

Final Project 1

Code: MGM 496-PMG496

Project Template

Faculty of Management
Midocean University

أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية
المؤسسات الحكومية للتصدي للاختراقات – دراسة ميدانية على وزارات
المنطقة الشرقية

أسم الطالب

معاذ التركي

233000082

مشروع تخرج- 1

كلية الإدارة- جامعة ميدأوشن

إشراف

د. عبدالرحيم نادر

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي

جدول المحتويات

1. الفصل الأول: الإطار العام للدراسة	3
1.1. المقدمة:	4
1.2. مشكلة الدراسة	5
1.2.1. فجوات على المستوى النظري	5
1.2.2. فجوات على المستوى التطبيقي	6
1.3. أهمية الدراسة	7
1.3.1. على المستوى النظري:	7
1.3.2. على المستوى التطبيقي:	7
1.4. أسئلة الدراسة	8
1.5. أهداف الدراسة	9
1.6. فرضيات الدراسة	9
1.7. نموذج الدراسة	10
1.8. منهجية الدراسة	10
1.9. الدراسة الميدانية	10
1.10. مخطط المشروع المقترح	10
2. الفصل الثاني: الدراسات السابقة	
1.	1
2.1. المقدمة:	12
2.2. المتغير المستقل	12
2.3. المتغير التابع	13
2.4. العلاقة بين المتغير المستقل والمتغير التابع	13
2.5. الخاتمة	13
قائمة المراجع	13

1. الفصل الأول: الإطار العام للدراسة

1.1. المقدمة:

يشهد العالم اليوم تحولاً رقمياً متسارعاً أعاد تشكيل طبيعة العمل المؤسسي وأسلوب تقديم الخدمات الحكومية، إذ باتت البنى التحتية الرقمية ركيزة أساسية لاقتصادات الدول وأمنها الوطني. وقد أفرز هذا التحول واقعاً جديداً تتعاظم فيه المخاطر السيبرانية بوصفها أحد أبرز التهديدات التي تواجه الحكومات والمنظمات على حدٍ سواء؛ حيث تستهدف الهجمات السيبرانية البيانات الحساسة والأنظمة الحيوية والخدمات العامة، بما يهدد استقرار المؤسسات وثقة المواطنين فيها. وفي ضوء ذلك، أصبح الأمن السيبراني عنصراً استراتيجياً لا غنى عنه ضمن منظومة الحوكمة الرقمية الحديثة، خاصة في القطاعات الحكومية التي تتعامل مع بيانات وطنية حساسة وتُقدّم خدمات لا تحتل التوقف. (Pemmasani, 2023)

وفي هذا السياق العالمي المتغيّر، أولت المملكة العربية السعودية الأمن السيبراني اهتماماً بالغاً انسجاماً مع مستهدفات رؤية المملكة 2030، فأنشأت الهيئة الوطنية للأمن السيبراني (NCA) عام 1438هـ بوصفها الجهة المختصة بتنظيم الأمن السيبراني على المستوى الوطني وتعزيزه وحماية المصالح الحيوية للدولة. وقد أصدرت الهيئة منظومة متكاملة من الأطر والضوابط، يأتي في مقدمتها الضوابط الأساسية للأمن السيبراني (ECC) التي تتضمن في نسختها المحدثّة (ECC-2:2024) خمسة مكونات رئيسية و(29) مكوناً فرعياً و(114) ضابطاً، تمثل الحد الأدنى الإلزامي الذي يتعين على الجهات الوطنية الالتزام به لحماية أصولها المعلوماتية والتقنية. كما أصدرت الهيئة ضوابط متخصصة مثل ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC) وضوابط التقنية التشغيلية (OTCC)، بهدف توحيد مستويات النضج السيبراني وتقليل المخاطر الوطنية.

