

عنوان مشروع التخرج/ إطار تحسين إدارة مشاريع الأمن السيبراني

إعداد الطالب/ نواف عدنان الجهني

إشراف/ د. الفیصل عبد الحمید

العام الدراسي:

2026

الشكر والتقدير:

أتقدم بخالص الشكر والعرفان لكل من ساهم في إنجاز هذا المشروع، وفي مقدمتهم أعضاء هيئة التدريس في كلية إدارة الأعمال بجامعة ميدأوشن على دعمهم العلمي والإرشادي المستمر، كما أتوجه بجزيل الشكر لمشرف المشروع

د. الفیصل عبد الحمید على توجيهاته القيّمة وملاحظاته البناءة التي كان لها الأثر الكبير في تطوير هذا العمل. ولا يفوتني أن أعرب عن تقديري لجميع الزملاء والخبراء الذين شاركوا بأرائهم وملاحظاتهم أثناء إعداد هذا البحث.

وأخص بالشكر أسرتي الكريمة على دعمهم وتشجيعهم المتواصل الذي كان حافزاً لي في إتمام هذا المشروع أسأل الله أن يجعل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به كل من يهتم بتطوير حوكمة مشاريع الأمن السيبراني.

فهرس المحتويات:

Contents

4.....	الفصل الأول مقدمة البحث العلمي
5.....	المقدمة:
6.....	مشكلة الدراسة:
7.....	أهمية الدراسة:
8.....	أهداف الدراسة:
9.....	تساؤلات الدراسة:
10.....	فروض الدراسة:
11.....	النظرية العلمية المتبعة لإعداد البحث:
12.....	الفصل الثاني الدراسات السابقة
13.....	الدراسات السابقة:
14.....	التحليل المقارن والنقدي:
15.....	الإطار النظري:
16.....	الفصل الثالث منهجية الدراسة
17.....	المنهجية وطرق البحث:
19.....	الفصل الرابع النتائج والتوصيات
20.....	تحليل البيانات:
21.....	النتائج:
23.....	التوصيات:
24.....	خاتمة الدراسة:
25.....	المراجع:
25.....	المراجع المحلية:
25.....	المراجع الأجنبية:
26.....	الاستبانة:
30.....	الفصل الخامس الاطار التحسيني المقترح
31.....	الإطار التحسيني المقترح:
33.....	خامسًا: الشكل التوضيحي للإطار:
35.....	الملخص Abstract

الفصل الأول

مقدمة البحث العلمي

المقدمة:

يشهد العالم في الوقت الراهن تطورًا متسارعًا في مجالات التقنية والتحول الرقمي، مما أدى إلى بروز الأمن السيبراني كأحد أهم ركائز حماية البيانات واستدامة الأعمال في القطاعين العام والخاص. وقد أصبحت التهديدات والهجمات الإلكترونية تمثل خطرًا استراتيجيًا يهدد البنية التحتية الرقمية للمؤسسات، الأمر الذي دفع الدول، ومن ضمنها المملكة العربية السعودية، إلى تبني سياسات وطنية شاملة للأمن السيبراني تضمن استمرارية الأعمال وحماية الأصول المعلوماتية. وفي هذا السياق، تبنت المملكة العديد من المبادرات الوطنية الهادفة إلى تعزيز قدرات المؤسسات في مواجهة التحديات السيبرانية، من أبرزها تأسيس الهيئة الوطنية للأمن السيبراني (NCA) وإصدار الأطر التنظيمية والسياسات الموحدة لحوكمة الأمن السيبراني في القطاعات الحكومية والخاصة. ومع ذلك، لا تزال العديد من مؤسسات القطاع الخاص تواجه صعوبات في حوكمة إدارة مشاريع الأمن السيبراني، خصوصًا في الجوانب المتعلقة بتحديد الأدوار والمسؤوليات، وإدارة المخاطر، وضمان فعالية التنفيذ واستدامته. وتبرز أهمية الحوكمة في مشاريع الأمن السيبراني في كونها تمثل الإطار الذي ينظم العلاقة بين الجهات التنفيذية والإشرافية، ويحدد خطوط المساءلة والمراقبة، ويضمن تحقيق التوازن بين الأهداف التقنية والاستراتيجية للمؤسسة. فضعف الحوكمة يؤدي غالبًا إلى تعثر المشاريع، وتجاوز التكاليف، وتأخر الجداول الزمنية، وضعف جودة المخرجات التقنية. وتستند هذه الدراسة إلى مجموعة من الوثائق والمصادر المحلية والدولية، مثل: الاستراتيجية الوطنية للأمن السيبراني للهيئة الوطنية للأمن السيبراني (2022)، وإطار حوكمة المشاريع من معهد إدارة المشاريع (PMI, 2020)، ومبادئ OECD (2021) للحوكمة الرقمية والشفافية في إدارة المشاريع. ويُتوقع أن يساهم توظيف هذه الأطر في دعم التحليل الميداني وتعزيز موثوقية النتائج المقترحة.

مشكلة الدراسة:

وفي ظل التوسع الكبير في استخدام التقنيات الرقمية والاعتماد المتزايد على الأنظمة المعلوماتية في مختلف القطاعات، أصبحت مشاريع الأمن السيبراني من المشاريع الحيوية التي تعتمد عليها المؤسسات لضمان حماية بياناتها وأنظمتها الرقمية. ويستلزم نجاح هذه المشاريع وجود إدارة فعالة تعتمد على ممارسات حوكمة واضحة تضمن تنظيم عمليات التخطيط والتنفيذ والمتابعة، إضافة إلى تحديد المسؤوليات بين الجهات المعنية داخل المؤسسة. كما تسهم الحوكمة الفعالة في تعزيز القدرة على اتخاذ القرارات المناسبة في الوقت المناسب، وتوفير بيئة تنظيمية تساعد على تحقيق التكامل بين الجوانب التقنية والإدارية في إدارة المشاريع السيبرانية.

كما أن تطبيق مبادئ الحوكمة في إدارة مشاريع الأمن السيبراني يساهم في تحسين مستوى الشفافية والمساءلة داخل المؤسسات، ويعزز من قدرتها على متابعة أداء المشاريع وتقييم نتائجها بشكل دوري. ويساعد ذلك في الكشف المبكر عن المشكلات التي قد تواجه تنفيذ المشاريع، والعمل على معالجتها قبل أن تتسبب في تعثر المشروع أو انخفاض جودة مخرجاته. إضافة إلى ذلك، فإن وجود نظام حوكمة واضح يساهم في تعزيز الثقة بين الإدارة العليا والفرق التنفيذية، ويضمن الاستخدام الأمثل للموارد البشرية والتقنية المخصصة للمشاريع.

ومن ناحية أخرى، فإن غياب إطار حوكمة متكامل قد يؤدي إلى ضعف التنسيق بين الإدارات المختلفة داخل المؤسسة، الأمر الذي ينعكس سلباً على كفاءة تنفيذ مشاريع الأمن السيبراني. كما قد يؤدي ذلك إلى عدم وضوح الأولويات الاستراتيجية للمشاريع أو ضعف آليات المتابعة والتقييم، مما يحد من قدرة المؤسسات على تحقيق الاستفادة الكاملة من هذه المشاريع. ولذلك تبرز أهمية دراسة واقع حوكمة إدارة مشاريع الأمن السيبراني في المؤسسات وتحليل العوامل التي تؤثر في كفاءة تطبيقها، بهدف الوصول إلى مقترحات عملية يمكن أن تساهم في تطوير ممارسات الحوكمة وتحسين مستوى إدارة المشاريع السيبرانية.

السؤال الرئيس للدراسة:

ما فرص تحسين حوكمة إدارة مشاريع الأمن السيبراني في المؤسسات بما يضمن رفع كفاءة وفعالية تنفيذ مبادرات الأمن السيبراني وتحقيق استدامتها؟

أهمية الدراسة:

تكتسب هذه الدراسة أهميتها من تزايد الاعتماد على التقنيات الرقمية والأنظمة المعلوماتية في مختلف القطاعات، الأمر الذي جعل الأمن السيبراني عنصراً أساسياً في حماية البيانات والبنية التحتية الرقمية للمؤسسات. ومع التطور المتسارع في مجال التحول الرقمي، أصبحت المؤسسات تعتمد بشكل كبير على الأنظمة التقنية لإدارة عملياتها وتقديم خدماتها، مما يزيد من أهمية وجود ممارسات فعالة لإدارة مشاريع الأمن السيبراني وضمان تنفيذها وفق أسس تنظيمية واضحة. ومن هنا تبرز أهمية حوكمة إدارة المشاريع السيبرانية بوصفها إطاراً تنظيمياً يساهم في تعزيز كفاءة التخطيط والتنفيذ والمتابعة، ويضمن تحقيق الأهداف الاستراتيجية للمؤسسات.

