

جامعة ميدأوشن



كلية الإدارة

قسم / تخصص إدارة مخاطر

تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية دراسة تطبيقية

على المؤسسات المالية السعودية

إعداد الطالب/

ندى راشد أبالخير

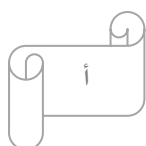
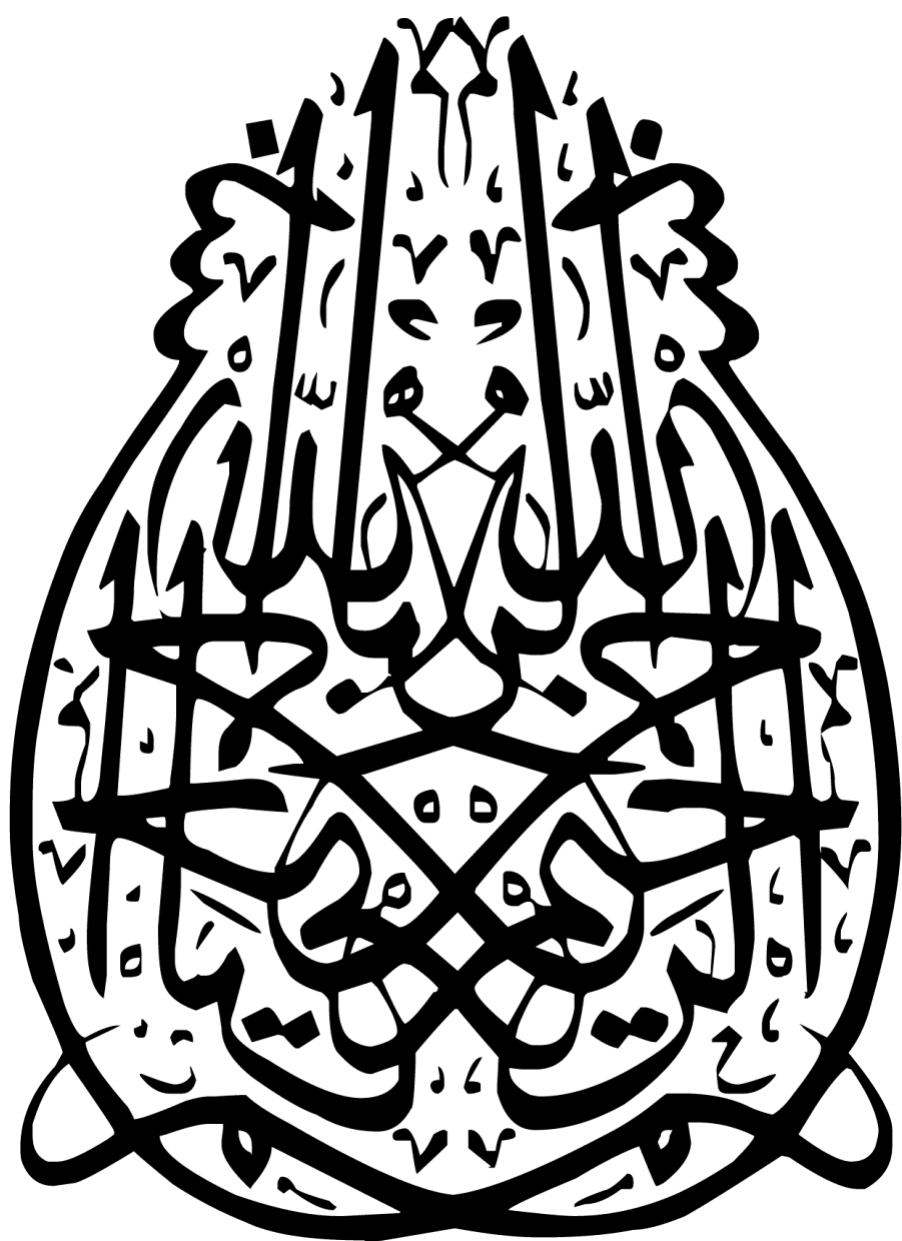
242000219

إشراف/

أ.د / الفیصل عبد الحمید

أ.د / فايز جراد

2025 – 1446

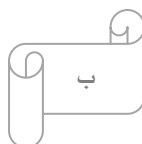


# إهداء

إلى أظهر قلبين في حياتي... والديَّ العزيزين

إلى جميع الأقارب والأصدقاء

أهديكم بحثي، وأدعو الله أن يحوز إعجابكم.



# شكر ونفلة

نحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي،

والذي ألهمنا الصحة والعافية والعزيمة.

فالحمد لله حمداً كثيراً

نتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور /

د. فايز علي جراد

د. الفیصل عبد الحمید محمد حسن

على كل ما قدمه لنا من توجيهات ومعلومات قيمة ساهمت في إثراء موضوع دراستنا في

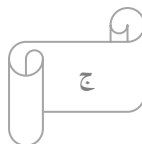
جوانبها المختلفة.

والشكر والتقدير موصول إلى إدارة جامعة ميد أوشن ممثلة بالكادر الأكاديمي والإداري، لما

قدموه من تسهيلات وتشجيع وتوفير الخدمات المطلوبة.

