

فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية
السعودية في ضوء التحول الرقمي

إعداد الطالب/

مشاري علي العريني

الرقم الجامعي/

253000115

إشراف/

د. الفيصّل عبد الحميد محمد حسن

د. فايز جرّاد

العام الدراسي

2026م

قائمة المحتويات

3.....	المقدمة
4.....	مشكلة الدراسة
5.....	أهمية الدراسة
6.....	أهداف الدراسة
7.....	تساؤلات الدراسة
7.....	فرضيات الدراسة
8.....	الدراسات السابقة
12.....	المنطلقات النظرية للدراسة
14.....	المنهجية وطرق البحث
15.....	أدوات الدراسة
16.....	حدود الدراسة
18.....	المراجع

المقدمة

يشهد العالم اليوم تحولات رقمية متسارعة أطلقت عصر الاعتماد المكثف على التقنيات الرقمية في جميع القطاعات، بما في ذلك الجهات الحكومية، حيث أصبحت الأنظمة الإلكترونية والخدمات الرقمية تشكل العمود الفقري لتقديم الخدمات للمواطنين والمستفيدين. وقد أدت هذه التحولات إلى تعزيز الكفاءة وسرعة الوصول إلى المعلومات، لكنها في الوقت ذاته خلقت تحديات جديدة مرتبطة بالأمن السيبراني، إذ أصبحت البيانات الحكومية والمعلومات الحساسة أكثر عرضة للتهديدات الإلكترونية والهجمات الرقمية المتطورة. ومن هذا المنطلق، باتت فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني قضية محورية لضمان استمرارية العمليات الحكومية وحماية المعلومات الحيوية، بما يعزز الثقة في الأنظمة الرقمية ويضمن تحقيق أهداف التحول الرقمي (Radebe، 2024).

تعتبر إدارة مخاطر الأمن السيبراني عملية شاملة تهدف إلى التعرف على التهديدات السيبرانية، تقييم مدى تأثيرها على الجهات الحكومية، ووضع الإجراءات الوقائية والتصحيحية للحد من تلك المخاطر. ويشمل ذلك تطوير سياسات أمنية متكاملة، تبني ضوابط تقنية وإدارية، وإجراء تقييم دوري للمخاطر لضمان قدرة الجهات الحكومية على الاستجابة السريعة لأي تهديد. وتشير الدراسات الحديثة إلى أن فاعلية هذه الاستراتيجيات تعتمد بشكل كبير على مدى دمجها مع أهداف التحول الرقمي، حيث تضمن الاستمرارية التشغيلية، حماية البيانات، والامتثال للمعايير الوطنية والدولية للأمن السيبراني (Melaku، 2023).

في المملكة العربية السعودية، أطلقت الحكومة برامج متعددة لتعزيز التحول الرقمي ضمن رؤية المملكة 2030، مما أدى إلى تبني حلول تقنية متقدمة في تقديم الخدمات العامة وربط الجهات الحكومية بأنظمة معلومات موحدة. ومع هذا التوسع الرقمي، برزت الحاجة إلى تطوير استراتيجيات إدارة مخاطر الأمن السيبراني بشكل يتماشى مع البيئة الرقمية الجديدة، بحيث لا تقتصر على الوقاية من الهجمات، بل تشمل أيضًا إدارة المخاطر التشغيلية، حماية المعلومات، وضمان استمرارية تقديم الخدمات الرقمية للمستفيدين. ومن هنا، تنبع أهمية هذه الدراسة في تسليط الضوء على فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية، وفهم مدى جاهزيتها لمواجهة التهديدات الرقمية المعقدة، وتحقيق التوازن بين التقدم الرقمي وحماية المعلومات الحساسة (Hossain، 2025).

تهدف الدراسة إلى تقديم رؤية علمية وتحليلية تمكن الجهات الحكومية من تحسين استراتيجيات إدارة المخاطر السيبرانية، بما يسهم في تعزيز الثقة في التحول الرقمي، حماية الأصول المعلوماتية، وتحقيق الاستفادة القصوى من التقنية في تقديم الخدمات العامة. كما تسعى الدراسة إلى تحديد التحديات والمعوقات التي تواجه تنفيذ هذه الاستراتيجيات، وتقديم توصيات عملية لتعزيز الفاعلية والكفاءة في مواجهة التهديدات السيبرانية الحديثة، بما يضمن استدامة الأمن الرقمي والمواءمة مع أهداف التنمية الوطنية.

مشكلة الدراسة

تواجه الجهات الحكومية في المملكة العربية السعودية تحديات متزايدة في مجال الأمن السيبراني نتيجة التحول الرقمي السريع الذي تشهده الدولة في إطار رؤية المملكة 2030. فالتوسع في استخدام الخدمات الرقمية، وأنظمة المعلومات الإلكترونية الموحدة، ورفع مستوى الاتصال الرقمي بين الجهات الحكومية والمستفيدين، على الرغم من فوائده الكبيرة في تحسين الكفاءة وجودة الخدمات، فإنه يعرض هذه الجهات لمخاطر سيبرانية متعددة تتراوح بين الاختراقات الأمنية، سرقة البيانات، الهجمات الإلكترونية المنظمة، وحتى التهديدات المتعلقة بالبرمجيات الخبيثة والهجمات على البنية التحتية الرقمية الحيوية. ويلاحظ أن بعض الجهات الحكومية لم تطبق استراتيجيات إدارة المخاطر السيبرانية بشكل شامل أو متكامل، مما يؤدي إلى فجوات في حماية البيانات وانخفاض القدرة على الاستجابة الفورية للتهديدات الرقمية، وبالتالي ضعف فاعلية النظام الرقمي بشكل عام.