ويتقاطع هذا التوجه الوطني مع توجهات دولية مماثلة تركز على بناء قدرات المؤسسات الحكومية لمواجهة الاختراقات، إذ تشير الأدبيات الحديثة إلى أن الجاهزية السيبرانية (Cybersecurity Readiness) أصبحت محدداً جوهرياً لأداء المؤسسات وقدرتها على الصمود في وجه التهديدات، وأن الالتزام بأطر الحوكمة السيبرانية ينعكس إيجاباً على فاعلية الاستجابة للحوادث وإدارة المخاطر (Mohamed Noor et al., 2026)؛ (Majeed et al., 2026) كما بيّنت دراسات مقارنة بين بيانات مختلفة أن وجود إطار تنظيمي وطني واضح

يُمثّل عاملاً حاسماً في رفع مستوى النضج السيبراني وتقليل الفجوة بين السياسات والتطبيق الفعلي (Rawindaran et al., 2023).

غير أن الواقع التطبيقي يكشف أن إصدار الضوابط وحده لا يكفي لتحقيق الجاهزية المطلوبة، إذ تتفاوت المؤسسات الحكومية في مستوى التزامها وقدرتها على ترجمة هذه الضوابط إلى ممارسات فعلية وإجراءات تشغيلية مؤثرة. وتتأثر هذه الجاهزية بعوامل متعددة منها: مستوى الوعي السيبراني، توافر الكفاءات البشرية، كفاية الموازنات المخصصة، ومدى تكامل الحوكمة السيبرانية مع باقي منظومات الحوكمة المؤسسية. وتُعدّ المنطقة الشرقية في المملكة العربية السعودية بيئة ذات أهمية خاصة في هذا السياق، نظراً لاحتضانها قطاعات حيوية تجعل وزاراتها وفروعها الحكومية مستهدفة بصفة متكررة من الهجمات السيبرانية.

ومن هذا المنطلق، تأتي الدراسة الحالية لتسليط الضوء على أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات، من خلال دراسة ميدانية على وزارات المنطقة الشرقية، وذلك بهدف قياس مستوى الالتزام الفعلي بهذه المعايير، وتحديد طبيعة العلاقة بينها وبين مؤشرات الجاهزية، والوقوف على الفجوات التي تحول دون تحقيق الفاعلية المرجوة، بما يُسهم في تقديم توصيات عملية تدعم صناع القرار في تعزيز المنظومة السيبرانية الوطنية.

1.2. مشكلة الدراسة

على الرغم من الجهود التشريعية والتنظيمية التي بذلتها الهيئة الوطنية للأمن السيبراني (NCA) في إصدار حزمة متكاملة من الضوابط الإلزامية، وفي مقدمتها الضوابط الأساسية للأمن السيبراني (ECC) بنسختها الأحدث (ECC-2:2024)، إلا أن مؤشرات الواقع تشير إلى استمرار وقوع الجهات الحكومية ضحايا لاختراقات سيبرانية متفاوتة الخطورة، وإلى تباين واضح بين المؤسسات في مستوى تطبيقها للضوابط وفي درجة جاهزيتها الفعلية للتصدي للتهديدات. وهذا يطرح تساؤلاً جوهرياً حول العلاقة بين الالتزام الشكلي بالمعايير من جهة، وتحقيق الجاهزية التشغيلية الحقيقية من جهة أخرى، خاصة في ظل ندرة الدراسات الميدانية التي تناولت هذه العلاقة في السياق السعودي عموماً، وفي وزارات المنطقة الشرقية على وجه التحديد.