كما أتقدم بالشكر الجزيل لكل من لم يسعنا الحظ بذكر أسمائهم راجياً من المولي عز

وجل أن تكون هذه الدراسة نافذة لدراسات أخرى .



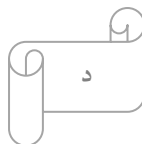
## المستخلص

تهدف هذه الدراسة إلى تحليل تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية ، و تم اختيار عينة عشوائية طبقية متناسبة من 364 مديراً في الإدارات العليا والوسطى، حيث تم جمع البيانات باستخدام استبانة إلكترونية وتحليلها باستخدام المنهج الوصفي التحليلي. تم تطبيق مجموعة من الأساليب الإحصائية.

أظهرت نتائج الدراسة أن ارتفاع مستوى البنية التحتية التكنولوجية كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية ، ارتفاع مستوى البرمجيات والتصميمات كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية

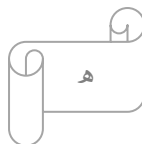
بناءً على هذه النتائج ، توصي الدراسة الاهتمام بتوفير الموارد المالية والإمكانيات اللوجستية والدعم الخاص التي يمكن من خلالها الحفاظ على المستوى المتميز من تطبيق الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة بالمملكة العربية السعودية ، العمل على توفير البيئة التحتية التي تساهم في زيادة قدرة المؤسسات المالية السعودية العاملة بالمملكة العربية السعودية على تحقيق أهدافها وفقاً لرؤية المملكة 2030

الكلمات المفتاحية: الابتكار التكنولوجي – إدارة المخاطر السيبرانية – المؤسسات المالية السعودية

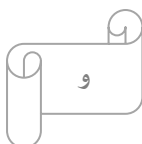


## قائمة المحتويات

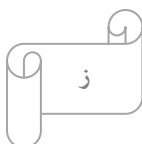
|         |                                        |
|---------|----------------------------------------|
| أ.....  | بسم الله الرحمن الرحيم.....            |
| ب.....  | الإهداء.....                           |
| ج.....  | الشكر والتقدير.....                    |
| د.....  | المستخلص.....                          |
| ه.....  | قائمة المحتويات.....                   |
| ط.....  | قائمة الجداول.....                     |
| 1.....  | الفصل الأول: الإطار العام للدراسة..... |
| 1.....  | المقدمة.....                           |
| 2.....  | 1.1 مشكلة الدراسة:.....                |
| 3.....  | 2.1 أهمية الدراسة:.....                |
| 3.....  | 1.2.1 الأهمية العلمية.....             |
| 4.....  | 2.2.1 الأهمية العملية.....             |
| 5.....  | 3.1 أهداف الدراسة:.....                |
| 7.....  | 4.1 تساؤلات الدراسة:.....              |
| 8.....  | 5.1 فرضيات الدراسة:.....               |
| 8.....  | 6.1 الدراسات السابقة:.....             |
| 14..... | 7.1 المنطلقات النظرية للدراسة:.....    |



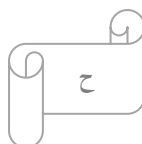
|    |                                         |
|----|-----------------------------------------|
| 16 | 8.1 المنهجية وطرق البحث:                |
| 19 | 9.1 أدوات الدراسة:                      |
| 21 | 10.1 حدود الدراسة:                      |
| 24 | الفصل الثاني: الإطار النظري             |
| 24 | المبحث الأول: الابتكار التكنولوجي       |
| 24 | المقدمة                                 |
| 25 | 1.1.2 التمييز بين المصطلحات             |
| 25 | 2.1.2 الفرق بين الإبداع والابتكار       |
| 27 | 3.1.2 مسارات الابتكار                   |
| 27 | 4.1.2 تطور الابتكار                     |
| 28 | 5.1.2 خصائص الابتكار                    |
| 28 | 6.1.2 مبادئ الابتكار ومصادره            |
| 29 | 7.1.2 مصادر الابتكار                    |
| 30 | 8.1.2 عناصر الابتكار                    |
| 31 | 9.1.2 التفكير الاستراتيجي               |
| 32 | 10.1.2 خطوات الابتكار                   |
| 32 | 11.1.2 سمات المدراء المبتكرين           |
| 34 | المبحث الثاني: إدارة المخاطر السيبرانية |
| 34 | 1.2.2 مفهوم المخاطر                     |



|    |                                                        |
|----|--------------------------------------------------------|
| 35 | 2.2.2 العلاقة بين المخاطر وعدم التأكد.....             |
| 37 | 3.2.2 أنواع المخاطر.....                               |
| 38 | 4.2.2 مفهوم الأمن السيبراني والتهديدات السيبرانية..... |
| 43 | 5.2.2 عناصر إدارة الأمن السيبراني.....                 |
| 44 | 6.2.2 الخلفية التاريخية لإدارة المخاطر وتطورها.....    |
| 45 | 7.2.2 تطور مفهوم إدارة المخاطر.....                    |
| 45 | 8.2.2 مفهوم إدارة المخاطر السيبرانية.....              |
| 47 | 9.2.2 أهمية إدارة المخاطر السيبرانية.....              |
| 48 | 10.2.2 مراحل إدارة المخاطر السيبرانية (الابعاد).....   |
| 57 | الفصل الثالث: منهجية وإجراءات الدراسة.....             |
| 57 | مقدمة.....                                             |
| 57 | 1.3 منهجية البحث.....                                  |
| 57 | 2.3 مجتمع وعينة الدراسة.....                           |
| 57 | 3.3 مصادر جمع البيانات:.....                           |
| 58 | 5.3 أداة الدراسة.....                                  |
| 59 | 6.3 صدق أداة الدراسة.....                              |
| 59 | ☐ المحور الأول: الابتكار التكنولوجي.....               |
| 62 | ☐ المحور الثاني: إدارة المخاطر السيبرانية.....         |
| 63 | 7.3 ثبات أداة الدراسة:.....                            |