كما تنبع أهمية هذه الدراسة من الحاجة المتزايدة إلى تطوير ممارسات الحوكمة في إدارة مشاريع الأمن السيبراني داخل مؤسسات القطاع الخاص في المملكة العربية السعودية، خصوصاً في ظل التوسع الكبير في تبني التقنيات الرقمية والخدمات الإلكترونية. فوجود إطار حوكمة واضح يساعد المؤسسات على تنظيم عمليات اتخاذ القرار وتحديد المسؤوليات بين الإدارات المختلفة، إضافة إلى تعزيز مستوى الشفافية والمساءلة في إدارة المشاريع التقنية. كما يساهم ذلك في تحسين مستوى التنسيق بين الفرق الفنية والإدارية المشاركة في تنفيذ المشاريع، الأمر الذي يؤدي إلى رفع كفاءة الأداء وتقليل المخاطر المرتبطة بالمشاريع السيبرانية. وتبرز أهمية هذه الدراسة أيضاً في كونها تساهم في إثراء الأدبيات العلمية المتعلقة بحوكمة إدارة المشاريع في مجال الأمن السيبراني، وهو مجال لا يزال بحاجة إلى المزيد من الدراسات التطبيقية التي تركز على واقع المؤسسات في المملكة العربية السعودية. كما أن هذه الدراسة تسعى إلى تقديم تحليل علمي لواقع الممارسات التنظيمية المرتبطة بإدارة مشاريع الأمن السيبراني، الأمر الذي يمكن أن يساهم في توفير فهم أعمق للعوامل التي تؤثر في نجاح هذه المشاريع أو تعثرها.

ومن الناحية التطبيقية، يمكن أن تساعد نتائج هذه الدراسة المؤسسات في تطوير ممارسات أكثر فاعلية لحوكمة إدارة مشاريع الأمن السيبراني، من خلال تحديد أبرز التحديات التنظيمية والإدارية التي قد تواجه تنفيذ هذه المشاريع. كما يمكن أن تساهم التوصيات المقترحة في تحسين آليات التخطيط والمتابعة والتقييم داخل المؤسسات، وتعزيز قدرتها على إدارة المخاطر السيبرانية بشكل أكثر كفاءة. إضافة إلى ذلك، فإن تطبيق ممارسات الحوكمة الفعالة يساهم في تحسين جودة مخرجات المشاريع التقنية ويعزز من استدامة المبادرات السيبرانية على المدى الطويل.

كما تتجلى أهمية هذه الدراسة في دعم الجهود الوطنية الرامية إلى تعزيز الأمن السيبراني في المملكة العربية السعودية، بما يتوافق مع التوجهات الاستراتيجية للتحول الرقمي ورؤية المملكة 2030. فتعزيز ممارسات الحوكمة في إدارة مشاريع الأمن السيبراني يساهم في رفع مستوى جاهزية المؤسسات لمواجهة التهديدات السيبرانية المتزايدة، ويعزز قدرتها على حماية أصولها الرقمية وضمان استمرارية أعمالها في بيئة رقمية متغيرة. ولذلك فإن هذه الدراسة تسعى إلى تقديم إطار معرّي وتطبيقي يمكن أن يدعم المؤسسات في تطوير أنظمة حوكمة فعالة لإدارة مشاريع الأمن السيبراني وتحقيق أعلى مستويات الكفاءة والاستدامة في تنفيذ هذه المشاريع.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل واقع تطبيق ممارسات حوكمة إدارة مشاريع الأمن السيبراني في مؤسسات القطاع الخاص في المملكة العربية السعودية، وذلك من خلال دراسة طبيعة الأطر التنظيمية والإدارية التي تحكم تنفيذ هذه المشاريع، ومدى توافقها مع المعايير والممارسات الدولية في مجال الحوكمة وإدارة المشاريع التقنية. كما تسعى الدراسة إلى فهم كيفية تأثير مستوى نضج الحوكمة المؤسسية على كفاءة تنفيذ مشاريع الأمن السيبراني وقدرتها على تحقيق الأهداف الاستراتيجية للمؤسسات.

كما تهدف الدراسة إلى التعرف على مستوى الوعي المؤسسي بأهمية حوكمة مشاريع الأمن السيبراني، ومدى تطبيق السياسات والإجراءات التنظيمية التي تضمن وضوح الأدوار والمسؤوليات بين الفرق الفنية والإدارية المشاركة في تنفيذ المشاريع. وتولي الدراسة اهتمامًا خاصًا بتحليل آليات المتابعة والتقييم المستخدمة داخل المؤسسات، ومدى فاعليتها في ضمان تحقيق الأهداف المخطط لها وتقليل المخاطر المرتبطة بالمشاريع السيبرانية.

ومن الأهداف الرئيسة للدراسة أيضًا تحديد أبرز التحديات التنظيمية والإدارية التي تواجه المؤسسات أثناء تنفيذ مشاريع الأمن السيبراني، مثل ضعف التنسيق بين الإدارات المختلفة، أو نقص الكفاءات المتخصصة، أو غياب الأطر المؤسسية الواضحة لإدارة المخاطر. ويساعد تحليل هذه التحديات في تقديم فهم أعمق للعوامل التي قد تؤثر في نجاح أو تعثر المشاريع السيبرانية داخل المؤسسات.

كما تسعى الدراسة إلى مقارنة الممارسات المتبعة في المؤسسات المحلية مع الأطر والمعايير الدولية المعتمدة في مجال حوكمة المشاريع وإدارة الأمن السيبراني، مثل الأطر التي يقدمها معهد إدارة المشاريع وإطار COBIT لإدارة تقنية المعلومات، وذلك بهدف تحديد الفجوات التنظيمية وفرص التحسين الممكنة التي يمكن أن تسهم في رفع مستوى كفاءة إدارة المشاريع السيبرانية.

وفي ضوء ما سبق يمكن تحديد أهداف الدراسة في النقاط الآتية:

- 1- تحليل واقع تطبيق ممارسات حوكمة إدارة المشاريع في مجال الأمن السيبراني في مؤسسات القطاع الخاص السعودي.
- 2- تحديد أبرز التحديات التنظيمية والإدارية التي تؤثر في فعالية حوكمة مشاريع الأمن السيبراني.
- 3- دراسة العلاقة بين مستوى نضج ممارسات الحوكمة ومستوى نجاح مشاريع الأمن السيبراني.
- 4- مقارنة الممارسات المحلية بالمعايير الدولية في حوكمة المشاريع والأمن السيبراني.
- 5- اقتراح إطار تطبيقي لتحسين فعالية واستدامة حوكمة إدارة مشاريع الأمن السيبراني في المؤسسات.

تساؤلات الدراسة:

في ضوء مشكلة الدراسة وأهدافها، تسعى هذه الدراسة إلى الإجابة عن مجموعة من التساؤلات التي تهدف إلى فهم واقع تطبيق ممارسات حوكمة إدارة مشاريع الأمن السيبراني في مؤسسات القطاع الخاص في المملكة العربية السعودية. كما تهدف هذه التساؤلات إلى تحليل طبيعة الأطر التنظيمية والإدارية التي تنظم تنفيذ هذه المشاريع، ومدى قدرتها على تعزيز كفاءة إدارة المشاريع السيبرانية وتحقيق الأهداف الاستراتيجية للمؤسسات.

وتأتي أهمية هذه التساؤلات في كونها تساهم في استكشاف مستوى تطبيق مبادئ الحوكمة المؤسسية في إدارة مشاريع الأمن السيبراني، إضافة إلى تحديد أبرز التحديات التنظيمية والإدارية التي قد تواجه المؤسسات أثناء تنفيذ هذه المشاريع. كما تساعد هذه التساؤلات في فهم العلاقة بين مستوى نضج الحوكمة داخل المؤسسات ومستوى نجاح مشاريع الأمن السيبراني، ومدى توافق الممارسات المحلية مع المعايير والأطر الدولية المعتمدة في مجال حوكمة المشاريع وإدارة الأمن السيبراني.

