه عام تتفق نتائج الدراسة الحالية مع الدراسات السابقة في التأكيد على أهمية التكامل المؤسسي، ووضوح السياسات، وتعزيز الوعي والتدريب، ومعالجة التحديات التنظيمية والتقنية، إلا أن الدراسة الحالية تميزت بتركيزها على تحليل العلاقة التكاملية بين ممارسات إدارة المخاطر المؤسسية وفاعلية الأمن السيبراني داخل جامعة سعودية مما يضيف إسهاماً علمياً وتطبيقياً للأدبيات المحلية في هذا المجال.

التوصيات:

- في ضوء النتائج التي توصلت إليها الدراسة الحالية حول دور ممارسات إدارة المخاطر في تعزيز فاعلية الأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية، توصي الدراسة بما يلي:
- تعزيز التكامل المؤسسي بين إدارة المخاطر وإدارة الأمن السيبراني وتقنية المعلومات من خلال إنشاء آليات تنسيق رسمية لتبادل المعلومات المتعلقة بالمخاطر السيبرانية، بما يسهم في تحسين سرعة الاستجابة للحوادث السيبرانية واتخاذ القرارات المبنية على تقييمات دقيقة للمخاطر.
 - تطوير إطار مؤسسي متكامل لإدارة المخاطر السيبرانية يربط بين ممارسات إدارة المخاطر المؤسسية والسياسات والإجراءات الخاصة بالأمن السيبراني، بحيث يتم تضمين تقييم المخاطر السيبرانية ضمن عملية التخطيط الاستراتيجي وإدارة المخاطر في الجامعة.
 - تعزيز برامج التدريب والتأهيل المتخصص في مجال الأمن السيبراني من خلال تصميم برامج تدريبية دورية تستهدف الموظفين في الإدارات التقنية والإدارية على حد سواء، بهدف رفع مستوى الوعي السيبراني وتقليل الأخطاء البشرية التي قد تؤدي إلى حدوث اختراقات أمنية.
 - استقطاب وتطوير الكوادر البشرية المتخصصة في الأمن السيبراني وإدارة المخاطر الرقمية، وذلك من خلال دعم برامج التأهيل المهني والشهادات الاحترافية في مجال الأمن السيبراني، بما يسهم في سد الفجوة المتعلقة بنقص الخبرات المتخصصة التي أشارت إليها نتائج الدراسة.
 - مراجعة وتحديث السياسات والإجراءات التنظيمية المرتبطة بالأمن السيبراني بشكل دوري لضمان توافقتها مع المستجدات التقنية والتهديدات السيبرانية المتغيرة وكذلك لضمان توافقتها مع الضوابط والمعايير الوطنية الصادرة عن الهيئة الوطنية للأمن السيبراني.
 - تعزيز ثقافة الأمن السيبراني داخل البيئة الجامعية من خلال تنفيذ حملات توعوية وبرامج تثقيفية مستمرة تستهدف جميع منسوبي الجامعة بما في ذلك أعضاء هيئة التدريس، والموظفين، والطلاب وذلك بهدف تعزيز السلوك الأمني وتقليل المخاطر المرتبطة بالاستخدام غير الآمن للتقنيات الرقمية.

- تطوير مؤشرات أداء ومقاييس لقياس فاعلية إدارة المخاطر السيبرانية داخل الجامعة بحيث يتم تقييم مستوى تطبيق السياسات والإجراءات الأمنية بشكل دوري وقياس مدى جاهزية المؤسسة للتعامل مع التهديدات السيبرانية.
- تعزيز دعم الإدارة العليا لمبادرات الأمن السيبراني وإدارة المخاطر الرقمية لما لذلك من دور محوري في توفير الموارد اللازمة وتبني سياسات مؤسسية واضحة تدعم تطبيق أفضل الممارسات في مجال الحوكمة السيبرانية.
- العمل على تبني نموذج حوكمة سيبرانية متكامل داخل الجامعات السعودية يربط بين الأبعاد التقنية والتنظيمية والبشرية ويضمن تكامل الأدوار بين مختلف الإدارات المعنية بإدارة المخاطر والأمن السيبراني.