ومن هنا، تنبع المشكلة الرئيسية للدراسة: ما مدى فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي؟. إذ إن عدم كفاءة هذه الاستراتيجيات أو ضعف تطبيقها يمكن أن يؤدي إلى عدد من المشكلات المترتبة، أهمها:

- زيادة احتمالية التعرض للهجمات السيبرانية بسبب ضعف الإجراءات الوقائية وعدم تكامل الضوابط التقنية والإدارية.
- فقدان البيانات والمعلومات الحساسة ما يؤثر على الثقة في الخدمات الحكومية الرقمية ويهدد الخصوصية وحماية المواطنين.

- انقطاع أو تعطيل الخدمات الرقمية ما يؤدي إلى ضعف الأداء المؤسسي وتأخر تقديم الخدمات الحيوية للمستفيدين.
- ارتفاع التكاليف التشغيلية نتيجة استجابة الجهات الحكومية للأزمات الناتجة عن الهجمات السيبرانية أو التهديدات الأمنية.
- ضعف التوافق مع معايير الحوكمة والأمن السيبراني الوطنية والدولية، مما قد يعيق تحقيق أهداف التحول الرقمي وتعزيز الاستدامة الرقمية (Abn_hammad، 2025).

استناداً إلى مشكلة الدراسة الرئيسية والمشكلات المترتبة عليها، يطرح البحث السؤال الرئيسي الذي يحدد محور الدراسة ويقود عملية التحليل والبحث العلمي: ما مدى فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، وما تأثير هذه الاستراتيجيات في حماية البيانات وضمان استمرارية تقديم الخدمات الرقمية؟

أهمية الدراسة

- الأهمية العلمية

تكتسب هذه الدراسة أهميتها العلمية من مساهمتها في توسيع المعرفة النظرية حول إدارة مخاطر الأمن السيبراني في القطاع الحكومي، خاصة في ظل التحول الرقمي المتسارع الذي تشهده المملكة العربية السعودية. إذ تمثل إدارة المخاطر السيبرانية عنصراً محورياً في ضمان استمرارية العمليات الرقمية وحماية البيانات الحكومية الحساسة، وبالتالي فهي تدخل ضمن الدراسات الحديثة في الإدارة العامة والأمن الرقمي. وتسعى الدراسة إلى تطوير إطار نظري متكامل يربط بين استراتيجيات إدارة المخاطر، فاعلية تنفيذها، وتحقيق أهداف التحول الرقمي، مع مراعاة الخصائص المحلية للبيئة الحكومية السعودية. كما توفر الدراسة قاعدة علمية للبحوث المستقبلية من خلال قياس أثر السياسات والإجراءات الوقائية على الحد من المخاطر السيبرانية، وتحليل العوامل التي تؤثر في فاعلية الاستراتيجيات المعتمدة، ما يساهم في إثراء الأدبيات المتعلقة بالأمن الرقمي، الحوكمة الإلكترونية، وإدارة المخاطر في المؤسسات العامة (Haque، 2025).

- الأهمية العملية

من الناحية العملية، تهدف الدراسة إلى تقديم توصيات تطبيقية تساعد الجهات الحكومية في المملكة على تعزيز فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني وتحسين قدرتها على مواجهة التهديدات الرقمية. فنتائج الدراسة توفر للجهات المسؤولة عن الأمن الرقمي إطاراً عملياً لتقييم الوضع الحالي، تحديد نقاط القوة والضعف في الاستراتيجيات المعتمدة، ووضع خطط تحسين مستمرة تتماشى مع متطلبات التحول الرقمي. كما تساعد الدراسة في رفع مستوى الوعي لدى صناع القرار حول أهمية حماية البيانات، ضمان استمرارية الخدمات الرقمية، وتقليل الخسائر الناتجة عن الهجمات الإلكترونية. وبذلك، تسهم الدراسة في تعزيز الثقة العامة في الخدمات الحكومية الرقمية، وتحسين كفاءة الأداء المؤسسي، فضلاً عن دعم الاستدامة الرقمية وتطوير بيئة أمن سيبراني قوية تواكب التطورات التكنولوجية العالمية مع مراعاة الخصوصية والقيم الوطنية (Johri، 2023).

أهداف الدراسة

الهدف الرئيسي

- تهدف الدراسة إلى تقييم فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، بما يسهم في تعزيز حماية البيانات، ضمان استمرارية الخدمات الرقمية، وتحقيق الاستفادة القصوى من التحول الرقمي في القطاع الحكومي.

الأهداف الفرعية

1. تحديد الاستراتيجيات المعتمدة لإدارة مخاطر الأمن السيبراني في الجهات الحكومية السعودية.
2. تقييم مدى فاعلية تطبيق هذه الاستراتيجيات في حماية البيانات والمعلومات الحساسة.
3. تحليل العلاقة بين جودة استراتيجيات إدارة المخاطر والأداء الرقمي للخدمات الحكومية.
4. تحديد المعوقات التي تواجه الجهات الحكومية في تنفيذ استراتيجيات الأمن السيبراني.
5. تقديم توصيات عملية لتعزيز فاعلية إدارة المخاطر السيبرانية وتحسين قدرة الجهات الحكومية على مواجهة التهديدات الرقمية.