كما تسعى الدراسة من خلال هذه التساؤلات إلى توفير فهم أعمق للبيئة التنظيمية التي تعمل ضمنها مشاريع الأمن السيبراني في المؤسسات، وتحليل مدى تكامل الجوانب الإدارية والتقنية في إدارة هذه المشاريع. ويساهم ذلك في تحديد الممارسات الفعالة التي يمكن أن تعزز كفاءة إدارة المشاريع السيبرانية، إضافة إلى الكشف عن أوجه القصور أو التحديات التي قد تحد من تحقيق النتائج المرجوة من هذه المشاريع.

كذلك تهدف هذه التساؤلات إلى استكشاف الدور الذي يمكن أن تلعبه الحوكمة المؤسسية في دعم عملية اتخاذ القرار داخل المؤسسات، وتعزيز مستوى التنسيق بين الإدارات المختلفة المشاركة في تنفيذ مشاريع الأمن السيبراني. ويساعد ذلك في فهم كيفية تطوير ممارسات تنظيمية أكثر كفاءة تساهم في تقليل المخاطر المرتبطة بالمشاريع التقنية وتحسين مستوى الأداء المؤسسي. وانطلاقاً من ذلك، تسعى الدراسة للإجابة عن التساؤلات الآتية:

- 1- ما واقع تطبيق ممارسات حوكمة إدارة مشاريع الأمن السيبراني في مؤسسات القطاع الخاص في المملكة العربية السعودية؟
- 2- ما أبرز التحديات التنظيمية والإدارية التي تؤثر في فعالية حوكمة مشاريع الأمن السيبراني أثناء مراحل تنفيذ المشاريع؟
- 3- ما مدى العلاقة بين مستوى نضج ممارسات الحوكمة ومستوى نجاح مشاريع الأمن السيبراني داخل المؤسسات؟
- 4- ما الفجوات بين الممارسات المتبعة في المؤسسات المحلية والمعايير الدولية في مجال حوكمة إدارة المشاريع والأمن السيبراني؟
- 5- ما الآليات أو الأطر التنظيمية التي يمكن أن تساهم في تحسين فعالية واستدامة حوكمة إدارة مشاريع الأمن السيبراني في مؤسسات القطاع الخاص؟

فروض الدراسة:

استنادًا إلى مشكلة الدراسة وتساؤلاتها، تسعى هذه الدراسة إلى اختبار مجموعة من الفروض التي تهدف إلى تحليل العلاقة بين مستوى تطبيق ممارسات الحوكمة ونجاح مشاريع الأمن السيبراني في مؤسسات القطاع الخاص. وتستند هذه الفروض إلى الأدبيات العلمية في مجال حوكمة المشاريع وإدارة الأمن السيبراني، والتي تشير إلى أن وجود أطر تنظيمية واضحة وآليات متابعة فعالة يساهم في تعزيز كفاءة تنفيذ المشاريع وتقليل المخاطر المرتبطة بها. كما تؤكد العديد من الدراسات أن الحوكمة المؤسسية تمثل عنصرًا أساسيًا في نجاح المشاريع التقنية، نظرًا لدورها في تنظيم عمليات اتخاذ القرار وتحديد المسؤوليات وتعزيز مستوى المساءلة والشفافية داخل المؤسسات.

كما تفترض الدراسة أن مستوى نضج الحوكمة المؤسسية داخل المؤسسات قد يكون له دور مهم في تحسين أداء مشاريع الأمن السيبراني، من خلال تنظيم عمليات التخطيط والتنفيذ والمتابعة، إضافة إلى تعزيز التنسيق بين الإدارات المختلفة المشاركة في تنفيذ المشاريع. ويساهم تطبيق ممارسات الحوكمة الفعالة في تحسين إدارة الموارد المتاحة وتقليل احتمالية تعثر المشاريع أو تجاوز الميزانيات المخصصة لها. كما أن وجود سياسات واضحة لإدارة المخاطر والمتابعة الدورية يساهم في تعزيز قدرة المؤسسات على التعامل مع التهديدات السيبرانية والتحديات التقنية التي قد تواجه تنفيذ المشاريع.

وتفترض الدراسة أيضًا أن المؤسسات التي تعتمد أطرًا تنظيمية واضحة لحوكمة المشاريع تكون أكثر قدرة على تحقيق التكامل بين الأهداف التقنية والاستراتيجية للمؤسسة، مما يساعد في تحسين جودة مخرجات المشاريع وتعزيز استدامتها على المدى الطويل. كما أن تبني المعايير الدولية في مجال إدارة المشاريع والأمن السيبراني قد يساهم في تطوير الممارسات التنظيمية داخل المؤسسات ورفع مستوى كفاءة إدارة المشاريع السيبرانية.

وفي ضوء ما سبق، تعتمد الدراسة على اختبار الفروض الآتية:

- 1- توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق ممارسات حوكمة إدارة المشاريع ومستوى نجاح مشاريع الأمن السيبراني في مؤسسات القطاع الخاص.
- 2- يؤثر وضوح الأدوار والمسؤوليات التنظيمية بين الفرق الفنية والإدارية تأثيرًا إيجابيًا في فعالية تنفيذ مشاريع الأمن السيبراني.
- 3- يساهم تطبيق آليات المتابعة والتقييم الدورية في تعزيز كفاءة إدارة مشاريع الأمن السيبراني وتقليل احتمالية تعثرها.
- 4- توجد فروق ذات دلالة إحصائية في مستوى تطبيق حوكمة مشاريع الأمن السيبراني تعزى إلى حجم المؤسسة أو مستوى نضجها الرقمي.
- 5- يساهم تبني المعايير والأطر الدولية لحوكمة المشاريع وإدارة الأمن السيبراني في تحسين جودة تنفيذ المشاريع ورفع مستوى استدامتها داخل المؤسسات.

النظرية العلمية المتبعة لإعداد البحث:

تستند هذه الدراسة إلى عدد من النظريات العلمية التي تشكل الإطار المفاهيمي الذي يوجه البحث ويحدد العلاقة بين متغيراته الأساسية.

أولاً: **نظرية الحوكمة المؤسسية (Corporate Governance Theory)** ، التي تؤكد أهمية وجود أنظمة واضحة للمساءلة والشفافية وتحديد الأدوار والمسؤوليات بين الإدارات، وهو ما يمثل جوهر مفهوم حوكمة مشاريع الأمن السيبراني.

ثانياً: **نظرية إدارة المشاريع (Project Management Theory)** ، التي تُعنى بالتخطيط والتنظيم والتنفيذ والمتابعة لتحقيق أهداف المشروع ضمن نطاقه الزمني والمالي، مما يجعلها الأساس العلمي لتحليل كفاءة تنفيذ المشاريع في هذه الدراسة.

ثالثاً: **نظرية النضج المؤسسي (Organizational Maturity Theory)** ، التي تفترض أن المؤسسات ذات النضج العالي في تطبيق سياسات الحوكمة والإدارة تحقق مستويات أعلى من النجاح والاستدامة في مشاريعها، خاصة في بيئات معقدة كبيئة الأمن السيبراني.

وبناءً على هذه النظريات الثلاث، تم بناء الإطار النظري للدراسة وتحليل العلاقة بين مستوى نضج الحوكمة وفعالية تنفيذ مشاريع الأمن السيبراني في المؤسسات.

الفصل الثاني
الدراسات السابقة

الدراسات السابقة:

ثانيًا: الدراسات المحلية:

- القرني (2024)
أظهرت وجود فجوة بين تبني الأطر التنظيمية والتطبيق الفعلي داخل المشاريع.
- الشهري (2023)
أكد وجود علاقة إيجابية بين نضج الحوكمة وتحسن مؤشرات الأداء.
- الجهني (2022)
أوضح ضعف الهياكل التنظيمية في المنشآت الصغيرة والمتوسطة.
- العتيبي (2023)
أشار إلى أن التحول الرقمي السريع يتطلب تعزيز أطر الحوكمة.
- السلمي (2024)
أكد تفاوت مستويات الالتزام بضوابط NCA بين المؤسسات.