المقترحات:

- ◆ إجراء دراسات تطبيقية أو تجريبية لتحليل أثر برامج التدريب والتوعية في مجال الأمن السيبراني في تقليل الحوادث الأمنية داخل الجامعات، وذلك من خلال قياس مدى تأثير هذه البرامج في رفع مستوى الوعي السيبراني وتعزيز السلوك الأمني لدى العاملين في المؤسسات التعليمية.
- ◆ دراسة التحديات التنظيمية والتقنية التي تواجه تطبيق ضوابط الهيئة الوطنية للأمن السيبراني في المؤسسات التعليمية وتحليل مدى توافق السياسات والإجراءات المؤسسية في الجامعات مع تلك الضوابط، بما يسهم في تطوير الأطر التنظيمية وتعزيز مستوى الامتثال للمعايير الوطنية للأمن السيبراني.
- ◆ دراسة أثر القيادة المؤسسية والتحول الرقمي في تعزيز الأمن السيبراني داخل الجامعات مع التركيز على دور الإدارة العليا في دعم مبادرات إدارة المخاطر السيبرانية وتطوير السياسات والإجراءات التنظيمية بما يسهم في رفع مستوى الحوكمة السيبرانية في مؤسسات التعليم العالي.

خاتمة الفصل:

تناول هذا الفصل عرض وتحليل نتائج الدراسة الميدانية المتعلقة بدور ممارسات إدارة المخاطر في تعزيز فاعلية الأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية حيث تم تحليل بيانات الاستبانة باستخدام مجموعة من الأساليب الإحصائية الوصفية والاستدلالية، وذلك بهدف التعرف على مستوى استجابات أفراد العينة تجاه محاور الدراسة المختلفة، وقد تم عرض نتائج التحليل الوصفي لمتغيرات الدراسة والتي شملت ممارسات إدارة المخاطر المؤسسية، وفاعلية الأمن السيبراني والتكامل المؤسسي بين إدارة المخاطر والأمن السيبراني، إضافة إلى التحديات التنظيمية والتقنية، وفاعلية الإطار التنظيمي والسياسات والإجراءات، وتنمية القدرات البشرية ونشر الوعي بالأمن السيبراني، كما تم اختبار فرضيات الدراسة باستخدام معامل ارتباط بيرسون للتعرف على طبيعة العلاقة بين ممارسات إدارة المخاطر وأبعاد فاعلية الأمن السيبراني.

وفي ضوء نتائج التحليل الإحصائي تم عرض نتائج الدراسة ومناقشتها بالاستناد إلى ما توصلت إليه الدراسات السابقة وصولاً إلى تقديم مجموعة من التوصيات والمقترحات التي تسهم في تعزيز التكامل بين إدارة المخاطر والأمن السيبراني.

المراجع

المراجع العربية:

- البيشي، منيرة عبد الله. (2021). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية: دراسة على جامعة بيشة. مجلة التعليم العالي الإلكتروني. مسترجع من :
<https://journals.iugaza.edu.ps/index.php/IUGJEPS/article/view/10518>
- الحربي، ياسر ساير. (2022). أثر التحول الرقمي على كفاءة الأداء الأكاديمي - حالة دراسية لهيئة أعضاء التدريس بجامعة الملك عبد العزيز. المجلة العربية للنشر العلمي AJSP ،المجلد الخامس، الإصدار الثالث والأربعون، 647-686. مسترجع من:
<https://www.ajsp.net/volume.php?vol=24>
- الخضري، جيهان، وسلامي، هدى، وكليبي، نعمة. (2020). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة. مجلة تطوير الأداء الجامعي، 1(12)، 217-233 ، مسترجع من :
https://jpud.journals.ekb.eg/article_170391.html
- السميري، سامي سعد. (2022). واقع الأمن السيبراني وتحدياته في السعودية. المجلة العلمية لجامعة الملك فيصل - العلوم الأساسية والتطبيقية، 23(1)، 66-74. مسترجع من:
<https://services.kfu.edu.sa/ScientificJournal/Handlers/FileHandler.ashx?Folder=UploadFiles&file=10+210075+1.pdf>
- القحطاني، نورة بنت ناصر. (2019). مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي. مجلة شؤون اجتماعية، 36(144)، 120-85، مسترجع من:
<https://search.emarefa.net/detail/BIM-922380>
- المنيع، الجوهرة عبد الرحمن. (2022). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030. مجلة كلية التربية، 38(1)، 156-194. مسترجع من:
<https://search.shamaa.org/fullrecord?ID=332323>
- الهيئة الوطنية للأمن السيبراني. (2017). تنظيم الهيئة الوطنية للأمن السيبراني: صادر بالأمر الملكي رقم (6801) وتاريخ 1439/2/11 هـ. الرياض: المملكة العربية السعودية. مسترجع من:
https://cdn.nca.gov.sa/api/files/public/upload/b8032cb5-70c4-40ad-884e-b962001b6704_الهيئة_الوطنية_للأمن_السيبراني.pdf