1.2.1. فجوات على المستوى النظري

تتمثل الفجوات النظرية التي تسعى الدراسة إلى معالجتها في أن معظم الأدبيات السابقة التي تناولت الأمن السيبراني الحكومي ركزت على الجوانب التقنية أو السياساتية بمعزل عن قياس الأثر الفعلي للأطر الوطنية على الجاهزية المؤسسية. فقد بحثت دراسة (Pemmasani, 2023) في أطر الأمن السيبراني الوطنية للبنى التحتية الحرجة من منظور مقارن دون التعمق في إطار تنظيمي قطري بعينه، كما تناولت دراسة (Rawindaran et al., 2023) حوكمة الأمن السيبراني في المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية والمملكة المتحدة دون التطرق إلى المؤسسات الحكومية. وفي المقابل، ركزت دراسة (Mohamed Noor et al., 2026) على أثر الجاهزية السيبرانية على الأداء الأمني التنظيمي في البيئة الماليزية، بينما تناولت دراسة (Majeed et al., 2026) حوكمة الأمن السيبراني في السياق الباكستاني، وهو ما يكشف عن غياب دراسات نظرية تربط مباشرة بين منظومة معايير NCA السعودية ومؤشرات الجاهزية للتصدي للاختراقات في القطاع الحكومي. كما يُلاحظ ندرة الأطر النظرية التي تُكامل بين أبعاد الحوكمة وإدارة المخاطر والصمود التنظيمي ضمن نموذج واحد يُختبر في السياق السعودي، وهو ما تسعى هذه الدراسة إلى الإسهام في معالجته من خلال بناء إطار مفاهيمي يربط بين متغيرات تطبيق الضوابط ومخرجات الجاهزية.

1.2.2. فجوات على المستوى التطبيقي

أما على المستوى التطبيقي، فإن قاعدة الدراسات الميدانية التي قيّمت الأثر الفعلي لتطبيق معايير NCA على جاهزية الجهات الحكومية السعودية لا تزال محدودة، ولم يُرصد حسب علم الباحث وجود دراسة ميدانية مخصصة لوزارات المنطقة الشرقية تحديداً، مع ما تتميز به هذه المنطقة من ثقل اقتصادي وحضور لقطاعات حيوية يجعل مؤسساتها هدفاً متكرراً للهجمات السيبرانية. كما يُلاحظ في الواقع التطبيقي تفاوت واضح بين الجهات الحكومية في مستوى نضج الأمن السيبراني، وفي مدى ترجمة الالتزام التنظيمي بالضوابط إلى ممارسات تشغيلية فاعلة على أرض الواقع، إضافة إلى وجود تحديات تتعلق بنقص الكوادر المتخصصة، ومحدودية الوعي السيبراني لدى الموظفين، وضعف تكامل منظومات الاستجابة للحوادث، وهو ما أشارت إليه ضمناً تقارير الجهات الرقابية ومؤشرات النضج السيبراني الوطنية. ويُضاف إلى ذلك غياب أدوات قياس عملية تربط بين كل بُعد من أبعاد الضوابط الأساسية ومؤشر محدد من مؤشرات الجاهزية للتصدي للاختراقات، مما يُصعب على الجهات الحكومية تشخيص فجواتها الفعلية وتحديد أولويات التحسين.

وفي ضوء ما تقدّم من فجوات نظرية وتطبيقية، يمكن صياغة السؤال الرئيسي للدراسة على النحو الآتي:

ما أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية؟

1.3. أهمية الدراسة

تستمد هذه الدراسة أهميتها من حداثة موضوعها وارتباطه المباشر بأحد أهم محاور رؤية المملكة 2030 المتعلق ببناء اقتصاد رقمي آمن ومستدام، فضلاً عن كونها تتناول قطاعاً حساساً يتمثل في المؤسسات الحكومية التي تُعدّ خط الدفاع الأول عن البيانات الوطنية والخدمات العامة. وتنقسم أهمية الدراسة إلى بُعدين متكاملين:

1.3.1. على المستوى النظري:

تُسهّم الدراسة في إثراء الأدبيات العربية والسعودية المتعلقة بالأمن السيبراني الحكومي من خلال تقديم إطار نظري يربط بين معايير – NCA بوصفها متغيراً مستقلاً متعدد الأبعاد يشمل الحوكمة وتعزيز الأمن السيبراني وصموده ومكوّناته المتعلقة بالأطراف الخارجية والحوسبة السحابية والأنظمة الصناعية – ومتغير الجاهزية للتصدي للاختراقات بوصفه متغيراً تابعاً يشمل أبعاد الوقاية والاكتشاف والاستجابة والتعافي. كما تُعدّ الدراسة إضافة معرفية تُقلّص الفجوة في الأبحاث التي تناولت أثر الأطر التنظيمية الوطنية على الأداء السيبراني للمؤسسات الحكومية في السياق السعودي، وتفتح المجال أمام دراسات لاحقة لاختبار النموذج في قطاعات أو مناطق جغرافية أخرى، أو لإجراء دراسات مقارنة مع أطر مماثلة في دول الخليج والشرق الأوسط. ويُتوقع أن تُسهّم نتائج الدراسة في تطوير الأدوات المفاهيمية المستخدمة في قياس النضج السيبراني المؤسسي، وفي تعميق فهم العلاقة بين الامتثال التنظيمي والصمود السيبراني الفعلي.