ثانيًا: الدراسات الأجنبية:

- PMI (2020)
أثبت أن ضعف الحوكمة يزيد من تعثر مشاريع الأمن السيبراني.
- OECD (2021)
ركزت على مبادئ الحوكمة الرقمية والشفافية.
- Smith & Clarke (2023)
وجدت علاقة قوية بين نضج الحوكمة ونجاح المشاريع في أوروبا.
- ISACA (2022)
أكدت أهمية إطار COBIT في تعزيز المساءلة وتقليل المخاطر.
- World Economic Forum (2023)
أشار إلى أن غياب الحوكمة المؤسسية من أبرز أسباب فشل المبادرات السيبرانية.
- Deloitte (2024)
أكدت أن ربط الحوكمة بالتحول الرقمي يرفع العائد الاستثماري.

التحليل المقارن والنقدي:

عند تحليل الدراسات السابقة المتعلقة بحوكمة إدارة المشاريع في مجال الأمن السيبراني، يتضح وجود اهتمام متزايد بدراسة العلاقة بين مستوى تطبيق ممارسات الحوكمة ونجاح المشاريع التقنية. فقد ركزت العديد من الدراسات الأجنبية على تطوير نماذج وأطر تنظيمية تهدف إلى تحسين كفاءة إدارة المشاريع السيبرانية وتعزيز القدرة على إدارة المخاطر المرتبطة بها. وتشير هذه الدراسات إلى أن تطبيق ممارسات الحوكمة المؤسسية يساهم في تنظيم عمليات اتخاذ القرار وتحديد المسؤوليات بين الأطراف المعنية، مما يساعد على تقليل احتمالية تعثر المشاريع وتحسين جودة مخرجاتها.

ومن خلال المقارنة بين الدراسات المحلية والدراسات الأجنبية، يتضح أن الدراسات الأجنبية غالبًا ما ركزت على استخدام النماذج المعيارية والأطر التنظيمية المعتمدة دوليًا مثل إطار COBIT وإطار إدارة المشاريع الصادر عن معهد إدارة المشاريع (PMI). وقد تناولت هذه الدراسات العلاقة بين نضج الحوكمة المؤسسية ومستوى نجاح المشاريع التقنية، وأظهرت نتائجها أن المؤسسات التي تعتمد أطر حوكمة واضحة تكون أكثر قدرة على إدارة المخاطر التقنية وتحقيق أهداف المشاريع بكفاءة أعلى.

أما الدراسات المحلية، فقد ركزت بشكل أكبر على تحليل واقع تطبيق ممارسات الحوكمة في المؤسسات، مع التركيز على التحديات التنظيمية والإدارية التي قد تواجه تطبيق هذه الممارسات في البيئة المحلية. وقد أشارت بعض الدراسات إلى وجود فجوة بين تبني السياسات التنظيمية المتعلقة بحوكمة الأمن السيبراني وبين التطبيق الفعلي لهذه السياسات داخل المؤسسات، الأمر الذي قد يؤثر في كفاءة تنفيذ المشاريع السيبرانية ويحد من قدرتها على تحقيق النتائج المرجوة.

كما تظهر المقارنة بين هذه الدراسات أن معظمها تناول موضوع الحوكمة ضمن إطار عام لإدارة تقنية المعلومات، دون التركيز بشكل مباشر على حوكمة إدارة مشاريع الأمن السيبراني تحديدًا، خاصة في مؤسسات القطاع الخاص في المملكة العربية السعودية. ويشير ذلك إلى وجود فجوة بحثية تتعلق بدراسة العلاقة بين ممارسات الحوكمة المؤسسية وإدارة مشاريع الأمن السيبراني في السياق المحلي، وهو ما تسعى هذه الدراسة إلى معالجته من خلال تحليل واقع هذه الممارسات وتحديد أبرز التحديات التي قد تواجه المؤسسات في هذا المجال.

ومن خلال هذا التحليل المقارن، يتضح أن تعزيز ممارسات حوكمة إدارة مشاريع الأمن السيبراني يتطلب تبني أطر تنظيمية واضحة تجمع بين الجوانب الإدارية والتقنية، إضافة إلى تطوير آليات فعالة للمتابعة والتقييم وإدارة المخاطر. كما أن الاستفادة من التجارب الدولية في هذا المجال يمكن أن يساهم في تطوير الممارسات التنظيمية داخل المؤسسات المحلية، وتحسين مستوى كفاءة إدارة المشاريع السيبرانية بما يتوافق مع أفضل الممارسات العالمية.

الإطار النظري:

تُعد حوكمة المشاريع من المفاهيم الإدارية الحديثة التي برزت نتيجة الحاجة إلى تنظيم العلاقة بين مختلف المستويات الإدارية داخل المؤسسة، بما يضمن تحقيق الأهداف بكفاءة وشفافية. ولا تقتصر الحوكمة على وضع السياسات والإجراءات، بل تمتد لتشمل بناء منظومة متكاملة من الضوابط التي تحدد الأدوار والمسؤوليات، وتدعم اتخاذ القرار، وتُفَعِّل آليات الرقابة والمتابعة المستمرة. وفي سياق إدارة المشاريع، تكتسب الحوكمة أهمية مضاعفة، كونها تمثل الإطار الذي يوجه تنفيذ المشروع ويضمن توافقه مع الاستراتيجية العامة للمؤسسة.

وفي مجال الأمن السيبراني، تصبح حوكمة المشاريع أكثر تعقيداً نظراً لطبيعة المخاطر المرتبطة بالبيئة الرقمية، والتي تتسم بالتغير المستمر والتطور السريع. فمشاريع الأمن السيبراني لا تتعامل فقط مع متطلبات تقنية، بل ترتبط أيضاً بأبعاد تنظيمية وتشريعية وإدارية، مما يستدعي وجود إطار حوكمة واضح يضمن التكامل بين هذه الجوانب. وتشمل إدارة مشاريع الأمن السيبراني مجموعة من العمليات المترابطة التي تبدأ بتحديد الأهداف ونطاق المشروع، مروراً بتخطيط الموارد وتوزيع الأدوار، وانتهاءً بعمليات التنفيذ والمتابعة والتقييم، مع ضرورة الاستجابة المستمرة للمخاطر والتهديدات المحتملة.

كما يُعد الأمن السيبراني عنصراً أساسياً في استدامة الأعمال، حيث يساهم في حماية الأصول المعلوماتية وضمان استمرارية العمليات التشغيلية. إلا أن فعالية هذه الحماية لا تعتمد فقط على الحلول التقنية، بل تتطلب وجود بيئة تنظيمية داعمة تقوم على مبادئ الحوكمة الرشيدة. فغياب التنسيق بين الإدارات، أو ضعف وضوح السياسات، قد يؤدي إلى وجود فجوات أمنية رغم توفر التقنيات المتقدمة، وهو ما يؤكد على أهمية التكامل بين الحوكمة والأمن السيبراني.

وتبرز العلاقة بين حوكمة المشاريع وإدارة مشاريع الأمن السيبراني من خلال التأثير المباشر لمستوى نضج الحوكمة على نتائج المشاريع. إذ إن المؤسسات التي تبني ممارسات حوكمة واضحة، مثل تحديد مؤشرات الأداء، وتفعيل آليات المساءلة، وتطبيق منهجيات إدارة المخاطر، تكون أكثر قدرة على تنفيذ مشاريعها بكفاءة وتحقيق أهدافها ضمن الإطار الزمني والمالي المحدد. في المقابل، يؤدي ضعف الحوكمة إلى ظهور عدد من التحديات، مثل تضارب الصلاحيات، وضعف التنسيق بين الفرق، وتأخر اتخاذ القرارات، مما ينعكس سلباً على جودة التنفيذ واستدامة المشروع.

ومن منظور تكاملي، يمكن النظر إلى حوكمة مشاريع الأمن السيبراني على أنها حلقة وصل بين التوجهات الاستراتيجية للمؤسسة والمتطلبات التشغيلية للمشاريع. فهي تساهم في ترجمة الأهداف الاستراتيجية إلى خطط تنفيذية قابلة للتطبيق، مع ضمان الالتزام بالضوابط والمعايير المعتمدة. كما تساعد في تحقيق التوازن بين متطلبات الحماية الأمنية واعتبارات الكفاءة التشغيلية، وهو ما يمثل تحدياً رئيسياً في بيئات العمل الحديثة.