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2023) .سياسة إدارة الثغرات - OPP.ITS.009 (Vulnerability Management Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2023) .سياسة اختبار الاختراق - OPP.ITS.008 (Penetration Testing Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2023) .سياسة إدارة سجلات الأحداث السيبرانية والمراقبة - OPP.ITS.007 (Cybersecurity Event Log Management Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2024) .السياسة العامة للأمن السيبراني - OPP.ITS.031 (Cybersecurity Public Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2024) .سياسة الامتثال للتشريعات واللوائح الخاصة بالأمن السيبراني - OPP.ITS.028 (Compliance with Cybersecurity Regulations and Laws Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2024) .سياسة إدارة الحوادث والتهديدات السيبرانية - OPP.ITS.021 (Cybersecurity Incident and Threat Management Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2025) .سياسة إدارة مخاطر الأمن السيبراني - OPP.ITS.010 (Cybersecurity Risk Management Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2025) .سياسة إدارة المخاطر - OPP.TA.001 (Risk Management Policy) : إدارة المخاطر ، وثيقة داخلية.

-جامعة الملك سعود بن عبد العزيز للعلوم الصحية .(2025) .سياسة مراجعة وتدقيق الأمن السيبراني - OPP.ITS.029 (Cybersecurity Audit and Review Policy) : إدارة الأمن السيبراني ، وثيقة داخلية.

المراجع الأجنبية:

- Alharbi, Talal. (2022). Developing a Cost-effective Cybersecurity Management System for Academic Institutions in Saudi Arabia. Journal of Engineering and Applied Sciences ,9(1) 57-74 Retrieved from: [10.5455/jeas.2022050105](https://jeas.2022050105)
- Almomani, Iman., Ahmed, Mohanned., & Maglaras, Leandros. (2021). Cybersecurity Maturity Assessment Framework for Higher Education Institutions in Saudi Arabia (SCMAF). PeerJ Computer Science Journal. Retrieved from: <https://peerj.com/articles/cs-703/>
- Armas, Reismary & Taherdoost, Hamed. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. MDPI, 16(5), 336. Retrieved from: <https://www.mdpi.com/2078-2489/16/5/336>
- Cheng, Eric. C. K., & Wang, Tianchong. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. MDPI , 13(4), 192. Retrieved from: <https://www.mdpi.com/2078-2489/13/4/192>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management – Integrating with Strategy and Performance. Durham, NC: American Institute of Certified Public Accountants (AICPA). Retrieved from: <https://erm.ncsu.edu/resource-center/cosos-erm-framework/>
- Ganesen, R., Abu Bakar, A., Ramli, R., Rahim, F., & Ahmad Zawawi, M. (2022). Cybersecurity risk assessment: Modeling factors associated with higher education institutions. International Journal of Advanced Computer Science and Applications, 13(8). Retrieved from: <https://thesai.org/Publications/ViewPaper?Code=IJACSA&Issue=8&SerialNo=43&Volume=13>
- International Organization for Standardization (ISO). (2018). ISO 31000:2018 – Risk Management – Guidelines. Retrieved from: <https://www.iso.org/standard/65694.html>
- National Cybersecurity Authority (NCA). (2019). Critical Systems Cybersecurity Controls (CSCC-1: 2019). Riyadh, Saudi Arabia. Retrieved from: https://cdn.nca.gov.sa/api/files/public/upload/f15af01c-dc59-4281-95e2-03a770655937_Critical-Systems-Cybersecurity-Controls.pdf cdn.nca.gov.sa
- National Cybersecurity Authority (NCA). (2020). Cloud Cybersecurity Controls (CCC-1: 2020). Riyadh, Saudi Arabia. Retrieved from: <https://nca.gov.sa/ccs-en.pdf>
- National Cybersecurity Authority (NCA). (2021). Organizational Social Media Accounts Cybersecurity Controls (OSMACC-1: 2021). Riyadh, Saudi Arabia. Retrieved from: <https://nca.gov.sa/osmacc-en.pdf>