تساؤلات الدراسة

التساؤل الرئيسي للدراسة

- ما مدى فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي؟

التساؤلات الفرعية

1. ما هي الاستراتيجيات الرئيسية المتبعة في إدارة مخاطر الأمن السيبراني في الجهات الحكومية؟
2. كيف يمكن قياس فاعلية هذه الاستراتيجيات في حماية البيانات والمعلومات الحكومية؟
3. ما العلاقة بين تطبيق استراتيجيات إدارة المخاطر السيبرانية وتحقيق أهداف التحول الرقمي؟
4. ما هي التحديات والمعوقات التي تواجه الجهات الحكومية في تنفيذ استراتيجيات الأمن السيبراني؟
5. ما الحلول والتوصيات العملية التي يمكن اتباعها لتعزيز فاعلية إدارة المخاطر السيبرانية؟

فرضيات الدراسة

الفرضية الرئيسية

- استراتيجيات إدارة مخاطر الأمن السيبراني المطبقة في الجهات الحكومية بالمملكة العربية السعودية تؤثر بشكل إيجابي وذو دلالة إحصائية على فاعلية حماية البيانات وضمان استمرارية الخدمات الرقمية في ضوء التحول الرقمي.

الفرضيات الفرعية

1. هناك علاقة إيجابية بين وضوح الاستراتيجيات المعتمدة لإدارة المخاطر السيبرانية وفاعلية حماية البيانات.
2. استخدام الإجراءات التقنية والإدارية الحديثة في إدارة المخاطر يعزز قدرة الجهات الحكومية على الاستجابة للتهديدات الرقمية.
3. التدريب والتوعية المستمرة للعاملين في الأمن السيبراني يزيد من فاعلية تنفيذ الاستراتيجيات المتبعة.
4. المعوقات التنظيمية والتقنية تؤثر سلبًا على فاعلية استراتيجيات إدارة المخاطر السيبرانية.

5. تطبيق استراتيجيات متكاملة ومرنة لإدارة المخاطر يساهم في تحسين الأداء الرقمي وتحقيق أهداف التحول

الرقمي في الجهات الحكومية.

الدراسات السابقة

تزايد استخدام المؤسسات السعودية للتقنيات الرقمية. ورغم الجهود المبذولة للاستفادة من التحول الرقمي، إلا أن قلة من الشركات حققت نتائج ملموسة. وقد ربطت دراسات عديدة نجاح أو فشل عملية التحول الرقمي بالموظفين. وقد طرحت دراسة (Assiri، 2022) ثلاث فرضيات تتعلق بأمن التحول الرقمي، تشمل تحديد كيفية تطور الأمن نتيجةً لتزايد استخدام الأنظمة الرقمية، بالإضافة إلى تحديد أفضل استراتيجيات إدارة المخاطر. وستلحق مجموعة من الجهات السعودية العامة والخاصة استبيانًا إلكترونيًا كجزء من هذه الدراسة. وخلصت الدراسة إلى أنه مع نمو التحول الرقمي، تزايد مخاطر الأمن، مما يستلزم تطبيق نظام أمني قوي وأكثر تدابير إدارة المخاطر فعالية. كما يجب على الشركات إشراك موظفيها في تطوير وتنفيذ التحول الرقمي للحفاظ على ولائهم. كذلك، يجب على جميع الموظفين فهم أهداف التحول الرقمي وغاياته وخطته والموافقة عليها. ويستطيع قادة الأعمال الناجحون بناء رؤية ملهمة، وتوحيد جهود الموظفين، وإشراكهم في تبني أساليب جديدة في العمل.

يُعد أمن المعلومات وخصوصيتها في الخدمات العامة من الاعتبارات الأساسية في عصرنا الرقمي، حيث تعتمد الحكومات بشكل متزايد على التكنولوجيا لتقديم الخدمات بكفاءة مع الحفاظ على سرية المعلومات الحساسة. ويعتمد نجاح استخدام هذه الخدمات الإلكترونية على مستوى ثقة المواطنين في قنوات الحكومة الإلكترونية. لذا، ينبغي أن يراعي تصميم مؤسسات الخدمة العامة سهولة استخدام ضوابط الأمان. في هذه الدراسة (Saeed، 2025)، نعرض نتائج دراسة كمية أُجريت في المملكة العربية السعودية لفهم تصورات المستخدمين النهائيين حول أمن المعلومات وخصوصيتها في استخدامهم للخدمات العامة. وبناءً على هذه النتائج، نقدم نموذجًا لتحسين جوانب أمن المعلومات وخصوصيتها، مما يُساعد صانعي السياسات والممارسين على تحسين تقديم الخدمات العامة إلكترونيًا. ويمكن تطوير هذا النموذج في سياقات جغرافية مختلفة لتعزيز الأمن السيبراني في تقديم خدمات الحكومة الإلكترونية من خلال تضافر جهود المواطنين ومؤسسات تقديم الخدمات والهيئات الحكومية المعنية بالأمن السيبراني.

تتبنى المملكة العربية السعودية التحول الرقمي وخدمات الحكومة الإلكترونية، بهدف تحسين الكفاءة وسهولة الوصول والتركيز على المواطن. ومع ذلك، تواجه المملكة تحديات، منها التهديدات السيبرانية المتطورة. تهدف هذه