وعليه، فإن تعزيز ممارسات الحوكمة في إدارة مشاريع الأمن السيبراني يُعد عاملاً حاسماً في تحسين جودة التنفيذ وتقليل المخاطر، كما يساهم في بناء بيئة تنظيمية قائمة على الوضوح والانضباط المؤسسي. ويؤكد ذلك أهمية تبني نماذج حوكمة ناضجة تستند إلى أفضل الممارسات والمعايير الدولية، بما يدعم قدرة المؤسسات في القطاع الخاص على مواجهة التحديات السيبرانية وتحقيق الاستدامة في ظل التحول الرقمي المتسارع.

الفصل الثالث

منهجية الدراسة

المنهجية وطرق البحث:

اعتمدت الدراسة على المنهج الوصفي التحليلي (Descriptive-Analytical Method)،
ويجمع البحث بين البيانات الكمية والنوعية (Mixed Methods) .

- البيانات الكمية: تم جمعها من الوثائق الرسمية والتقارير الصادرة عن مؤسسات القطاع الخاص.
- البيانات النوعية: تم الحصول عليها من خلال مقابلات شبه منظمة مع مديري المشاريع وخبراء الأمن السيبراني.
- تحليل الوثائق: مراجعة السياسات والإجراءات والأطر التنظيمية للأمن السيبراني (مثل إطار NCA ، ومعايير PMI و COBIT).

مجتمع البحث:

مديري المشاريع، مديري الحوكمة، مديري الجودة، وخبراء الأمن السيبراني في المؤسسات والقطاعات السعودي.
تم اختيار العينة بطريقة عمدية (Purposive Sampling) لضمان مشاركة الأفراد ذوي الخبرة في حوكمة مشاريع الأمن السيبراني.

أدوات جمع البيانات:

1. تحليل الوثائق الرسمية: لتقييم مدى الالتزام بالمعايير الوطنية والدولية.
2. المقابلات شبه المنظمة: للحصول على بيانات نوعية حول التحديات والفرص.
3. تحليل الدراسات السابقة: لتدعيم النتائج النظرية وتوضيح الفجوات البحثية.

صدق وثبات الأداة:

تم التحقق من صدق الأدوات من خلال عرضها على مجموعة من المختصين في إدارة المشاريع والأمن السيبراني،
كما تم التأكد من الثبات عبر مقارنة الإجابات وتحليل التكرار لضمان اتساق النتائج.

طرق تحليل البيانات:

- تحليل وصفي: لتحديد واقع ممارسات الحوكمة داخل المؤسسات.
- تحليل نوعي (تحليل المحتوى): لاستخلاص الأنماط المشتركة والتحديات المتكررة.
- تحليل مقارنة: لمقارنة النتائج المحلية بالمعايير الدولية.

حدود البحث:

- الموضوعية: يقتصر البحث على حوكمة إدارة مشاريع الأمن السيبراني فقط.
- المكانية: يطبق البحث على مؤسسات القطاع الخاص داخل المملكة العربية السعودية.
- الزمانية: المشاريع المنفذة خلال الفترة (2020-2025).
- البشرية: تشمل مديري المشاريع، ومديري الحوكمة والجودة، وخبراء الأمن السيبراني.

الفصل الرابع
النتائج والتوصيات

تحليل البيانات:

اعتمد تحليل البيانات في هذه الدراسة على المقابلات النوعية وتحليل الوثائق الرسمية، إضافة إلى المراجعة المقارنة مع الأطر الدولية (COBIT, PMI, OECD). وتم التركيز على أربعة محاور رئيسية:

- واقع تطبيق الحوكمة.
- التحديات التي تواجه تنفيذ المشاريع.
- العوامل المؤثرة في فعالية الحوكمة.
- مدى توافق الممارسات المحلية مع المعايير الدولية.

وفيما يتعلق بال محور الأول، أظهرت نتائج المقابلات أن مستوى تطبيق ممارسات الحوكمة في مشاريع الأمن السيبراني يتفاوت بين المؤسسات، حيث تلتزم بعض الجهات بتطبيق سياسات وإجراءات واضحة، في حين تكتفي جهات أخرى بتطبيق جزئي أو غير منهجي لمفاهيم الحوكمة. كما تبين أن وجود هياكل تنظيمية واضحة ولجان إشرافية مختصة يساهم بشكل كبير في تعزيز مستوى الالتزام وتحسين جودة تنفيذ المشاريع.

أما فيما يخص التحديات التي تواجه تنفيذ المشاريع، فقد كشفت البيانات عن مجموعة من المعوقات المتكررة، من أبرزها ضعف وضوح الأدوار والمسؤوليات بين الفرق الفنية والإدارية، وقصور آليات المتابعة والتقييم، إضافة إلى محدودية الموارد البشرية المتخصصة في مجال الأمن السيبراني. كما أشار المشاركون إلى أن سرعة التغير في التهديدات السيبرانية تمثل تحديًا إضافيًا يتطلب استجابة مرنة ومنهجية متطورة في إدارة المشاريع.

وفي المحور الثالث، المتعلق بالعوامل المؤثرة في فعالية الحوكمة، أظهرت النتائج أن مستوى دعم الإدارة العليا يُعد من أهم العوامل الحاسمة في نجاح تطبيق ممارسات الحوكمة، إلى جانب وضوح السياسات والإجراءات، وتوفير الكفاءات المؤهلة، واعتماد منهجيات واضحة لإدارة المخاطر. كما برزت أهمية ثقافة المنظمة في تعزيز الالتزام بالحوكمة، حيث تساهم بيئة العمل التي تشجع على المساءلة والانضباط في رفع كفاءة الأداء وتحقيق نتائج أفضل.

أما بالنسبة لمدى توافق الممارسات المحلية مع المعايير الدولية، فقد أظهرت المراجعة المقارنة وجود فجوة نسبية بين ما هو مطبق فعليًا في بعض المؤسسات وما تنص عليه الأطر الدولية. حيث تركز الأطر مثل COBIT و PMI على وجود نماذج واضحة للحوكمة، ومؤشرات أداء محددة، وآليات رقابة مستمرة، في حين أن التطبيق المحلي قد يفتقر في بعض الحالات إلى التكامل بين هذه العناصر. ومع ذلك، لوحظ أن هناك توجهًا متزايدًا نحو تبني هذه الأطر والاستفادة منها، خاصة في المؤسسات الكبيرة التي تسعى إلى تحقيق مستويات أعلى من النضج المؤسسي. وبشكل عام، تشير نتائج تحليل البيانات إلى أن تحسين حوكمة إدارة مشاريع الأمن السيبراني يتطلب تبني نهج متكامل يجمع بين الجوانب التنظيمية والتقنية، مع التركيز على تطوير السياسات، وتعزيز الكفاءات، وتفعيل أدوات المتابعة والتقييم. كما تؤكد النتائج أهمية مواكبة الممارسات المحلية مع المعايير الدولية، بما يساهم في تقليل الفجوات وتحقيق مستوى أعلى من الكفاءة والاستدامة في تنفيذ المشاريع.

النتائج:

نتائج محور واقع تطبيق الحوكمة:

- أظهرت النتائج أن مستوى نضج الحوكمة في مؤسسات القطاع الخاص متوسط، ويتفاوت بين المؤسسات الكبرى والمتوسطة.
- أغلب المؤسسات تمتلك سياسات مكتوبة للأمن السيبراني، ولكنها غير مفعلة بالكامل في المشاريع التشغيلية.
- يوجد ضعف في المتابعة الدورية وتقييم الأداء في مراحل تنفيذ مشاريع الأمن السيبراني.

نتائج محور التحديات:

- تداخل الأدوار والمسؤوليات بين الإدارات الفنية والإدارية أدى إلى ضعف المساءلة.
- نقص الخبرات المتخصصة في حوكمة مشاريع الأمن السيبراني، خصوصاً في المنشآت الصغيرة والمتوسطة.
- ضعف التواصل بين فرق العمل التنفيذية والقيادية مما يؤثر على جودة التنفيذ.