|          |                                                  |
|----------|--------------------------------------------------|
| 65.....  | الفصل الرابع: تحليل النتائج                      |
| 65 ..... | مقدمة                                            |
| 65 ..... | 1.4 أولاً: خصائص عينة الدراسة                    |
| 66 ..... | 2.4 ثانياً: تحليل استمارة الاستبيان              |
| 72 ..... | 3.4 ثالثاً: اختبار فروض الدراسة                  |
| 77.....  | الفصل الخامس: خلاصة النتائج والتوصيات والمقترحات |
| 77 ..... | مقدمة                                            |
| 77 ..... | 1.5 خلاصة نتائج الدراسة                          |
| 79 ..... | 2.5 التوصيات                                     |
| 80 ..... | 3.5 المقترحات                                    |
| 81.....  | Abstract                                         |
| 82.....  | المراجع:                                         |
| 82 ..... | أولاً: المراجع العربية                           |
| 83 ..... | ثانياً: المراجع الأجنبية                         |
| 88.....  | الملاحق                                          |
| 89.....  | استمارة استبيان                                  |



## قائمة الجداول

| رقم<br>الجدول | اسم الجدول                                                                                                 | رقم<br>الصفحة |
|---------------|------------------------------------------------------------------------------------------------------------|---------------|
| (1)           | جدول (1) مستويات موافقة عينة الدراسة على عبارات أداة الدراسة                                               | 58            |
| (2)           | جدول (2) معاملات الارتباط لعبارات المحور الأول                                                             | 59            |
| (3)           | جدول (3) معاملات الارتباط لعبارات المحور الثاني                                                            | 61            |
| (4)           | جدول (4) معامل الثبات لمجاور استمارة الاستبيان                                                             | 62            |
| (5)           | جدول (5) توزيع عينة الدراسة وفقا لخصائصها                                                                  | 64            |
| (6)           | جدول (6) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات البنية التحتية التكنولوجية | 65            |
| (7)           | جدول (7) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات البرمجيات والتصميمات       | 66            |
| (8)           | جدول (8) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات الخدمات المبتكرة           | 68            |
| (9)           | جدول (9) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات التفاعل والتواصل           | 69            |
| (10)          | جدول (10) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات إدارة المخاطر السيبرانية  | 70            |

|    |                                                                             |      |
|----|-----------------------------------------------------------------------------|------|
| 71 | جدول (11) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الرئيسية        | (11) |
| 72 | جدول (12) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الاولى  | (12) |
| 73 | جدول (13) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثانية | (13) |
| 74 | جدول (14) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثالثة | (14) |

# الفصل الأول: الإطار العام للدراسة

## المقدمة

في ظل الثورة الرقمية المتسارعة التي تشهدها معظم المجالات، أصبحت المؤسسات المالية أكثر اعتمادًا على الابتكار التكنولوجي لتعزيز قدرتها التنافسية وتقديم خدمات متميزة تلبي احتياجات عملائها. ومع تقدم التقنيات مثل الذكاء الاصطناعي، وتحليل البيانات الضخمة، والبلوك تشين، تتزايد الفرص المتاحة لهذه المؤسسات، لكن في المقابل، تزداد المخاطر المرتبطة بالتهديدات السيبرانية. لذلك، يعتبر تحليل تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية من الموضوعات الحيوية التي تتطلب اهتمامًا خاصًا، نظرًا لأهمية القطاع المالي في الاقتصاد الوطني وإمكانية تعريضه لخسائر كبيرة نتيجة الهجمات السيبرانية (Diener، 2021).

تسهم الابتكارات التكنولوجية في تطوير استراتيجيات جديدة لإدارة المخاطر السيبرانية، حيث تعمل على تحسين قدرات المؤسسات في رصد وتقييم التهديدات بشكل أسرع وأكثر دقة. كما تتيح التقنيات الحديثة مثل التعلم الآلي وأدوات التحليل المتقدمة تحليل الأنماط والاتجاهات المتعلقة بالهجمات، مما يساعد في اتخاذ القرارات السريعة والفعالة لتقليل الأضرار. ومع ذلك، تتطلب هذه الابتكارات أيضًا استثمارات ضخمة في البنية التحتية التكنولوجية وتطوير المهارات البشرية، وهو ما يمثل تحديًا كبيرًا للمؤسسات المالية، خاصة في بيئة عمل تنافسية ومعقدة (Barroso، 2022).

