

عنوان البحث

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

إعداد الطالبة/

روى عبد العزيز محمد المزيد
الرقم الجامعي: ٢٥٢٠٠١١٥٦

إشراف/

د. الفيصّل عبد الحميد
د. فايز جراد

العام الدراسي:

٢٠٢٥ م / ١٤٤٧ هـ

فهرس المحتويات

3	مقدمة:
5	مشكلة الدراسة:
6	أهمية الدراسة:
6	أولاً: الأهمية العلمية:
6	ثانياً: الأهمية العملية:
7	أهداف الدراسة:
8	تساؤلات الدراسة:
8	سؤال البحث الرئيسي:
8	أسئلة البحث الفرعية:
8	فروض الدراسة:
8	الفرضية الرئيسية:
8	الفرضيات الفرعية:
9	الدراسات السابقة:
15	المنطلقات النظرية للدراسة:
17	المنهجية وطرق البحث:
18	أدوات الدراسة:
18	حدود الدراسة:
19	المراجع:

مقدمة:

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 (البيشي، 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 اهتمامًا كبيرًا 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 شهدها قطاع التعليم العالي في المملكة العربية السعودية في مجال التحول الرقمي وتطوير بنيته التقنية، وما رافق ذلك من توسّع 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 الممنّي 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:

تنبع 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.

تسعى 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). 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:

ومعايير تقييم تساعد القيادات الجامعية وصناع القرار في متابعة مدى (KPIs) توفر الدراسة مؤشرات قياس أداء 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، ويحد 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 أبرز فئات المخاطر السيبرانية المحتملة في بيئة الجامعات السعودية، وكيف تُدار ضمن الأطر والسياسات المؤسسية لإدارة المخاطر؟
- السؤال الفرعي الثالث: كيف يسهم التكامل المؤسسي بين إدارة المخاطر ووحدة الأمن السيبراني في تعزيز الوقاية من التهديدات والاستجابة لها؟
- السؤال الفرعي الرابع: ما أهم التحديات التنظيمية والتقنية التي تعيق تحقيق التكامل الفعّال بين إدارة المخاطر والأمن السيبراني في الجامعات السعودية؟

فروض الدراسة:

الفرضية الرئيسية:

توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق إدارة المخاطر وفاعلية الأمن السيبراني في جامعة الملك سعود بن عبد العزيز للعلوم الصحية.

الفرضيات الفرعية:

الفرض الأول: يُسهم تطبيق مبادئ إدارة المخاطر في تعزيز مستوى أمن المعلومات وحماية الأنظمة التقنية بالجامعة.

الفرض الثاني : يؤدي التكامل بين إدارة المخاطر ووحدة الأمن السيبراني إلى رفع كفاءة الوقاية من التهديدات والاستجابة للحوادث الرقمية.

الفرض الثالث : تؤثر وضوح السياسات والإجراءات التنظيمية في رفع مستوى الجاهزية السيبرانية وضمان استمرارية الخدمات الأكاديمية والإدارية.

الفرض الرابع: تمثل التحديات التنظيمية والتقنية أحد العوامل التي تحدّ من فاعلية التكامل بين إدارة المخاطر والأمن السيبراني داخل الجامعة.

الفرض الخامس : ينعكس مستوى الوعي والتدريب لدى منسوبي الجامعة على فاعلية تطبيق ممارسات إدارة المخاطر وتحقيق الأمن السيبراني الشامل.

الدراسات السابقة:

1-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.

2-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.

3-دراسة (2021, Almomani, I., Ahmed, M., & Maglaras, L.) بعنوان:
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 ISO و NIST 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، خصوصًا 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.

4-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.

5-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.

6-دراسة (الحري، 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 شدّدت 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.

7-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 تحد 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 أكدت 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.

8-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 خصيصًا 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 لتناسب الجامعات، بالإضافة إلى رفع وعي العاملين والتدريب المستمر واستحداث مؤشرات أداء واضحة للحماية السيبرانية في البيئة الجامعية السعودية.

9-دراسة (الهزاني، 2023) بعنوان: ضوابط ومتطلبات تطبيق الأمن السيبراني في جامعة الأميرة نورة بنت عبدالرحمن.

-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.

10-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.

من خلال الاعتماد على نماذج ونظريات (Deductive Approach) استخدمت الدراسة منهج الاستدلال الاستنباطي مسبقاً 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 يساهمان 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.