نتائج محور العوامل المؤثرة:

- وجود إطار حوكمة مؤسسي واضح يساهم في تحسين الأداء وتقليل المخاطر.
- المؤسسات التي تطبق المتابعة الدورية والتقارير المرحلية تحقق نتائج أفضل واستدامة أعلى للمشاريع.
- وضوح الأدوار والمسؤوليات من أهم عوامل نجاح المشاريع.

نتائج محور الممارسات والمعايير الدولية:

- المؤسسات السعودية تطبق بعض مبادئ NCA وPMI، لكنها لا تطبقها بشكل متكامل كما في COBIT أو OECD.
- الفجوات الرئيسة تظهر في آليات الرقابة، المتابعة، وإدارة المخاطر.

النتائج العامة للدراسة:

استناداً إلى التحليل، توصلت الدراسة إلى النتائج الآتية:

1. هناك علاقة إيجابية قوية بين مستوى نضج الحوكمة ونجاح مشاريع الأمن السيبراني.
2. المؤسسات التي تمتلك هياكل حوكمة واضحة تحقق استدامة أعلى وكفاءة تنفيذ أفضل.
3. ضعف وضوح الأدوار والمسؤوليات الإدارية والفنية يؤدي إلى تعثر بعض المشاريع وتأخر إنجازها.

4. وجود آلية متابعة وتقييم دوري يزيد من جودة التنفيذ ويقلل من المخاطر التشغيلية.
5. تتطلب المنشآت الصغيرة والمتوسطة دعمًا إضافيًا في بناء هياكل حوكمة متخصصة.
6. ربط الحوكمة بالتحول الرقمي يحقق تكاملًا استراتيجيًا يعزز من كفاءة المؤسسات واستعدادها الأمني.
7. الحاجة إلى إطار وطني موحد لتطبيق حوكمة مشاريع الأمن السيبراني في القطاع الخاص السعودي.

التوصيات:

انطلاقاً من النتائج السابقة، توصي الدراسة بما يلي:

أولاً: التوصيات الاستراتيجية:

- تطوير إطار وطني موحد لحوكمة مشاريع الأمن السيبراني في القطاع الخاص السعودي، يستند إلى معايير NCA و COBIT و PMI.
- تعزيز التكامل بين أهداف الأمن السيبراني وأهداف الحوكمة المؤسسية بما يتماشى مع رؤية المملكة 2030.

ثانياً: التوصيات الإدارية والتنظيمية:

- توضيح الأدوار والمسؤوليات بين الإدارات التنفيذية والإشرافية لضمان كفاءة التنفيذ والمساءلة.
- إنشاء لجان دائمة لحوكمة المشاريع تتولى المتابعة والتقييم المستمر لمراحل التنفيذ.
- اعتماد تقارير دورية تقيس أداء مشاريع الأمن السيبراني وجودة التنفيذ في كل مرحلة.

ثالثاً: التوصيات الفنية والتطويرية:

- تدريب وتأهيل الكوادر في مجال حوكمة المشاريع والأمن السيبراني من خلال برامج تخصصية معتمدة.
- تطبيق أدوات التحليل الإحصائي والرقمي لقياس نضج الحوكمة وفعالية التنفيذ في المؤسسات.
- الاستفادة من الخبرات الدولية في بناء أطر حوكمة متقدمة تواكب التطورات التقنية العالمية.

رابعاً: التوصيات البحثية المستقبلية:

- إجراء دراسات ميدانية كمية موسّعة لتقييم أثر نضج الحوكمة على الأداء المؤسسي.
- دراسة العلاقة بين الحوكمة وإدارة المخاطر في مشاريع التحول الرقمي بالقطاع العام والخاص.

خاتمة الدراسة:

اختتمت هذه الدراسة إلى أن نجاح مشاريع الأمن السيبراني في مؤسسات القطاع الخاص بالمملكة العربية السعودية يعتمد بدرجة كبيرة على مستوى نضج الحوكمة المؤسسية ومدى وضوح الأدوار والمسؤوليات وآليات المتابعة والتقييم داخل تلك المؤسسات. فقد أظهرت النتائج أن المؤسسات التي تطبق أطر حوكمة واضحة ومنظمة تتمتع بقدرة أعلى على تحقيق أهداف مشاريعها التقنية في الوقت المحدد، وبجودة أعلى وكفاءة تشغيلية أكبر، مقارنة بتلك التي تفتقر إلى هيكل حوكمة فعال.

وتبيّن من خلال تحليل الدراسات السابقة والمقابلات النوعية أن القصور في تحديد الصلاحيات والمسؤوليات، وضعف التواصل بين الفرق الفنية والإدارية، يمثلان من أبرز التحديات التي تعيق تحقيق التكامل في مشاريع الأمن السيبراني. كما كشفت النتائج عن تفاوت كبير في ممارسات الحوكمة بين المؤسسات الصغيرة والمتوسطة والكبيرة، مما يؤكد الحاجة إلى إطار وطني موحد يضمن تطبيق معايير الحوكمة بصورة متكاملة في مختلف القطاعات.

وانطلاقاً من ذلك، تؤكد هذه الدراسة على أهمية تبني إطار وطني شامل لتحسين حوكمة إدارة مشاريع الأمن السيبراني، بحيث يشمل مراحل التخطيط، التنفيذ، المراقبة، والتقييم، مع تحديد آليات واضحة للمتابعة والمساءلة على جميع المستويات. إن وجود هذا الإطار من شأنه أن يعزز كفاءة المؤسسات في إدارة المخاطر السيبرانية، ويرفع من مستوى الجاهزية الرقمية، ويُسهم في حماية البنية التحتية الوطنية من التهديدات والهجمات الإلكترونية المتزايدة.

كما توصي الدراسة بضرورة إدراج الحوكمة كعنصر استراتيجي في منظومة التحول الرقمي الوطني، بحيث لا تُعامل كمجموعة إجراءات تنظيمية فحسب، بل كمنهج إداري متكامل يعزز الشفافية والمساءلة ويضمن استدامة مبادرات الأمن السيبراني. ويمكن تحقيق ذلك من خلال إشراك جميع الأطراف المعنية في مراحل اعتماد المشاريع، ابتداءً من التقييم التقني المسبق للمشروع، مروراً بمراجعة طرف ثالث محايد لتحديد جدوى التنفيذ، وانتهاءً بالاعتماد النهائي من إدارة المشاريع في المؤسسة.

إن تطبيق هذا الإطار الشامل من شأنه أن يسهم في تحقيق التحول الرقمي الآمن والمستدام الذي تسعى إليه المملكة ضمن رؤية 2030، عبر مواءمة الأهداف التقنية مع الأهداف الاستراتيجية للمؤسسات، وتبني أفضل الممارسات العالمية في الحوكمة والمساءلة.

وبذلك، تمثل نتائج هذه الدراسة خطوة علمية وعملية مهمة نحو بناء بيئة سيبرانية أكثر كفاءة واستدامة، تُمكن مؤسسات القطاع الخاص من المساهمة الفاعلة في حماية أمن المملكة الرقمي وتعزيز تنافسيتها عالمياً.

المراجع:

المراجع المحلية:

- القرني، م. (2024).
حوكمة مشاريع الأمن السيبراني في القطاع الخاص السعودي.
- * الشهري، أ. (2023).
* تطبيق معايير الحوكمة ونضج المشاريع التقنية.
- الجهنّي، س. (2022).
حوكمة الأمن السيبراني في المنشآت الصغيرة والمتوسطة.
- السلمي، ر. (2024).
تقييم الالتزام بضوابط NCA.

المراجع الأجنبية:

- Project Management Institute. (2020). Governance in Cybersecurity Projects. Newtown Square, PA: Author.
- Organisation for Economic Co-operation and Development. (2021). Digital Governance Principles. Paris: OECD Publishing.
- Information Systems Audit and Control Association. (2022). COBIT Framework and Cybersecurity Governance. Schaumburg, IL: ISACA.
- Smith, J., & Clarke, R. (2023). Impact of Governance Practices on Cybersecurity Performance. Journal of Information Governance, 15(2), 45–62.
- World Economic Forum. (2023). Global Cybersecurity Outlook 2023. Geneva: World Economic Forum.
- Deloitte. (2024). Cyber Governance and Digital Transformation Report. London: Deloitte Insights.
- European Union Agency for Cybersecurity. (2023). Cybersecurity Governance Maturity Report. Athens: ENISA Publications.
- National Cybersecurity Authority. (2022). Essential Cybersecurity Controls (ECC-1). Riyadh: NCA.