الدراسة إلى بحث العوامل المؤثرة على ممارسات الأمن السيبراني لضمان موثوقية وأمن خدمات الحكومة الإلكترونية. تبحث دراسة (Al-Hawamleh، 2024) في الديناميكيات المتعددة الأوجه لممارسات الأمن السيبراني وتأثيرها على جودة وفعالية خدمات الحكومة الإلكترونية. تشمل العوامل الرئيسية التي تم استكشافها: الثقافة التنظيمية، والبنية التحتية التقنية، والالتزام بالمعايير واللوائح، وتدريب الموظفين وتوعيتهم، والاستثمار المالي في الأمن السيبراني. استخدمت هذه الدراسة المنهج الكمي لجمع البيانات من 320 مشاركًا. جمع الباحث 285 استبيانًا مكتملًا، بعد استبعاد الإجابات غير الصالحة أو غير المكتملة، وحلل مجموعة البيانات النهائية باستخدام نمذجة المعادلات الهيكلية للمربعات الصغرى الجزئية. تُظهر النتائج أن الاستثمار المالي في الأمن السيبراني، وتدريب الموظفين، ورفع مستوى الوعي والالتزام بلوائح الأمن السيبراني، يؤثر بشكل كبير على تبني ممارسات فعالة في هذا المجال. مع ذلك، فإن العلاقة بين ثقافة المؤسسة وممارسات الأمن السيبراني ليست واضحة تمامًا. يُثبت البحث وجود ارتباط إيجابي قوي بين ممارسات الأمن السيبراني وجودة خدمات الحكومة الإلكترونية، مُسلطًا الضوء على دور الأمن في تعزيز ثقة الجمهور ورضا المستخدمين، وتلبية الاحتياجات المتغيرة للمواطنين والشركات. يُساهم هذا البحث بأدلة تجريبية قيّمة في مجال الحكومة الإلكترونية والأمن السيبراني، مُقدمًا رؤى تُسهم في اتخاذ قرارات سياساتية قائمة على الأدلة، وتخصيص الموارد بشكل فعال. من خلال فهم الديناميكيات الدقيقة المؤثرة، تُصبح المملكة العربية السعودية في وضع أفضل لتعزيز بنيتها التحتية للحكومة الرقمية، وتوفير خدمات حكومية إلكترونية آمنة وعالية الجودة لمواطنيها.

حققت المملكة العربية السعودية إنجازات بارزة في مجال الأمن السيبراني. فقد حافظت على آليات تنظيمية متينة لمنع الجرائم الإلكترونية وتعقب مرتكبيها ومعاقبتهم، وذلك لحماية مصالح الأفراد والمؤسسات من مخاطر سرقة البيانات واختلاسها. ويعزز الاستخدام الواسع لتقنية المعلومات وخدماتها التدابير الأمنية. وتُعدّ التهديدات السيبرانية المتطورة باستمرار موضوعًا يثير نقاشًا واسعًا. وفي هذا السياق، تُقدّم دراسة (Alhakami، 2024) نظرة شاملة على كيفية تطور الجرائم الإلكترونية في المملكة العربية السعودية حاليًا، كما تُلقي نظرة على بعض أبرز الهجمات التي شهدتها المنطقة. ويهدف الإطار التشريعي والتدابير الحالية في المملكة إلى ردع النشاط الإجرامي عبر الإنترنت. وقد وُضعت نماذج كفاءة مختلفة لتلبية الكفاءات اللازمة في مجال مكافحة الجرائم الإلكترونية. ويمكن للباحثين المتخصصين في هذا المجال الاستفادة بشكل أكبر من خلال تطوير مستوى كفاءة متقدم لتحقيق أعلى مستويات الأمن. للإجابة على هذا السؤال البحثي، يستخدم هذا التقييم منهجية مختبر تجارب وتقييم اتخاذ القرارات الضبابية (Fuzzy-DMTAE)،

وعملية التحليل الهرمي الضبابية (F.AHP)، ومنهجية TOPSIS الضبابية لتحقيق تطوير الكفاءات القطاعية في سياسة الأمن السيبراني. كما يناقش أوجه التشابه والاختلاف بين هذه المنهجيات الثلاث. وقد أظهر تحليل الأمن السيبراني أن المركز الوطني للأمن السيبراني يحظى بأعلى أولوية. وتختتم الدراسة باستعراض التحديات التي لا تزال بحاجة إلى دراسة وحل لتفعيل آليات أمن إلكتروني أكثر موثوقية وفعالية، بما يسهم في بناء اقتصاد أكثر قوة قائم على خدمات تكنولوجيا المعلومات في المملكة العربية السعودية. علاوة على ذلك، يحتاج متخصصو الأمن السيبراني وصناع السياسات إلى توحيد جهودهم لحماية الأصول الرقمية للبلاد في عصر الحرب السيبرانية العلنية والسرية.

يتمحور عصرنا الحالي حول تكنولوجيا المعلومات، إذ نشهد نهضةً في مجال المعلومات وتوسعها على مستويات ومجالات متعددة. ويسعى المتخصصون في التكنولوجيا، ممن يمتلكون معرفةً واسعةً بها وشغفًا كبيرًا بها، إلى نشر هذه المعلومات ومعالجتها على النحو الأمثل، وقد أصبحت الحواسيب اليوم من أهم الأدوات في العمليات الحكومية. وبدأت الشركات الكبرى بالفعل في استخدامها في معظم قطاعات أعمالها، وساهمت في توجيه بعض الإجراءات الحكومية نحو الحكومة الإلكترونية المشتركة، التي تتيح للمواطنين الوصول إلى الخدمات الحكومية من منازلهم عبر حواسيبهم. ومن الجدير بالذكر أنه مع ازدياد استخدام الحواسيب، ازدادت الجرائم الإلكترونية، مما ساهم في سنّ قوانين في مختلف الدول لمكافحتها. ومع تطور التكنولوجيا، تزايدت تعقيدات هذه التهديدات السيبرانية وتأثيرها، مما يشكل تحديات كبيرة للأمن السيبراني. يناقش دراسة (Alkhalifa, 2024) دور التكنولوجيا في مكافحة الجرائم السيبرانية، واللوائح المنظمة لها، والسلوكيات المسموح بها في استخدامها في المملكة العربية السعودية. كما يحلل البحث الجرائم السيبرانية في المملكة ونظام مكافحتها.