المنطلقات النظرية للدراسة:

تركز المنطلقات النظرية لهذه الدراسة على أن فاعلية الأمن السيبراني في جامعة الملك سعود بن عبد العزيز للعلوم الصحية تعتمد بدرجة كبيرة على مدى تبني ممارسات إدارة المخاطر المؤسسية وتكاملها مع الأطر الوطنية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني. ويُعد هذا التكامل عنصراً محورياً في تحقيق استمرارية الأعمال وحماية البيانات الحساسة وضمان استدامة الخدمات الأكاديمية والإدارية في بيئة التعليم العالي الرقمية. ويُعد المطلق النظري أحد الركائز الأساسية في هذه الدراسة، إذ يمثل الأساس الذي تُبنى عليه فرضيات البحث وتُفسّر من خلاله العلاقات بين المتغيرات محل الدراسة. كما يوفر هذا الإطار قاعدة معرفية ومنهجية تساعد على فهم المفاهيم النظرية المرتبطة بموضوع البحث وتوضيح العلاقة بين إدارة المخاطر والأمن السيبراني من منظور الحوكمة المؤسسية.

تستند هذه الدراسة في إطارها النظري إلى مجموعة من الأطر والمراجع الوطنية والدولية التي تشكّل الأساس العلمي لفهم العلاقة بين إدارة المخاطر والأمن السيبراني في المؤسسات التعليمية. فقد أكد إطار إدارة المخاطر المؤسسية والمعيار الدولي لإدارة المخاطر على أن إدارة المخاطر تمثل جزءاً جوهرياً من نظام الحوكمة المؤسسية، وأن تكاملها مع عمليات التخطيط وصنع القرار يساهم في تحقيق الأداء المؤسسي الفعال واستدامة الأعمال. كما تُعد الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني إطاراً وطنياً شاملاً يهدف إلى تعزيز الحماية الرقمية للمؤسسات وضمان سلامة الأنظمة والمعلومات، من خلال توحيد الممارسات التقنية والتنظيمية وفق معايير متوافقة مع الأطر العالمية وبناءً على هذه الأطر، تنطلق الدراسة من فرضية أن التكامل بين إدارة المخاطر والأمن السيبراني يشكل عنصراً محورياً في رفع كفاءة الحوكمة الرقمية وضمان حماية الأصول المعلوماتية في الجامعات السعودية.

أولاً: إدارة المخاطر المؤسسية

تُعرّف إدارة المخاطر بأنها: الأنشطة المنسقة لتوجيه المنظمة والسيطرة عليها فيما يتعلق بالمخاطر. وتُعد عملية منهجية تهدف إلى تحديد المخاطر المحتملة، وتحليلها، وتقييمها، ووضع الاستراتيجيات اللازمة لمعالجته (ISO 31000, 2018).

ثانياً: 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، ويشمل كذلك أمن المعلومات والأمن الإلكتروني والأمن الرقمي. وقد أكدت الضوابط الأساسية للأمن السيبراني على أن تحقيق الأمن السيبراني يتطلب تكامل الأدوار والمسؤوليات بين الإدارات الفنية والإدارية، وتبني نهج إداري يوازن بين الحماية التقنية والحوكمة المؤسسية (ECC-2:2024).

ثالثاً: العلاقة التكاملية بين إدارة المخاطر والأمن السيبراني

يُعد التكامل بين إدارة المخاطر والأمن السيبراني ضرورة استراتيجية في المؤسسات الحديثة، إذ يساهم في بناء نظام شامل لتحديد التهديدات التقنية وتحليلها والتخطيط المسبق للاستجابة لها. وتُظهر الدراسات الحديثة أن تبني منهجية إدارة المخاطر المؤسسية (ERM) ضمن إطار الأمن السيبراني يؤدي إلى تعزيز الجاهزية السيبرانية، وتقليل احتمالية وقوع الحوادث الرقمية، وتحسين كفاءة الاستجابة في حال وقوعها. كما أن هذا التكامل يعزز الحوكمة المؤسسية من خلال وضوح الأدوار والمسؤوليات وتكامل الإجراءات بين الإدارات المعنية مثل إدارة المخاطر ووحدة الأمن السيبراني وإدارة تقنية المعلومات.

رابعاً: الإطار الوطني والدولي الداعم للتكامل.

1- المعيار الدولي ISO 31000:2018

- يوفّر إطاراً عالمياً لإدارة المخاطر يمكن تطبيقه في مختلف القطاعات.