تعتبر المؤسسات المالية في المملكة العربية السعودية في مرحلة تحول رقمي سريع، حيث تهدف الحكومة إلى تعزيز استخدام التكنولوجيا المالية (FinTech) في إطار رؤية 2030. ويشكل هذا التحول فرصة فريدة لتبني استراتيجيات مبتكرة تساهم في تطوير إدارة المخاطر السيبرانية. ومع ذلك، فإن المخاطر المرتبطة بالتحول الرقمي ليست بسيطة، حيث تتعرض المؤسسات لتهديدات جديدة تتطلب تطوير استراتيجيات متكاملة تشمل جميع جوانب العمل، من الثقافة المؤسسية إلى السياسات والإجراءات (Noreen، 2024).

سيتناول هذا البحث دراسة العلاقة بين الابتكار التكنولوجي وإدارة المخاطر السيبرانية، مع التركيز على المؤسسات المالية في السعودية. سيتم تحليل العوامل التي تعزز استخدام الابتكار التكنولوجي في إدارة المخاطر، بالإضافة إلى التحديات التي قد تواجهها المؤسسات أثناء تطبيق هذه الاستراتيجيات. كما سيتناول البحث الأساليب الفعالة التي يمكن أن تعتمد عليها المؤسسات للتخفيف من آثار المخاطر السيبرانية من خلال الابتكار. يهدف هذا البحث إلى تقديم توصيات عملية للمؤسسات المالية حول كيفية الاستفادة من الابتكار التكنولوجي لتعزيز إدارة المخاطر السيبرانية، مما يساهم في تحقيق استدامة أعلى وضمان حماية المعلومات الحساسة للعملاء والمصالح التجارية (Alhalafi، 2023).

## 1.1 مشكلة الدراسة:

تتمثل المشكلة الرئيسية التي تدور حولها هذه الدراسة في التحديات المتزايدة التي تواجهها المؤسسات المالية في المملكة العربية السعودية نتيجة ارتفاع مستوى المخاطر السيبرانية في ظل الاعتماد المتزايد على الابتكار التكنولوجي. مع تسارع التحول الرقمي وظهور تقنيات جديدة، يزداد أيضًا نطاق التهديدات السيبرانية، مما يؤدي إلى ضرورة تطوير استراتيجيات فعالة لإدارة هذه المخاطر. ومن هنا، تبرز الحاجة الملحة لفهم كيف يمكن أن يؤثر الابتكار التكنولوجي على استراتيجيات إدارة المخاطر السيبرانية، وكيف يمكن للمؤسسات المالية التكيف مع هذه التغيرات لضمان حماية بياناتها ومواردها.

### المشاكل المترتبة على المشكلة الرئيسية:

✓ يتزايد عدد الهجمات السيبرانية بشكل متسارع، مما يشكل تهديدًا مباشرًا للمؤسسات المالية. تشمل هذه الهجمات الاختراقات، وهجمات برامج الفدية، والتصيد الاحتيالي، وغيرها من أساليب الاختراق التي تهدف إلى الوصول إلى البيانات الحساسة. وبالتالي، تحتاج المؤسسات إلى استراتيجيات قوية لمواجهة هذه التهديدات.

✓ تعاني العديد من المؤسسات من ضعف الوعي والثقافة الأمنية بين موظفيها، مما يسهل على المهاجمين استغلال الثغرات البشرية. فعدم تدريب الموظفين على ممارسات الأمان السيبراني قد يؤدي إلى انكشاف البيانات الحساسة، مما يتطلب من المؤسسات الاستثمار في تدريب وتوعية الكوادر البشرية.

- ✓ إن دمج الابتكارات التكنولوجية الجديدة ضمن البنية التحتية الحالية للمؤسسات قد يواجه عقبات تقنية وتشغيلية. قد يتطلب ذلك تحديث الأنظمة القائمة، وتطوير البنية التحتية، وتخصيص موارد كبيرة، مما يمثل تحديًا للمؤسسات التي تسعى إلى تحسين إدارة المخاطر السيبرانية.
- ✓ تتعرض المؤسسات المالية لتغييرات مستمرة في القوانين والتشريعات المتعلقة بالأمن السيبراني. يتعين على المؤسسات التكيف مع هذه التغييرات، مما قد يكون عبئًا إضافيًا في ظل الضغوط التنافسية. لذا، يجب أن تكون هناك استراتيجيات مرنة يمكنها التكيف مع هذه التغييرات.
- ✓ يتطلب تعزيز الابتكار التكنولوجي في إدارة المخاطر استثمارات كبيرة في التكنولوجيا والموارد البشرية. قد تواجه المؤسسات صعوبة في تخصيص ميزانيات كافية لهذا الغرض، خاصة في ظل المنافسة الشديدة في السوق المالية، مما قد يؤثر سلبيًا على قدرتها على تطبيق استراتيجيات فعالة.
- ✓ تواجه المؤسسات المالية نقصًا في الخبرات والمهارات اللازمة لإدارة المخاطر السيبرانية بشكل فعال. يتمثل التحدي في العثور على متخصصين قادرين على مواجهة التهديدات المتزايدة وتطبيق تقنيات مبتكرة، مما يتطلب تطوير برامج تعليمية وتدريبية فعالة (Cremer، 2022).