-National Cybersecurity Authority (NCA). (2021). Telework Cybersecurity Controls (TCC-1: 2021). Riyadh, Saudi Arabia. Retrieved from:
https://nca.gov.sa/telework_cybersecurity_controls-en.pdf

-National Cybersecurity Authority (NCA). (2022). Data Cybersecurity Controls (DCC-1: 2022). Riyadh, Saudi Arabia. Retrieved from:
https://cdn.nca.gov.sa/api/files/public/upload/1c2cfb9c-7788-4549-9f29-f337500f1787_Data-Cybersecurity-Controls-.pdf

-National Cybersecurity Authority (NCA). (2024). Essential Cybersecurity Controls (ECC-2: 2024). Riyadh, Saudi Arabia. Retrieved from:
https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654_ECC--2024-EN.pdf

-Ulven, J. B., & Wangen, G. (2021).
A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.
Retrieved from:
<https://www.mdpi.com/1999-5903/13/2/39>

الملاحق

الاستبانة

السلام عليكم ورحمة الله وبركاته،

الزملاء والزميلات الكرام،

تحية طيبة وبعد،

يسرني دعوتكم للمشاركة في استبانة علمية يتم إعدادها ضمن متطلبات الحصول على درجة الماجستير، بعنوان:

"دور إدارة المخاطر في تعزيز الأمن السيبراني بالجامعات السعودية"
دراسة تطبيقية على جامعة الملك سعود بن عبدالعزيز للعلوم الصحية

وتهدف هذه الدراسة إلى التعرف على دور ممارسات إدارة المخاطر المؤسسية في تعزيز فاعلية الأمن السيبراني داخل الجامعات السعودية، بالإضافة إلى دراسة مستوى التكامل المؤسسي بين إدارة المخاطر ووحدات الأمن السيبراني ومدى إسهام ذلك في حماية البنية الرقمية وضمان استمرارية الخدمات الأكاديمية والإدارية

ونظرًا لما تتمتعون به من خبرة ومعرفة في مجال العمل، فإن مشاركتكم في الإجابة عن فقرات هذه الاستبانة تمثل عنصرًا مهمًا في إنجاح هذه الدراسة وتحقيق أهدافها

لذا نأمل منكم التكرم بالمشاركة في هذه الدراسة من خلال الإجابة على فقرات الاستبانة بكل موضوعية ودقة، علمًا بأن جميع البيانات التي سيتم جمعها ستعامل بسرية تامة، ولن تستخدم إلا لأغراض البحث العلمي فقط

شاكراً ومقدِّراً لكم حسن تعاونكم ووقتكم الثمين،،

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الديموغرافية :

تهدف هذه البيانات إلى التعرف على الخصائص العامة لأفراد عينة الدراسة، وتستخدم لأغراض التحليل الإحصائي فقط.

1. الجنس:

☐ ذكر

☐ أنثى

2. المستوى التعليمي:

☐ دبلوم

☐ بكالوريوس

☐ ماجستير

☐ دكتوراه

3. المسمى الوظيفي:

☐ مدير

☐ رئيس قسم

☐ مشرف

☐ مسؤول

☐ خبير

☐ مهندس

☐ محلل

☐ إحصائي

☐ مصمم

☐ مشغل

☐ إداري

☐ عضو هيئة تدريس

4. عدد سنوات الخبرة:

- ☐ أقل من 5 سنوات
- ☐ من 5 إلى أقل من 10 سنوات
- ☐ من 10 إلى أقل من 15 سنة
- ☐ من 15 إلى أقل من 20 سنة
- ☐ 20 سنة فأكثر

5. المدينة الجامعية:

- ☐ الرياض
- ☐ جدة
- ☐ الأحساء

6. مدى ارتباط عملك بالأنظمة التقنية:

- ☐ ارتباط مباشر
- ☐ ارتباط غير مباشر

ثانياً: محاور الدراسة:

يرجى تحديد درجة الموافقة المناسبة لكل عبارة وفق المقياس الآتي بوضع علامة [√] في الخانة التي تعبر عن رأيكم:

- لا أوافق بشدة = (1)
- لا أوافق = (2)
- محايد = (3)
- أوافق = (4)
- أوافق بشدة = (5)

م.م	العبارات	1	2	3	4	5
		لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
المحور الأول: ممارسات إدارة المخاطر المؤسسية						
1	تقوم جامعة الملك سعود بن عبد العزيز للعلوم الصحية بتحديد المخاطر السيبرانية المرتبطة بالأنظمة الأكاديمية والإدارية بشكل واضح	[]	[]	[]	[]	[]
2	يتم توثيق المخاطر السيبرانية داخل الجامعة ضمن سجلات رسمية معتمدة	[]	[]	[]	[]	[]
3	يتم تحليل احتمالية حدوث المخاطر السيبرانية وتأثيرها قبل اتخاذ القرارات	[]	[]	[]	[]	[]
4	تعتمد جامعة الملك سعود بن عبد العزيز للعلوم الصحية على معايير واضحة لتصنيف المخاطر السيبرانية حسب درجة الخطورة	[]	[]	[]	[]	[]
	يتم تقييم المخاطر السيبرانية وفق منهجية موحدة داخل جامعة الملك سعود بن عبد العزيز للعلوم الصحية	[]	[]	[]	[]	[]
6	يتم ربط نتائج تقييم المخاطر بالأهداف الاستراتيجية للجامعة	[]	[]	[]	[]	[]
7	تتوفر خطط استجابة معتمدة للتعامل مع الحوادث السيبرانية بدرجة كافية	[]	[]	[]	[]	[]
8	يتم تحديث سياسات الأمن السيبراني وإدارة المخاطر في الجامعة بناءً على نتائج المراجعة والتقييم الدوري	[]	[]	[]	[]	[]

م.م	العبارات	1	2	3	4	5
		لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
المحور الثاني: فاعلية الأمن السيبراني						
1	تحظى البيانات الأكاديمية والبحثية بحماية كافية داخل جامعة الملك سعود بن عبد العزيز للعلوم الصحية	[]	[]	[]	[]	[]
2	يتم تحديد وتنظيم صلاحيات دخول المستخدمين إلى الأنظمة التقنية بما يتناسب مع مهامهم الوظيفية	[]	[]	[]	[]	[]
3	تُطبق جامعة الملك سعود بن عبد العزيز للعلوم الصحية ضوابط واضحة لضمان سرية وسلامة البيانات	[]	[]	[]	[]	[]
4	توجد آلية واضحة للإبلاغ عن الحوادث السيبرانية داخل الجامعة	[]	[]	[]	[]	[]
5	تُطبق جامعة الملك سعود بن عبد العزيز للعلوم الصحية إجراءات وقائية للحد من المخاطر السيبرانية قبل وقوعها	[]	[]	[]	[]	[]
6	تسهم سياسات الأمن السيبراني في ضمان استمرارية الخدمات الأكاديمية والإدارية	[]	[]	[]	[]	[]

م.م	العبارات	1	2	3	4	5
		لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
المحور الثالث: التكامل المؤسسي بين إدارة المخاطر والأمن السيبراني						
1	يوجد تنسيق واضح بين إدارة المخاطر ووحدة الأمن السيبراني داخل الجامعة	[]	[]	[]	[]	[]
2	يتم تبادل المعلومات المتعلقة بالمخاطر السيبرانية بين إدارة المخاطر، ووحدة الأمن السيبراني، وإدارة تقنية المعلومات بشكل منتظم	[]	[]	[]	[]	[]
3	يساعد التعاون بين إدارة المخاطر ووحدة الأمن السيبراني في سرعة وكفاءة الاستجابة للحوادث الرقمية	[]	[]	[]	[]	[]