التعليق على الدراسات السابقة:

- أوجه التشابه في الدراسات السابقة

تشارك الدراسات السابقة في التأكيد على الدور المحوري للأمن السيبراني في ضمان فاعلية التحول الرقمي داخل المؤسسات الحكومية والخاصة في المملكة العربية السعودية. فقد أظهرت جميع الدراسات أن نجاح التحول الرقمي يرتبط ارتباطاً وثيقاً بفاعلية استراتيجيات إدارة المخاطر السيبرانية، ومدى تكاملها مع السياسات الإدارية والبيئة التقنية. كما أكدت الدراسات على أهمية تدريب الموظفين وزيادة وعيهم بالأمن السيبراني، وإشراكهم في تبني الإجراءات الوقائية والتقنية الجديدة، بما يضمن استمرارية تقديم الخدمات الرقمية وحماية المعلومات الحساسة. وتشير

الدراسات أيضًا إلى أن الاستثمار المالي في الأمن السيبراني، وتطوير البنية التحتية الرقمية، والتزام الجهات الحكومية بالمعايير واللوائح، يمثلون عوامل مؤثرة في تعزيز فاعلية ممارسات الأمن السيبراني وتحقيق الثقة لدى المستفيدين.

- أوجه الاختلاف في الدراسات السابقة

رغم التشابه في التركيز على الأمن السيبراني والتحول الرقمي، تختلف الدراسات في منهجية البحث والأبعاد التي تناولتها. فبعض الدراسات ركزت على تصورات المستخدمين النهائيين حول أمن المعلومات وخصوصيتها في الخدمات العامة، بينما تناولت دراسات أخرى العوامل التنظيمية والفنية التي تؤثر على جودة الخدمات الإلكترونية مثل الثقافة التنظيمية، والاستثمار المالي، والتدريب والتوعية. كما اختلفت الدراسات في نطاقها المكاني والزمني، فقد ركزت بعض الدراسات على عدد محدود من الجهات الحكومية أو الشركات الخاصة، في حين شملت أخرى جهات متعددة عبر مناطق مختلفة في المملكة. كما تنوعت أدوات البحث بين الاستبيانات الكمية، ونماذج المعادلات الهيكلية، والتقييمات التجريبية المعتمدة على تقنيات التحليل الضبابي، مما أدى إلى اختلاف نتائجها من حيث تحديد أولويات المخاطر وتقييم فاعلية الاستراتيجيات.

- الفجوات البحثية التي يميزها البحث الحالي

تشير مراجعة الدراسات السابقة إلى وجود عدة فجوات يمكن أن يعالجها البحث الحالي. أولاً، هناك نقص في الدراسات التي تربط بشكل مباشر بين فاعلية استراتيجيات إدارة المخاطر السيبرانية وأداء الجهات الحكومية الرقمية في سياق التحول الرقمي، مع مراعاة كافة الأبعاد البشرية، التقنية، والتنظيمية. ثانيًا، معظم الدراسات ركزت على جانب واحد من الأمن السيبراني، مثل حماية البيانات أو تصورات المستخدمين، دون دراسة شاملة تتضمن استراتيجيات الوقاية والاستجابة والتعافي من التهديدات الرقمية. ثالثًا، هناك ندرة في الدراسات التي تقدم توصيات عملية قابلة للتطبيق لتعزيز قدرة الجهات الحكومية على مواجهة المخاطر السيبرانية الحديثة في بيئة التحول الرقمي. أخيرًا، لم تتناول الدراسات السابقة بشكل كافٍ تقييم الفاعلية الشاملة للاستراتيجيات الحالية وقياس أثرها على استمرارية الخدمات الرقمية، وهو ما يمثل مساهمة جوهرية للبحث الحالي في سد هذه الفجوات وتقديم رؤى علمية وعملية متكاملة لدعم الأمن السيبراني في المملكة.

المنطلقات النظرية للدراسة

- مفهوم إدارة مخاطر الأمن السيبراني

تُعرف إدارة مخاطر الأمن السيبراني بأنها العملية المنهجية التي تهدف إلى التعرف على التهديدات السيبرانية، تقييم المخاطر المرتبطة بها، ووضع استراتيجيات وقائية وتصحيحية للحد من أثارها على المؤسسات. وتشمل هذه العملية مجموعة متكاملة من الإجراءات والسياسات التي تهدف إلى حماية المعلومات والأنظمة الرقمية من الهجمات الإلكترونية، الاختراقات، وسرقة البيانات، فضلاً عن التهديدات المرتبطة بالبنية التحتية الرقمية الحيوية. وتشير الدراسات النظرية إلى أن إدارة المخاطر السيبرانية ليست مجرد إجراءات تقنية، بل تشمل بعداً تنظيمياً وإدارياً يضمن التنسيق بين السياسات الأمنية، التقنيات المستخدمة، والتدريب المستمر للعاملين في المؤسسات، بما يعزز قدرة المؤسسة على التكيف مع التهديدات الرقمية المتغيرة باستمرار (Jalali، 2019).