إن فهم هذه المشاكل المترتبة على الابتكار التكنولوجي وإدارة المخاطر السيبرانية يعد أمرًا ضروريًا للمؤسسات المالية في السعودية، خاصة في ظل التحول الرقمي السريع الذي تشهده البلاد. تسعى هذه الدراسة إلى تحليل كيفية تأثير الابتكار التكنولوجي على هذه التحديات، وتقديم توصيات عملية للمؤسسات المالية لتعزيز قدرتها على مواجهة المخاطر السيبرانية، وبالتالي حماية مصالحها واستدامتها في السوق.

## 2.1 أهمية الدراسة:

### 1.2.1 الأهمية العلمية

- تكتسب هذه الدراسة أهمية علمية بارزة في مجال الدراسات المتعلقة بالابتكار التكنولوجي وإدارة المخاطر السيبرانية، حيث تساهم في توسيع الفهم الأكاديمي للعلاقة المعقدة بين هذين المجالين. في

عصر يتسم بالتطور السريع للتكنولوجيا، أصبح من الضروري تطوير نظريات جديدة لفهم كيف يمكن أن يسهم الابتكار في تحسين إدارة المخاطر. تسعى الدراسة إلى تقديم إطار نظري متكامل يعكس التفاعلات بين الابتكار وإدارة المخاطر السيبرانية، مما يساعد الباحثين والمهتمين على بناء قاعدة معرفية قوية لفهم هذه الديناميكيات.

- تسهم هذه الدراسة في توسيع الأدلة التجريبية المتاحة في هذا المجال، حيث تقدم بيانات حقيقية من المؤسسات المالية في السعودية. وهذا يعد إضافة قيمة للأدبيات الحالية، إذ يفتح المجال أمام الباحثين لاستكشاف كيفية تأثير الابتكار على إدارة المخاطر السيبرانية بشكل عملي وملمس. يمكن أن تستند الأبحاث المستقبلية إلى النتائج المستخلصة من هذه الدراسة، مما يدعم النمو المعرفي في هذا المجال ويعزز من قدرته على تلبية التحديات الحالية والمستقبلية.
- تساعد الدراسة في تحديد الثغرات الموجودة في الأدبيات الحالية. من خلال تحديد المشكلات والتحديات التي تواجه المؤسسات المالية في هذا السياق، يمكن أن تكون هذه الدراسة بمثابة نقطة انطلاق لأبحاث جديدة تركز على استراتيجيات مبتكرة لتحسين الأمن السيبراني. وبهذا الشكل، تساهم الدراسة في بناء بيئة بحثية تعزز من تبادل المعرفة والخبرات بين الأكاديميين والممارسين (Safitra، 2023).

### 2.2.1 الأهمية العملية

- تتجاوز أهمية هذه الدراسة الحدود الأكاديمية لتصل إلى تطبيقات عملية لها تأثير مباشر على المؤسسات المالية. من خلال تحليل العلاقة بين الابتكار التكنولوجي وإدارة المخاطر، تقدم الدراسة استراتيجيات وأدوات فعالة يمكن للمؤسسات الاعتماد عليها لتحسين أدائها في مواجهة التهديدات السيبرانية. على سبيل المثال، تقدم الدراسة رؤى حول كيفية استخدام تقنيات مثل الذكاء الاصطناعي وتحليل البيانات لتحسين رصد التهديدات، مما يساعد المؤسسات على اتخاذ قرارات مستندة إلى بيانات موثوقة وسريعة.
- كما تساهم الدراسة في تعزيز الوعي الثقافي والتنظيمي بأهمية الأمن السيبراني داخل المؤسسات المالية. يعد إنشاء ثقافة تنظيمية تدعم التعاون والتواصل بين الفرق المختلفة أمراً ضرورياً لتطوير

استراتيجيات فعالة في مجال الأمن السيبراني. من خلال نشر المعرفة حول المخاطر السيبرانية وأساليب الحماية، يمكن للموظفين أن يصبحوا أكثر إدراكًا لتبعات أفعالهم، مما يسهم في تقليل المخاطر الناتجة عن الخطأ البشري.

- تلعب الدراسة دورًا مهمًا في توجيه استثمارات المؤسسات نحو التقنيات التي تعزز من كفاءة إدارة المخاطر. يتطلب تحسين الأمن السيبراني استثمارًا في الأدوات والتقنيات الجديدة، لذا توفر الدراسة توصيات مستندة إلى بيانات تحليلية حول المجالات الأكثر تأثيرًا في تحسين إدارة المخاطر. من خلال ذلك، يمكن للمؤسسات أن تعظم من فوائد استثماراتها وتحقق عوائد ملموسة على هذه الاستثمارات.
- تساهم الدراسة في تعزيز الثقة بين المؤسسات المالية وعملائها. فعندما تكون المؤسسات قادرة على حماية بيانات عملائها من التهديدات بشكل فعال، فإن ذلك يعزز من سمعتها ويزيد من ولاء العملاء. في عالم يتزايد فيه الوعي حول أهمية الأمن السيبراني، تعتبر القدرة على حماية المعلومات الحساسة ميزة تنافسية حيوية.

- تساهم هذه الدراسة في دعم الاستدامة المؤسسية من خلال تقديم استراتيجيات مبتكرة تساهم في تقليل المخاطر. إذ إن المؤسسات التي تستطيع التكيف مع التغيرات التكنولوجية والتهديدات السيبرانية ستكون أكثر قدرة على البقاء في سوق يتسم بالتنافسية العالية. من خلال تعزيز الأمن السيبراني، تستطيع المؤسسات ضمان استدامتها وتحقيق نجاح طويل الأمد (Kyambade، 2024).