- يؤكد على دمج إدارة المخاطر ضمن أنشطة القيادة والتخطيط وصنع القرار المؤسسي.

2- إطار (2017) COSO ERM

- يربط إدارة المخاطر بالأداء المؤسسي والاستراتيجية .

- يُشجع على اتخاذ القرارات المبنية على تحليل المخاطر وتعزيز القيمة التنظيمية.

3- ضوابط الهيئة الوطنية للأمن السيبراني (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.

المنهجية وطرق البحث:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي لملاءمته لطبيعة الموضوع الذي يهدف إلى تحليل دور إدارة المخاطر في تعزيز الأمن السيبراني داخل البيئة الجامعية. ويركز هذا المنهج على وصف الظاهرة كما هي في الواقع وتحليل العلاقات بين متغيراتها لفهم مستوى التكامل بين إدارة المخاطر ووحدة الأمن السيبراني في جامعة الملك سعود بن عبدالعزيز للعلوم الصحية .

يُستخدم المنهج الوصفي التحليلي في هذه الدراسة لتحديد مدى تطبيق ممارسات إدارة المخاطر في مجال الأمن السيبراني، وتحليل السياسات والإجراءات التنظيمية ذات الصلة لتقييم اتساقها مع المعايير الوطنية والدولية، بما في ذلك الضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني. ويسهم هذا الأسلوب في تفسير واقع التكامل المؤسسي بين الجوانب الإدارية والتقنية المرتبطة بحوكمة الأمن السيبراني.

كما تم توظيف المنهج التحليلي في الجانب التطبيقي من خلال الربط بين نتائج الاستبيان والسياسات والإجراءات التنظيمية الخاصة بالأمن السيبراني وإدارة المخاطر، بهدف الوصول إلى نتائج علمية دقيقة واستنتاجات عملية تسهم في تطوير الأطر والسياسات المؤسسية وتعزيز كفاءة منظومة الأمن السيبراني في مؤسسات التعليم العالي.

أدوات الدراسة :

تم إعداد الاستبانة لتناسب مع متغيرات هذه الدراسة، وذلك بالاعتماد على الأدبيات والدراسات السابقة ذات الصلة بموضوع إدارة المخاطر والأمن السيبراني في مؤسسات التعليم العالي.

تكوّنت الاستبانة من قسمين رئيسيين:

القسم الأول:

يتعلق بالبيانات الديموغرافية لعينة الدراسة من منسوبي جامعة الملك سعود بن عبدالعزيز للعلوم الصحية بمدينة الرياض، وشمل المتغيرات: الجنس، المؤهل العلمي، المسعى الوظيفي، وسنوات الخبرة.

القسم الثاني:

اشتمل على الفقرات والأبعاد التي تقيس متغيرات الدراسة المستقلة والتابعة، حيث تناول متغير إدارة المخاطر بوصفه المتغير المستقل، ومتغير الأمن السيبراني بوصفه المتغير التابع، لقياس مستوى التكامل بينهما داخل جامعة الملك سعود بن عبدالعزيز للعلوم الصحية.

حدود الدراسة :

الحدود الموضوعية: تركز الدراسة على تحليل العلاقة بين إدارة المخاطر والأمن السيبراني في بيئة الجامعات السعودية، من خلال تقييم التكامل المؤسسي بين الوحدتين، واستبعاد الجوانب التقنية البحتة التي لا ترتبط بالإدارة أو السياسات التنظيمية.

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

الحدود الزمانية: تشمل فترة الدراسة العام الأكاديمي 2024-2025م، وهي المدة التي يتم خلالها جمع البيانات وتحليل السياسات ذات العلاقة.

الحدود البشرية: تقتصر عينة الدراسة على منسوبي الجامعة من الإدارات ذات العلاقة مثل إدارة المخاطر، ووحدة الأمن السيبراني، وإدارة تقنية المعلومات، وعدد من أعضاء هيئة التدريس والموظفين الإداريين ذوي الصلة بالتحول الرقمي.

المراجع:

- 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>
- 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.
- 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، جهمان؛ سلامي، هدى؛ كليبي، 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>
- 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-للامن-السيبراني-.pdf>
- Alharbi, Talal. (2022). Developing a Cost-effective Cybersecurity Management System for Academic Institutions in Saudi Arabia. Journal of Engineering and Applied Sciences ,9(1)74 –57
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/>

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/ccc-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