- استراتيجيات إدارة المخاطر السيبرانية

تشمل الاستراتيجيات الفعالة لإدارة المخاطر السيبرانية مجموعة من الإجراءات المنهجية التي تركز على الوقاية، الكشف، الاستجابة، والتعافي من التهديدات. ومن بين هذه الاستراتيجيات: تطوير سياسات أمنية واضحة، استخدام ضوابط تقنية متقدمة، إجراء تقييم دوري للمخاطر، وتطبيق خطط استجابة للطوارئ. وتوضح الأدبيات النظرية أن الاستراتيجيات المرنة والقابلة للتطوير وفق التغيرات التقنية الحديثة تساهم بشكل كبير في تعزيز الفاعلية التشغيلية للجهات الحكومية، وتحافظ على سلامة البيانات والمعلومات الحيوية. كما أن دمج استراتيجيات الإدارة مع أهداف التحول الرقمي يساهم في تحقيق التوازن بين الابتكار التكنولوجي وحماية المعلومات، ويقلل من المخاطر التشغيلية المرتبطة بالتوسع الرقمي في تقديم الخدمات الحكومية (Knowles، 2026).

- فاعلية استراتيجيات الأمن السيبراني

تشير الدراسات النظرية إلى أن فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني تعتمد على مدى تكاملها مع البنية التنظيمية والتقنية للجهة الحكومية، وجودة تنفيذها، وكفاءة الموارد البشرية المعنية. فكلما كانت الاستراتيجيات أكثر

وضوحًا وتطبيقًا بشكل منهجي، زادت القدرة على الوقاية من الهجمات الإلكترونية والاستجابة السريعة لأي تهديد محتمل، ما ينعكس إيجابًا على استمرارية تقديم الخدمات الرقمية للمستخدمين. كما أن تقييم الفاعلية يشمل القدرة على حماية البيانات، الالتزام بالمعايير الوطنية والدولية للأمن السيبراني، وضمان استدامة العمليات الرقمية، مما يجعل تقييم هذه الفاعلية أمرًا جوهريًا لفهم العلاقة بين إدارة المخاطر والأداء الرقمي (Nygard، 2021).

- التحول الرقمي وعلاقته بإدارة المخاطر

يشير التحول الرقمي في الجهات الحكومية إلى استخدام التكنولوجيا الرقمية في تقديم الخدمات، تحسين الكفاءة التشغيلية، وتسهيل الوصول إلى المعلومات والخدمات للمستخدمين. ويبرز التحول الرقمي كعامل رئيسي يضاعف أهمية الأمن السيبراني، إذ أن زيادة الاعتماد على الأنظمة الرقمية تزيد من احتمالية التعرض للتهديدات السيبرانية. ومن هذا المنطلق، يجب أن تكون استراتيجيات إدارة المخاطر السيبرانية مصممة لتتكامل مع أهداف التحول الرقمي، بحيث توفر حماية مستمرة للبيانات والأنظمة، مع تمكين الجهات الحكومية من تحقيق الفاعلية التشغيلية، الابتكار في الخدمات، وتعزيز الثقة العامة في الأنظمة الرقمية الحكومية (Bennouk، 2024).

- التحديات النظرية والتطبيقية

تواجه الجهات الحكومية تحديات متعددة في إدارة المخاطر السيبرانية تشمل التغير السريع في طبيعة التهديدات الرقمية، قلة الموارد المتخصصة، ضعف الوعي الأمني بين الموظفين، وصعوبة دمج استراتيجيات الأمن مع أهداف التحول الرقمي. وتشير الدراسات النظرية إلى أن معالجة هذه التحديات تتطلب اعتماد استراتيجيات شاملة تشمل الجوانب التقنية والتنظيمية والبشرية، مع تقييم مستمر للتهديدات وتحديث السياسات والإجراءات الأمنية بما يتوافق مع المتطلبات المحلية والمعايير العالمية للأمن السيبراني. ويبرز من هذا السياق أن تطوير فاعلية استراتيجيات إدارة المخاطر ليس مجرد مسألة تقنية، بل يمثل عملية متكاملة تشمل التخطيط، التنفيذ، والمتابعة لضمان قدرة الجهات الحكومية على حماية البيانات واستمرارية الخدمات الرقمية بفاعلية (Slapničar، 2025).

المنهجية وطرق البحث

تعتمد هذه الدراسة على المنهجية الكمية كخيار رئيسي لدراسة فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية. وتتميز المنهجية الكمية بقدرتها على قياس المتغيرات بدقة وتحليل العلاقات بينها بأسلوب إحصائي موضوعي، ما يجعلها الأنسب لدراسة العلاقة بين سياسات واستراتيجيات الأمن السيبراني وفعاليتها في حماية البيانات وضمان استمرارية تقديم الخدمات الرقمية. كما أن المنهج الكمي يمكن الباحث من اختبار الفرضيات العلمية التي تم صياغتها استنادًا إلى الإطار النظري، مما يوفر نتائج قابلة للتعميم وتعزز موثوقية الاستنتاجات.

- تصميم البحث

تم تبني التصميم الوصفي-العلاقاتي للدراسة، إذ يسعى البحث أولاً إلى وصف الوضع الحالي لاستراتيجيات إدارة المخاطر السيبرانية في الجهات الحكومية، مع تحليل العناصر الأساسية لهذه الاستراتيجيات من حيث شموليتها وفعاليتها. كما يركز الجانب العلاقتي على تحديد العلاقة بين تطبيق الاستراتيجيات وفعاليتها في حماية البيانات واستمرارية الخدمات الرقمية، إضافة إلى قياس أثر هذه الاستراتيجيات على أداء التحول الرقمي. ويساعد هذا التصميم على توضيح نقاط القوة والضعف في الاستراتيجيات الحالية، وتحليل مدى كفاءتها في مواجهة التهديدات السيبرانية الحديثة، بما يتيح تقديم توصيات علمية وعملية دقيقة.