### 3.1 أهداف الدراسة:

**الهدف الرئيسي للدراسة:** تحليل تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية.

#### الأهداف الفرعية

1. تحديد أنواع الابتكارات التكنولوجية المستخدمة في المؤسسات المالية:

يسعى هذا الهدف إلى دراسة الأنواع المختلفة من الابتكارات التكنولوجية التي تعتمد عليها المؤسسات المالية السعودية، مثل تقنيات الذكاء الاصطناعي، تحليلات البيانات الكبيرة، تكنولوجيا البلوكتشين، والحلول السحابية. من خلال هذا التحليل، يمكن للباحثين فهم كيف تقوم هذه المؤسسات بتطبيق الابتكارات لتحسين أنظمة إدارة المخاطر السيبرانية. سيتم تقييم فعالية كل نوع من هذه التقنيات في تعزيز الأمان السيبراني، مما يوفر رؤية شاملة حول الاستراتيجيات الأكثر نجاحًا في مجال الابتكار التكنولوجي.

## 2. تقييم التحديات التي تواجه المؤسسات المالية في تطبيق الابتكار التكنولوجي:

يهدف هذا الهدف إلى استكشاف العقبات والصعوبات التي تواجه المؤسسات المالية عند اعتماد الابتكارات التكنولوجية. تشمل هذه التحديات الجوانب التقنية، مثل نقص المهارات الفنية، بالإضافة إلى العوائق التنظيمية والثقافية، مثل مقاومة التغيير. من خلال فهم هذه التحديات، يمكن تقديم توصيات عملية للمؤسسات المالية حول كيفية التغلب عليها، مما يعزز من قدرتها على تحسين إدارة المخاطر السيبرانية باستخدام الابتكارات التكنولوجية.

## 3. تحليل فعالية الابتكار التكنولوجي في تحسين استراتيجيات إدارة المخاطر:

يسعى هذا الهدف إلى فحص كيفية تأثير الابتكار التكنولوجي على فعالية استراتيجيات إدارة المخاطر السيبرانية. من خلال دراسة العلاقة بين الابتكار ونجاح الاستراتيجيات المستخدمة، سيتمكن البحث من توضيح كيفية تعزيز الابتكار لعمليات الحماية والتجارب مع التهديدات. سيتناول هذا الهدف أيضًا مدى أهمية التكيف السريع مع الابتكارات التكنولوجية في تحسين الأداء العام للمؤسسات المالية في مواجهة المخاطر السيبرانية.

## 4. استكشاف الفوائد المحتملة للاستثمار في الابتكار التكنولوجي:

يهدف هذا الهدف إلى تسليط الضوء على القيمة المضافة التي يمكن أن تحققها المؤسسات المالية من استثماراتها في الابتكار التكنولوجي. من خلال استعراض الفوائد المحتملة، مثل تحسين الأداء، وزيادة الثقة من قبل العملاء، وتقليل التكاليف المرتبطة بالاختراقات، يمكن تقديم أدلة قوية تدعم أهمية

الاستثمار في الابتكار. سيتم تحليل كيف يمكن لهذه الفوائد أن تسهم في تعزيز مكانة المؤسسات المالية في السوق وتعزيز استدامتها على المدى الطويل.

#### 5. تطوير آليات لقياس تأثير الابتكار التكنولوجي على إدارة المخاطر:

يسعى هذا الهدف إلى استكشاف الطرق والأساليب التي يمكن للمؤسسات المالية استخدامها لقياس تأثير الابتكار التكنولوجي على أدائها في إدارة المخاطر السيبرانية. سيتم تطوير مجموعة من مؤشرات الأداء الرئيسية (KPIs) والاستبيانات لقياس الفعالية والنمو في الأداء بعد اعتماد الابتكارات. من خلال هذه الآليات، يمكن للمؤسسات المالية مراقبة تقدمها وتحديد المناطق التي تحتاج إلى تحسين، مما يضمن تحقيق أقصى استفادة من الابتكارات التكنولوجية في سياق إدارة المخاطر.

### 4.1 تساؤلات الدراسة:

**السؤال الرئيسي للدراسة** كيف يؤثر الابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية؟

#### الأسئلة الفرعية

1. ما هي أنواع الابتكارات التكنولوجية التي تعتمد عليها المؤسسات المالية السعودية في تحسين إدارة المخاطر السيبرانية؟
2. ما هي التحديات التي تواجه المؤسسات المالية في تطبيق الابتكارات التكنولوجية لإدارة المخاطر السيبرانية؟
3. كيف تؤثر ممارسات الابتكار التكنولوجي على فعالية استراتيجيات إدارة المخاطر السيبرانية في المؤسسات المالية؟
4. ما هي الفوائد المحتملة التي تحققها المؤسسات المالية من خلال الاستثمار في الابتكار التكنولوجي في سياق إدارة المخاطر السيبرانية؟

5. كيف يمكن للمؤسسات المالية السعودية قياس تأثير الابتكار التكنولوجي على أدائها في إدارة المخاطر السيبرانية؟

## 5.1 فرضيات الدراسة:

### الفرضية الرئيسية للدراسة

- يوجد تأثير إيجابي للابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية.