م.م	العبارات	1	2	3	4	5
		لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
المحور الرابع: التحديات التنظيمية والتقنية						
1	تشكل قلة الوعي السيبراني لدى بعض الموظفين تحدياً مؤثراً على فاعلية الأمن السيبراني في الجامعة	[]	[]	[]	[]	[]
2	تشكل محدودية الكوادر البشرية المتخصصة عائقاً أمام تطبيق الأمن السيبراني بدرجة ملحوظة	[]	[]	[]	[]	[]
3	تؤثر التعقيدات التنظيمية والإجرائية على فاعلية تطبيق سياسات الأمن السيبراني في الجامعة	[]	[]	[]	[]	[]

م.م	العبارات	1	2	3	4	5
		لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
المحور الخامس: الإطار التنظيمي وسياسات الأمن السيبراني وإدارة المخاطر						
1	تتسم سياسات الأمن السيبراني وإدارة المخاطر في الجامعة بالوضوح والشمول الكافي لتنظيم العمل المؤسسي	[]	[]	[]	[]	[]
2	يتم تطبيق سياسات الأمن السيبراني وإدارة المخاطر في الجامعة بدرجة عالية من الالتزام عبر الإدارات المعنية	[]	[]	[]	[]	[]
3	تسهم سياسات الأمن السيبراني وإدارة المخاطر في توحيد الإجراءات وتحديد الأدوار والمسؤوليات داخل الجامعة بشكل فعال	[]	[]	[]	[]	[]

م.م	العبارات	1	2	3	4	5
		لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
المحور السادس: تنمية القدرات البشرية ونشر الوعي بالأمن السيبراني						
1	تحرص الجامعة على تنفيذ برامج تدريبية منتظمة لتنمية قدرات الموظفين في مجال الأمن السيبراني	[]	[]	[]	[]	[]
2	يتم نشر الوعي بمخاطر الأمن السيبراني وسبل الوقاية منها بين منسوبي الجامعة بدرجة كافية	[]	[]	[]	[]	[]
3	يسهم مستوى الوعي السيبراني لدى الموظفين في الحد من المخاطر السيبرانية داخل الجامعة بدرجة ملحوظة	[]	[]	[]	[]	[]

Abstract

This study aimed to analyze the role of risk management practices in enhancing the effectiveness of cybersecurity in Saudi universities, using King Saud bin Abdulaziz University for Health Sciences as a case study. The study focused on examining the relationship between risk management practices and several dimensions related to cybersecurity effectiveness, including institutional integration between risk management and cybersecurity, organizational and technical challenges associated with cybersecurity implementation, the effectiveness of regulatory frameworks, policies and procedures, as well as human capacity development and the promotion of cybersecurity awareness.

The study adopted the descriptive analytical approach, and a questionnaire was used as the primary tool for data collection from the study sample. Means and standard deviations were used to analyze the study variables, and Pearson's correlation coefficient was applied to test the study hypotheses.

The results indicated that the level of risk management practices and cybersecurity effectiveness at the university was very high. The findings also revealed a statistically significant positive relationship between risk management practices and cybersecurity effectiveness. In addition, the results showed statistically significant positive relationships between risk management practices and institutional integration, organizational and technical challenges, the effectiveness of regulatory frameworks, policies and procedures, and human capacity development and cybersecurity awareness.

The results further indicated that strengthening risk management practices contributes to supporting institutional integration, improving organizational policies and procedures, and enhancing cybersecurity awareness among employees, which helps increase the level of digital protection within educational institutions.

In light of these findings, the study recommends strengthening institutional integration between risk management departments and cybersecurity and information technology units, developing cybersecurity training and awareness programs, attracting specialized human resources, and updating regulatory policies and procedures in accordance with national and international cybersecurity standards.

Keywords: Risk Management, Cybersecurity, Institutional Integration, Governance, Saudi Universities.

Midocean University

College of Management

Risk Management Master of



Title in English

**The Role of Risk Management in Enhancing Cybersecurity in Saudi Universities:
A Case Study of King Saud bin Abdulaziz University for Health Sciences**

Prepared by:

Rawa Abdulaziz Almaziad

Academic Number:

252001156

Supervised by:

Dr. Alfaisal Abdelhameed Mohamed

Dr. Fayez Ali Jrad

Year: 2026-1447