- مجتمع وعينة البحث

يشمل مجتمع الدراسة جميع الجهات الحكومية السعودية التي تعتمد على الأنظمة والخدمات الرقمية في تقديم خدماتها للمواطنين والمستفيدين. ولضمان دقة البيانات، تم اختيار عينة ممثلة من المسؤولين التنفيذيين والإداريين والفنيين المكلفين بإدارة الأمن السيبراني في هذه الجهات، باعتبارهم الأطراف الأكثر معرفة بتطبيق الاستراتيجيات وفعاليتها. كما تم اعتماد العينة العشوائية الطبقية لتوزيع المستجيبين بحسب مستوى الوظائف ومسؤولياتهم، بما يضمن تمثيل جميع الفئات ذات العلاقة ويعكس الصورة الحقيقية للوضع الأمني السيبراني في الجهات الحكومية المختلفة.

- أدوات جمع البيانات

تم اعتماد الاستبيان الكمي المهيكل والمغلق كأداة رئيسية لجمع البيانات، حيث صُمم ليغطي جميع أبعاد الدراسة، بما يشمل الاستراتيجيات المعتمدة لإدارة المخاطر، وفعاليتها في حماية البيانات، مستوى الالتزام بالإجراءات الأمنية،

وتحديات التنفيذ. وتم استخدام مقياس ليكرت الخماسي لقياس درجة الاتفاق أو الاختلاف مع كل بيان، مما يسهل تحويل البيانات النوعية إلى بيانات كمية قابلة للتحليل الإحصائي. وقد تم اختبار الاستبيان على عينة تجريبية أولية للتأكد من وضوح الأسئلة وملاءمتها، كما تم تقييم موثوقيته باستخدام معامل كرونباخ ألفا لضمان اتساق الإجابات وثباتها.

- أساليب تحليل البيانات

بعد جمع الاستبيانات، تم استخدام مجموعة من الأساليب الإحصائية لتحليل البيانات. شملت هذه الأساليب الإحصاءات الوصفية لتحديد الخصائص الأساسية للمتغيرات، والتحليل الارتباطي لقياس العلاقة بين استراتيجيات إدارة المخاطر وفعاليتها، بالإضافة إلى التحليل الانحداري لتحديد مدى تأثير هذه الاستراتيجيات على حماية البيانات واستمرارية الخدمات الرقمية. كما تم اختبار الفرضيات الفرعية والرئيسية باستخدام الاختبارات الإحصائية المناسبة، مما يضمن موثوقية النتائج ويتيح استخلاص استنتاجات دقيقة تدعم تقديم توصيات عملية للجهات الحكومية. تعكس هذه المنهجية الكمية الممنهجة قدرة الدراسة على تقديم تحليل علمي شامل لفاعلية استراتيجيات إدارة مخاطر الأمن السيبراني، وتتيح استكشاف العلاقة بين هذه الاستراتيجيات والأداء الرقمي للجهات الحكومية، بما يساهم في تعزيز أمن المعلومات، استدامة الخدمات الرقمية، وتحقيق أهداف التحول الرقمي في المملكة.

أدوات الدراسة

تمثل أدوات الدراسة الركيزة الأساسية لجمع المعلومات وتحليلها في ضوء المنهجية الكمية المعتمدة في هذا البحث، إذ تهدف إلى توفير بيانات دقيقة وقابلة للتحليل الإحصائي حول فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية. واعتمدت الدراسة على الاستبيان الكمي المهيكل والمغلق كأداة رئيسية لجمع البيانات، نظرًا لقدرته على قياس المتغيرات بطريقة منظمة وموضوعية، وتحويل الآراء والملاحظات إلى بيانات رقمية قابلة للتحليل.

صُمم الاستبيان ليغطي جميع أبعاد الدراسة، بدءًا من السياسات والاستراتيجيات المعتمدة لإدارة المخاطر السيبرانية، ومرورًا بفاعلية تنفيذ هذه الاستراتيجيات في حماية البيانات وضمان استمرارية الخدمات الرقمية، وصولًا إلى التحديات والمعوقات التي تواجه الجهات الحكومية في هذا المجال. وقد تم صياغة الأسئلة بطريقة تسمح للمتلقي

بالإجابة ضمن مقياس ليكرت الخماسي، حيث يمثل الرقم 1 أقصى درجة موافقة والرقم 5 أقصى درجة رفض، بما يسهل تحويل التقييمات إلى بيانات كمية يمكن تحليلها إحصائياً.

وقبل تطبيق الاستبيان على عينة الدراسة، تم إجراء اختبار تجريبي أولي للتأكد من وضوح الأسئلة وسهولة فهمها من قبل المستجيبين، كما تم قياس موثوقية الأداة باستخدام معامل كرونباخ ألفا لضمان اتساق الإجابات وثباتها. وبهذه الطريقة، توفر الأداة قاعدة بيانات متكاملة يمكن تحليلها باستخدام الأساليب الإحصائية الوصفية والاستدلالية، بما يعزز دقة النتائج ويسهم في اختبار الفرضيات العلمية المرتبطة بالبحث.

يمثل الاستبيان الكمي أداة محورية في هذه الدراسة، إذ لا يقتصر دوره على جمع البيانات فحسب، بل يربط بين النظرية والممارسة من خلال قياس فاعلية الاستراتيجيات المعتمدة، وتحليل أثرها على حماية المعلومات واستدامة الخدمات الرقمية في الجهات الحكومية، بما يدعم تقديم توصيات عملية قابلة للتطبيق على الواقع المحلي في المملكة العربية السعودية.