الاستبانة:

جامعة ميدأوشن

كلية إدارة الأعمال

برنامج الماجستير في إدارة المشاريع

عنوان المشروع: إطار تحسين حوكمة إدارة مشاريع الأمن السيبراني.

تهدف هذه الاستبانة إلى جمع آراء المختصين حول واقع ممارسات حوكمة مشاريع الأمن السيبراني في المؤسسات و القطاع الخاص، والتحديات التي تواجه تنفيذها، بهدف تطوير إطار لتحسين فعالية واستدامة الحوكمة. تُستخدم المعلومات لأغراض البحث العلمي فقط، وستُعامل بسرية تامة. نأمل منك الإجابة بكل موضوعية وشكرًا لتعاونك.

أولاً: المعلومات العامة:

الخصائص الديموغرافية:

رقم	السؤال	الخيارات
1	الجنس	☐ ذكر ☐ أنثى
2	الفئة العمرية	☐ أقل من 30 سنة ☐ من 30 إلى 40 سنة ☐ من 41 إلى 50 سنة ☐ أكثر من 50 سنة
3	المؤهل العلمي	☐ دبلوم ☐ بكالوريوس ☐ ماجستير ☐ دكتوراه
4	سنوات الخبرة في مجال الأمن السيبراني	☐ أقل من 3 سنوات ☐ من 3 إلى 6 سنوات ☐ من 7 إلى 10 سنوات ☐ أكثر من 10 سنوات

رقم	السؤال	الخيارات
5	المسمى الوظيفي	☐ مدير مشروع ☐ مدير حوكمة ☐ خبير أمن سيبراني ☐ مدير جودة أخرى
6	نوع المؤسسة	☐ شركة خاصة ☐ مؤسسة مالية ☐ منشأة صناعية ☐ جهة خدمية ☐ أخرى
7	حجم المؤسسة	☐ صغيرة (1-50 موظف) ☐ متوسطة (51-250 موظف) ☐ كبيرة (أكثر من 250 موظف)
8	عدد مشاريع الأمن السيبراني المنفذة خلال آخر 3 سنوات	☐ 1-3 مشاريع ☐ 4-6 مشاريع ☐ أكثر من 6 مشاريع
9	هل لدى المؤسسة إطار حوكمة رسمي لمشاريع الأمن السيبراني؟	☐ نعم ☐ لا ☐ قيد التطوير

ثانيًا: محور واقع تطبيق الحوكمة في مشاريع الأمن السيبراني:

يرجى تحديد مدى موافقتك على العبارات التالية باستخدام مقياس ليكرت الخماسي:

(1 = أعارض بشدة، 5 = أوافق بشدة)

رقم	العبرة	1	2	3	4	5
1	تمتلك المؤسسة إطارًا معتمدًا لحوكمة مشاريع الأمن السيبراني	☐	☐	☐	☐	☐
2	يتم تحديد الأدوار والمسؤوليات بوضوح في جميع مراحل المشروع	☐	☐	☐	☐	☐
3	يوجد إشراف إداري دوري على مراحل تنفيذ المشروع	☐	☐	☐	☐	☐
4	يتم تقييم أداء المشاريع بانتظام وفق معايير واضحة	☐	☐	☐	☐	☐
5	آليات المتابعة والمساءلة فعالة داخل المؤسسة	☐	☐	☐	☐	☐

ثالثًا: محور التحديات والعوامل المؤثرة:

رقم	العبرة	1	2	3	4	5
6	ضعف التنسيق بين الإدارات الفنية والإدارية يؤثر على جودة التنفيذ.	☐	☐	☐	☐	☐
7	نقص الكفاءات المتخصصة في الحوكمة من أكبر التحديات.	☐	☐	☐	☐	☐
8	محدودية الميزانيات المخصصة للمشاريع تعيق تطبيق الحوكمة الفعالة.	☐	☐	☐	☐	☐
9	عدم وضوح السياسات الداخلية يحد من فعالية اتخاذ القرار.	☐	☐	☐	☐	☐
10	ضعف ثقافة الحوكمة في بعض المؤسسات يعرقل التطوير.	☐	☐	☐	☐	☐

رابعًا: محور العلاقة بين الحوكمة ونجاح المشاريع:

رقم	العبرة	1	2	3	4	5
11	وجود إطار حوكمة واضح يساهم في تحسين نتائج المشاريع.	☐	☐	☐	☐	☐
12	وضوح الأدوار والمسؤوليات يعزز سرعة اتخاذ القرار.	☐	☐	☐	☐	☐
13	المتابعة الدورية تساهم في تقليل المخاطر التشغيلية.	☐	☐	☐	☐	☐

رقم	العبارة	1	2	3	4	5
14	مشاريع الأمن السيبراني التي تطبق الحوكمة تحقق نتائج أفضل.	☐	☐	☐	☐	☐
15	تطبيق الحوكمة يزيد من استدامة المشاريع وجودة المخرجات.	☐	☐	☐	☐	☐

خامساً: مقترحات التطوير

يرجى كتابة ملاحظاتك أو اقتراحاتك في تحسين حوكمة مشاريع الأمن السيبراني:

.....

.....

.....

شكر وتقدير

نشكر لكم تعاونكم ومساهمتم في إنجاح هذا البحث،
ونسأل الله أن ينفع بنتائجه مؤسسات القطاعين الخاص والعام في تعزيز كفاءة واستدامة الأمن السيبراني.

الفصل الخامس

الاطار التحسيني المقترح

الإطار التحسيني المقترح:

أولاً: فكرة الإطار:

يقترح الباحث نموذجًا تحسينيًا يهدف إلى رفع كفاءة حوكمة القرار في مشاريع الأمن السيبراني قبل اعتمادها وتنفيذها، وذلك من خلال تطبيق عملية تقييم متعددة المراحل تضمن فحص المشروع من الزوايا التقنية، الاستراتيجية، والإدارية، بما يضمن توافقه مع أهداف المؤسسة وتقليل المخاطر المحتملة.

ثانيًا: مراحل الاعتماد المقترحة:

المخرجات المتوقعة	وصف المرحلة	الجهة المسؤولة	المرحلة
تقرير فني يوضح الضرورة التقنية وجدوى المشروع.	يتم فيها تحليل مبررات المشروع من منظور تقني لتحديد مدى الحاجة إليه، وتقييم المخاطر والثغرات التي يسعى لمعالجتها.	قسم الأمن السيبراني / فريق الخبراء الفنيين	المرحلة الأولى: التقييم التقني المبدئي
تقرير محايد يحدد مستوى الأولوية والمخاطر.	تتم مراجعة نتائج التقييم الداخلي بواسطة طرف ثالث مختص لتأكيد مدى واقعية الحاجة إلى المشروع وتحديد أولويته الفعلية بناءً على درجة الخطورة أو الثغرة الأمنية.	جهة خارجية مستقلة أو استشاري محايد	المرحلة الثانية: التقييم المحايد (الطرف الثالث)
قرار اعتماد المشروع كجزء من خطة الأمن السيبراني السنوية.	بعد اكتمال التقييمين الفني والمحايد، يتم رفع التوصية إلى اللجنة الإدارية لاتخاذ قرار الاعتماد الرسمي.	إدارة المشاريع / اللجنة العليا للأمن السيبراني	المرحلة الثالثة: الموافقة المؤسسية والإدارية

ثالثًا: أهداف الإطار:

- ضمان الحوكمة الرشيدة في اختيار مشاريع الأمن السيبراني.
- تقليل الهدر المالي والزمني في المشاريع غير الضرورية أو المكررة.
- رفع مستوى الشفافية والمساءلة في القرارات المتعلقة باعتماد المشاريع.
- تحقيق التوازن بين الأهداف التقنية والاستراتيجية للمؤسسة.