### الفرضيات الفرعية

1. تسهم تقنيات الذكاء الاصطناعي في تحسين إدارة المخاطر السيبرانية في المؤسسات المالية السعودية.
2. تؤدي ممارسات تحليل البيانات الكبيرة إلى تحسين فعالية استراتيجيات إدارة المخاطر السيبرانية.
3. تساهم تكنولوجيا البلوكتشين في تعزيز أمان المعاملات المالية وبالتالي تحسين إدارة المخاطر السيبرانية.
4. تؤثر الابتكارات في نظم الأمن السيبراني (مثل الجدران النارية المتطورة وأنظمة الكشف عن التسلل) بشكل إيجابي على القدرة على التعامل مع المخاطر السيبرانية.
5. تؤثر العوامل الثقافية والتنظيمية داخل المؤسسات المالية على مدى فعالية الابتكار التكنولوجي في إدارة المخاطر السيبرانية.

## 6.1 الدراسات السابقة:

إن أمن المعلومات يشكل مصدر قلق كبير لمستخدمي الكمبيوتر، وهو ليس مجرد مشكلة تقنية، بل إنه مرتبط أيضاً بالعوامل البشرية. ومن القضايا الرئيسية في المملكة العربية السعودية المتعلقة بالخدمات المصرفية عبر الإنترنت ضعف الأمان في تطبيقات الخدمات المصرفية عبر الإنترنت. لذلك ستبحث هذه الدراسة بشكل أعمق في الحل لتعزيز قضايا الأمن في تنفيذ الخدمات المصرفية عبر الإنترنت.

في عالم اليوم عالي السرعة، تحدث ملايين المعاملات كل دقيقة. ولهذه المعاملات، يجب أن تكون البيانات متاحة بسهولة للأشخاص الحقيقيين الذين يريدون الوصول إليها، ويجب الاحتفاظ بها بأمان من المحتالين. يتم قياس أمن المعلومات من خلال درجة تطبيق معايير ISO 27001 و PCI-DSS على البنوك السعودية، بينما يتم قياس أداء البنوك من خلال مؤشرات الربحية وجودة الأصول. تهدف هذه الورقة إلى تحديد وتقييم إدارة أمن المعلومات للبنوك الإلكترونية في المملكة العربية السعودية بشكل شامل مع محاولة سد الفجوة في الأدبيات (Elamin، 2016).

تتميز التكنولوجيا المالية بتقاطعها بين التمويل والتكنولوجيا، وقد غيرت المشهد المالي على مستوى العالم، وأعدت تشكيل نماذج الخدمات المصرفية التقليدية مع استمرار ابتكاراتها في الظهور. تسعى الدراسة الحالية إلى تقديم فحص شامل لتأثير التكنولوجيا المالية على الأداء المالي للبنوك السعودية. وقد تم التحقيق في تسعة بنوك وطنية سعودية. وقد تم جمع البيانات من التقارير السنوية من عام 2017 إلى عام 2022. وقد اتبعت الدراسة الانحدار المتعدد لاختبار العلاقة بين العوامل. ووجدت الدراسة أنه لم يكن هناك تأثير ملحوظ لأدوات التكنولوجيا المالية، مثل الرسائل المصرفية، والخدمات المصرفية عبر الإنترنت، وتطبيقات الهاتف المحمول، والتحويلات الرقمية، على العائد على الأصول (ROA) والعائد على الأسهم (ROE) عند النظر في كل أداة على حدة. ومع ذلك، عند النظر في كل هذه الأدوات مجتمعة، هناك تأثير كبير بنسبة 93.2٪ على العائد على الأصول، و 84.2٪ على العائد على حقوق الملكية (Alqahtani، 2024).

ارتفع المعدل السنوي لانتهاكات الأمن السيبراني في السنوات القليلة الماضية، مما أدى إلى كشف ملايين السجلات في بعض الحالات. بلغ متوسط تكلفة خرق البيانات في عام 2021 مبلغًا هائلًا قدره 4.24 مليون دولار. تدرس هذه الدراسة وعي العملاء ورضاهم عن الأمن السيبراني في سياق التحول الرقمي للخدمات المصرفية في المملكة العربية السعودية. الدراسة تجريبية وتستند إلى البيانات التي تم جمعها من 355 عميلًا مصرفيًا في المملكة العربية السعودية. تم تحليل ثلاثة جوانب مهمة للأمن السيبراني، بما في ذلك الهجمات الإلكترونية والتصيد الاحتيالي والقرصنة، من خلال أبعاد مختلفة. كما تمت دراسة رضا العملاء عن مساعدة الأمن السيبراني في البنوك وتوقعاتهم من الدعم الفني والخدمات المتعلقة بالأمن السيبراني. يتم استخدام تحليل التباين وتحليل الانحدار ثنائي المتغيرات لدراسة تأثير الهجوم الإلكتروني والتصيد

الاحتيالي والقرصنة ومساعدة الأمن السيبراني والتوقعات على الوعي الفني للأمن السيبراني على رضا العملاء. تظهر النتائج أن التحول الرقمي عزز القطاع المصرفي، ويستفيد المستخدمون من الخدمات عبر الإنترنت. ومع ذلك، فإن زيادة مستوى وعي العملاء بشأن أنشطة الهجمات الإلكترونية والتصيد والقرصنة من شأنها أن تؤثر على رضا العملاء عن المعاملات الرقمية. وكشفت النتائج أيضاً أن العملاء يحتاجون إلى مزيد من الرضا فيما يتعلق بجوانب مستوى الأمان من جانب البنك، ويجب على البنوك توفير برامج تدريبية منتظمة لحماية العملاء من الهجمات الإلكترونية. وإذا أعدت البنوك إدارة أكثر أماناً للأمن السيبراني، فيمكن تحقيق أهداف الاستدامة طويلة الأجل بسهولة (Johri، 2023).