حدود الدراسة

- الحدود البشرية

تركز هذه الدراسة على المسؤولين التنفيذيين والإداريين والفنيين المكلفين بإدارة الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية، باعتبارهم الأطراف الأكثر معرفة باستراتيجيات إدارة المخاطر السيبرانية وفعاليتها. وتشمل هذه الفئة المديرين التنفيذيين، مدراء أقسام الأمن السيبراني، والمختصين الفنيين، حيث يمتلكون الخبرة العملية والمعرفة الكافية بتطبيق السياسات والإجراءات الأمنية الرقمية. وقد تم اختيار هذه الفئة لأنها قادرة على تقديم بيانات دقيقة وموثوقة حول الاستراتيجيات المعتمدة، مدى فاعليتها، التحديات التي تواجهها، والأثر العملي لهذه الاستراتيجيات على حماية البيانات واستمرارية الخدمات الرقمية.

- الحدود الزمانية

تقتصر الدراسة على الفترة الحالية، مع التركيز على آخر ثلاث سنوات، وذلك لمواكبة التطورات الرقمية والتكنولوجية الحديثة التي شهدتها الجهات الحكومية السعودية، خاصة في سياق برامج التحول الرقمي ورؤية المملكة 2030. ويأتي

تحديد هذه الفترة الزمنية لضمان أن تكون البيانات حديثة وذات صلة بالواقع الرقمي الحالي، كما يعكس تقييم الفاعلية مدى جاهزية الجهات الحكومية لمواجهة التهديدات السيبرانية الحديثة، ويتيح تحليل أثر الاستراتيجيات المطبقة ضمن بيئة رقمية متطورة ومتغيرة باستمرار.

- الحدود المكانية

تتركز الدراسة على الجهات الحكومية داخل المملكة العربية السعودية التي تعتمد على أنظمة وخدمات رقمية في تقديم خدماتها للمواطنين والمستفيدين. ويشمل ذلك مجموعة من الوزارات والهيئات الحكومية والمدن الكبرى، مثل الرياض، جدة، والدمام، بهدف تمثيل التنوع في العمليات والخدمات الرقمية عبر مختلف مناطق المملكة. وقد تم تحديد هذا النطاق المكاني لضمان أن تعكس نتائج الدراسة الواقع العملي للجهات الحكومية السعودية، مع مراعاة الخصائص التنظيمية والتقنية المحلية التي تؤثر في فاعلية تطبيق استراتيجيات إدارة المخاطر السيبرانية.

- Abn_hammad, M. Z. (2025). The Evolution of E-Government in Saudi Arabia: A Comprehensive Review of Digital Transformation Strategies, Institutional Readiness, and Citizen-Centric Service Delivery in The Vision 2030 Era. Retrieved from https://www.researchgate.net/publication/394916653_The_Evolution_of_E-Government_in_Saudi_Arabia_A_Comprehensive_Review_of_Digital_Transformation_Strategies_Institutional_Readiness_and_Citizen-Centric_Service_Delivery_in_The_Vision_2030_Era
- Alhakami, W. (2024). Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach. Retrieved from <https://www.sciencedirect.com/org/science/article/pii/S1546221824002443>
- Al-Hawamleh, A. M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. Retrieved from <https://www.emerald.com/dprg/article/26/3/317/1223750/Investigating-the-multifaceted-dynamics-of>
- Alkhalifa, M. (2024). Top 5 Deadly Cybersecurity Threats to Kingdom of Saudi Arabia. Retrieved from <https://www.preprints.org/manuscript/202408.2244>
- Assiri, K. (2022). Security Challenges for Digital Transformation in Saudi Arabia. Retrieved from https://www.researchgate.net/publication/361620051_Security_Challenges_for_Digital_Transformation_in_Saudi_Arabia
- Bennouk, K. (2024). A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. Retrieved from <https://www.mdpi.com/2624-800X/4/4/40>
- Haque, G. M. (2025). Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review. Retrieved from https://www.researchgate.net/publication/394549149_Cybersecurity_Risk_Management_in_the_Age_of_Digital_Transformation_A_Systematic_Literature_Review
- Hossain, S. T. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2664328624000792>

- Jalali, p. S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0963868717304353>
- Johri, A. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Retrieved from <https://www.semanticscholar.org/paper/Exploring-Customer-Awareness-towards-Their-Cyber-in-Johri-Kumar/261f1fe97abc642125f30d50105c3ec8d7a22e1c>
- Knowles, M. (2026). Cybersecurity Risk Management: Frameworks, Best Practices and Audit Readiness. Retrieved from <https://hyperproof.io/resource/cybersecurity-risk-management-process/>
- Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. Retrieved from <https://www.mdpi.com/2227-9091/11/6/101>
- Nygard, K. E. (2021). Dimensions of Cybersecurity Risk Management. Retrieved from https://www.researchgate.net/publication/352435513_Dimensions_of_Cybersecurity_Risk_Management
- Radebe, M. J. (2024). Public Sector Communication in the Digital Age. Retrieved from https://www.researchgate.net/publication/384950467_Public_Sector_Communication_in_the_Digital_Age
- Saeed, S. (2025). Digital Transformation in Governmental Public Service Provision and Usable Security Perception in Saudi Arabia. Retrieved from <https://www.mdpi.com/2078-2489/16/3/247>
- Slapničar, S. (2025). Cyber risk management: an illusion of a risk-based approach. Retrieved from <https://link.springer.com/article/10.1007/s00187-025-00401-z>

Midocean University

College of Management

Master's Program in Risk Management

**The Effectiveness of Cybersecurity Risk Management Strategies in Saudi Arabian
Government Entities in Light of Digital Transformation**

Prepared by the student/

University ID/

Supervisor/

Year

2026