رابعاً: الآلية التشغيلية للإطار:

الخطوة	الوصف	الأداة المستخدمة
1	استقبال طلب المشروع من الجهة المعنية بالأمن السيبراني	نموذج طلب مشروع سيبراني
2	تنفيذ تحليل فني شامل للمخاطر والاحتياجات	مصفوفة تقييم المخاطر (Risk Matrix)
3	إحالة المشروع إلى جهة محايدة للمراجعة	تقرير تقييم محايد
4	مراجعة نهائية من قسم إدارة المشاريع واعتماد الجدول الزمني والميزانية	نموذج الموافقة النهائية (Approval Form)
5	تسجيل المشروع ضمن محفظة مشاريع الأمن السيبراني المؤسسية	قاعدة بيانات المشاريع (Project Portfolio)

خامسًا: الشكل التوضيحي للإطار:



يبدأ المسار من قسم الأمن السيبراني الذي يرفع طلب المشروع بناءً على تقييم الحاجة الفعلية. بعد ذلك ينتقل الطلب بعد ذلك إلى الطرف الثالث المحايد لتقييم الأهمية والأولوية وضمان الحيادية في القرار. ثم يُحال إلى إدارة المشاريع لاعتماد المشروع رسميًا ضمن الخطة السيبرانية السنوية للمؤسسة. وأخيرًا تتم متابعة التنفيذ والتقييم لضمان تحقيق الأهداف وتقليل المخاطر التشغيلية.

سادسا: الفوائد المتوقعة من تطبيق الإطار:

- تحسين جودة قرارات اعتماد مشاريع الأمن السيبراني من خلال تطبيق آلية تقييم متعددة المراحل، تجمع بين التحليل الفني المتخصص والمراجعة المحايدة، مما يضمن اختيار المشاريع الأكثر أهمية وتأثيراً على مستوى المؤسسة.
- تعزيز مستوى الشفافية في عمليات اتخاذ القرار عبر الاعتماد على معايير واضحة ومحددة لتقييم المشاريع، الأمر الذي يقلل من التحيزات الداخلية ويعزز الثقة بين مختلف الأطراف المعنية.
- دعم مبدأ الحيادية المؤسسية من خلال إشراك طرف ثالث مستقل في عملية التقييم، مما يساهم في تقديم رؤية موضوعية حول أولوية المشروع وجدواه الفعلية.
- توحيد معايير وإجراءات تقييم مشاريع الأمن السيبراني بين الإدارات المختلفة داخل المؤسسة، بما يحد من التباين في أساليب التقييم ويعزز التكامل التنظيمي.
- رفع مستوى الكفاءة التشغيلية من خلال التركيز على تنفيذ المشاريع ذات القيمة الاستراتيجية العالية، وتقليل الهدر في الموارد الناتج عن تنفيذ مشاريع منخفضة الجدوى.
- تحسين استغلال الموارد البشرية والتقنية والمالية، من خلال توجيهها نحو المشاريع الأكثر تأثيراً في تقليل المخاطر وتعزيز الأمن السيبراني.
- تعزيز قدرات إدارة المخاطر عبر تطبيق تقييم مبكر وشامل للمخاطر السيبرانية، مما يساعد في اكتشاف التهديدات المحتملة ومعالجتها قبل مرحلة التنفيذ.
- تقليل احتمالية تعثر المشاريع أو تأخرها، نتيجة وضوح مراحل الاعتماد وآليات المتابعة والتقييم المستمر خلال دورة حياة المشروع.
- تحسين جودة مخرجات مشاريع الأمن السيبراني، من خلال ضمان توافقها مع الأهداف الاستراتيجية للمؤسسة والمعايير المهنية المعتمدة.
- تعزيز مستوى المساءلة المؤسسية عبر تحديد واضح للأدوار والمسؤوليات في جميع مراحل اعتماد وتنفيذ المشاريع.
- دعم التكامل بين الجوانب التقنية والإدارية في إدارة مشاريع الأمن السيبراني، بما يحقق توازناً فعالاً بين متطلبات الحماية والأهداف التشغيلية.
- تحقيق التوافق مع المعايير الوطنية والدولية في مجال الحوكمة، مثل معايير الهيئة الوطنية للأمن السيبراني (NCA) وأطر COBIT و PMI، مما يعزز الامتثال التنظيمي ويرفع مستوى النضج المؤسسي.
- الإسهام في رفع مستوى نضج الحوكمة داخل المؤسسات، من خلال تطبيق ممارسات منظمة وقابلة للقياس والتطوير المستمر.
- تعزيز القدرة التنافسية للمؤسسات في البيئة الرقمية، عبر تحسين كفاءة إدارة المشاريع السيبرانية ورفع مستوى الجاهزية لمواجهة التهديدات.
- دعم استدامة مبادرات الأمن السيبراني على المدى الطويل، من خلال ضمان اختيار المشاريع ذات الأثر الاستراتيجي واستمرارية متابعتها وتقييمها.

الملخص Abstract

يشهد قطاع الأمن السيبراني في مؤسسات القطاع الخاص تحديات متزايدة تتعلق بضعف الحوكمة وغياب الممارسات المنظمة لإدارة المشاريع، مما يؤدي إلى تعثر التنفيذ وضعف الكفاءة التشغيلية. تهدف هذه الدراسة إلى تطوير إطار تحسيني لحوكمة إدارة مشاريع الأمن السيبراني في مؤسسات القطاع الخاص السعودي، بما يساهم في رفع فعالية التنفيذ واستدامة المبادرات السيبرانية. اعتمدت الدراسة على منهج وصفي تحليلي يجمع بين تحليل الوثائق الرسمية والمقابلات شبه المنظمة مع الخبراء، إلى جانب مراجعة الأدبيات المحلية والدولية ذات الصلة. توصلت النتائج إلى وجود علاقة إيجابية بين مستوى نضج الحوكمة ونجاح مشاريع الأمن السيبراني، مع وجود فجوات في وضوح الأدوار والمسؤوليات وآليات المتابعة والتقييم. وانطلاقاً من هذه النتائج، اقترحت الدراسة إطاراً تحسينياً ثلاثي المراحل لاعتماد مشاريع الأمن السيبراني قبل تنفيذها، يشمل: (1) التقييم التقني الداخلي من قبل خبراء الأمن السيبراني، (2) مراجعة محايدة من طرف ثالث لتحديد أولوية المشروع وضرورته، و(3) الاعتماد النهائي من إدارة المشاريع. يساهم تطبيق هذا الإطار في تعزيز الشفافية والحوكمة الرشيدة، وتقليل الهدر المالي والزمني، وتحقيق التكامل بين الأهداف التقنية والإستراتيجية، بما يتوافق مع رؤية المملكة 2030 ومعايير الهيئة الوطنية للأمن السيبراني (NCA) والأطر العالمية مثل COBIT و PMI. ويُتوقع أن يؤدي هذا الإطار إلى رفع نضج الحوكمة وتحسين أداء مؤسسات القطاع الخاص في إدارة مشاريع الأمن السيبراني على نحو مستدام.

The cybersecurity sector within Saudi Arabia's private institutions faces increasing challenges due to weak governance practices and the absence of structured project management frameworks. These challenges often result in delayed execution, inefficient resource utilization, and limited sustainability of cybersecurity initiatives. This study aims to develop an enhancement framework for the governance of cybersecurity project management in the Saudi private sector to improve implementation efficiency and long-term sustainability. A descriptive-analytical methodology was adopted, combining document analysis, semi-structured expert interviews, and an extensive review of relevant local and international literature. Findings revealed a strong positive relationship between governance maturity and project success, alongside notable gaps in role clarity, risk management, and monitoring mechanisms. Based on these findings, the study proposes a three-stage enhancement framework for project approval prior to implementation: (1) a technical evaluation conducted by cybersecurity experts, (2) an independent third-party assessment to determine project priority and necessity, and (3) final approval by the project management department. The proposed framework enhances transparency, accountability, and strategic alignment, reducing financial and operational inefficiencies while ensuring compliance with Saudi National Cybersecurity Authority (NCA) standards and international frameworks such as COBIT and PMI. Its application is expected to strengthen governance maturity and improve the overall effectiveness and sustainability of cybersecurity project management in Saudi private institutions.

College of Management

Master of Project Management



Final Project Title:

**Framework for Improving Governance of Cybersecurity Project
Management**

Prepared by:

Nawaf Adnan Aljehani

Supervised by:

Al Faisal Abdul Hamid

Year: 2026