1.3.2. على المستوى التطبيقي:

تكتسب الدراسة أهميتها التطبيقية من كونها تقدّم تشخيصاً ميدانياً لواقع تطبيق معايير NCA في وزارات المنطقة الشرقية، وتوفّر للقيادات الحكومية ومسؤولي الأمن السيبراني صورة واضحة عن مستوى الجاهزية الفعلية ومواطن القوة والضعف في تطبيق الضوابط. كما تُسهّم نتائج الدراسة في تزويد الهيئة الوطنية للأمن السيبراني (NCA) بمؤشرات ميدانية مفيدة في مراجعة آليات الإشراف والمتابعة ودعم الجهات الحكومية في رحلة الامتثال، بما يُعزّز فاعلية المنظومة الوطنية ككل. ومن المتوقع أن تُفيد الدراسة الجهات الحكومية في توجيه

استثماراتها في الأمن السيبراني نحو الأبعاد الأكثر تأثيراً في الجاهزية، وفي تطوير برامج بناء القدرات والتدريب وفقاً للفجوات المُشخَّصة. كما قد تُشكّل التوصيات العملية للدراسة مرجعاً مساعداً لصنّاع القرار في تطوير السياسات الداخلية للوزارات، وتعزيز ثقافة الأمن السيبراني، وبناء قدرات الاستجابة للحوادث، بما يُسهم في النهاية في حماية الأصول الوطنية وتعزيز ثقة المستفيدين بالخدمات الحكومية الرقمية.

1.4. أسئلة الدراسة

السؤال الرئيسي : ما أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية؟

ويتفرع من السؤال الرئيسي مجموعة من الأسئلة الفرعية على النحو الآتي:

1. ما أثر تطبيق بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

2. ما أثر تطبيق بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

3. ما أثر تطبيق بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

4. ما أثر تطبيق بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

5. ما أثر تطبيق بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

1.5. أهداف الدراسة

تهدف هذه الدراسة إلى دراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

وينبثق من هذا الهدف الرئيسي مجموعة من الأهداف الفرعية التي تُسهم مجتمعة في تحقيقه، وهي على النحو الآتي:

- قياس أثر بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- الخروج بمجموعة من التوصيات والمقترحات العملية التي تُسهم في رفع كفاءة تطبيق معايير NCA، وتعزيز جاهزية المؤسسات الحكومية للتصدي للاختراقات، بما يدعم صناع القرار في الهيئة الوطنية للأمن السيبراني وفي الوزارات المعنية.

1.6. فرضيات الدراسة

1.7. نموذج الدراسة

1.8. منهجية الدراسة

1.9. الدراسة الميدانية

1.10. مخطط المشروع المقترح

2. الفصل الثاني: الدراسات السابقة

2.1. المقدمة:

2.2. المتغير المستقل

2.3. المتغير التابع

2.4. العلاقة بين المتغير المستقل والمتغير التابع

2.5. الخاتمة

قائمة المراجع

Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. *International Journal of Acta Informatica*, 2(1), 209-218

Mohamed Noor, A. F., Moghavvemi, S., & Tajudeen, F. P. (2026). Assessing the impact of cybersecurity readiness on organizational security performance: a study on Malaysian organizations. *Journal of Enterprise Information Management*, 39(3), 907-927.

Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan. *Social Science Review Archives*, 4(1), 1806-1829

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital*, 3(3), 200-231.