توصي لجنة بازل البنوك بالحفاظ على احتياطي رأس مال لمواجهة التعرض للمخاطر التشغيلية بناءً على أحجام الأعمال، على افتراض أن الإجراءات العدوانية لتحقيق نمو أسرع للأعمال قد تزيد من التعرض للمخاطر. ونحن نزعم أن الابتكارات التكنولوجية تعرض البنوك لمزيد من المخاطر التشغيلية لأن التكنولوجيا تساعد في زيادة حجم الأعمال، ولكن فشل النظام، والمشاكل المتعلقة بالعمليات الداخلية، والاضطرابات الناجمة عن التهديدات الأمنية الخارجية والداخلية متأصلة في التكنولوجيا. واستناداً إلى 10 سنوات من البيانات الخاصة بـ 264 بنكاً من 43 دولة، نجد أن العمليات المصرفية الرقمية هي محرك أساسي للمخاطر التشغيلية التي تأتي مع زيادة حجم الأعمال. تتخذ البنوك بشكل استباقي المزيد من المخاطر التشغيلية من خلال زيادة الإنفاق السيبراني لمعالجة المنافسة في مجال التكنولوجيا المالية في الاقتصاد الرقمي. قد تكون الرقمنة مهمة بشكل عام للتعرض للمخاطر التشغيلية، لكن التجربة الطبيعية لا تجد أن تهديدات الأمن السيبراني في حد ذاتها يمكن أن تزيد من المخاطر التشغيلية على الرغم من أن الأمن السيبراني يبدو أنه يشكل تهديداً خطيراً للخدمات المصرفية الرقمية. تفتح الدراسة طرقاً جديدة للبحث في المستقبل (Uddin، 2023).

تُحدث ابتكارات التكنولوجيا المالية تحولات في مجال الخدمات المصرفية على مستوى العالم. ويفرض تبنيها فرصاً ومخاطر جديدة على البنوك الإسلامية ذات المتطلبات الفريدة. وتبحث هذه الدراسة في آثار التكنولوجيا المالية على فعالية إدارة المخاطر في البنوك الإسلامية في دولة الإمارات العربية المتحدة. ويتضمن النموذج المفاهيمي عوامل مثل تبني التكنولوجيا المالية والقدرات الناشئة والنضج الرقمي وأمن

تكنولوجيا المعلومات التي تؤثر على النتائج. وقد تم جمع البيانات الأولية من خلال مسح أجري في تسعة بنوك إسلامية في دولة الإمارات العربية المتحدة وتم تحليلها باستخدام PLS-SEM. وتُظهر النتائج أن تبني التكنولوجيا المالية وقدراتها أثرت بشكل إيجابي على الفعالية، في حين لم يكن التحول الرقمي وحده هو الذي فعل ذلك. وتُظهر النتائج أيضاً أن البيئة التنظيمية لم تخفف من حدة العلاقات كما افترض البعض. وتوفر النتائج أدلة تجريبية على تحسين إدارة المخاطر من خلال تمكين التكنولوجيا المالية المسؤولة ومواءمة الإشراف في سياق دولة الإمارات العربية المتحدة (Hammadi، 2024).

لقد أدى الابتكار والتكنولوجيا إلى تحويل كل من العلاقات التجارية بين الشركات الصغيرة والشركات التجارية الداخلية. أصبح إعادة تنظيم وظائف التصميم والإنتاج والتسويق والتسليم والخدمة ممكناً من خلال سلاسل التوريد الموزعة والابتكار المستقل والتصنيع المستعان بمصادر خارجية والتخزين التعاقد والتسليم. هناك أزماتان ماليتان عالميتان رئيسيتان شهدناهما في العقود الماضية. أثرت الأزمة المالية على الاقتصاد العالمي الفعلي في عام 2008. وبالمقارنة، جاءت أزماتان أخريان مؤخراً أثناء مشكلة جائحة كوفيد-19. تستند هذه الدراسة إلى استراتيجية البلدان لتعزيز التحول المالي الرقمي في إدارة الأزمات: التحديات والفرص. الغرض من هذا البحث هو التحقيق في العلاقة بين تبني العملات الإلكترونية وتبادلها واستقرارها في الاقتصاد، وخاصة بالنظر إلى الأزمات المالية العالمية الأخيرة، فضلاً عن تأثيرات تقنيات التمويل الإلكتروني المبتكرة مثل تقنية blockchain والذكاء الاصطناعي. والبيانات الضخمة، من ناحية، على كفاءة وشمول القطاع المصرفي في البلدان النامية، وكيف يساعد في دعم التحول المالي الرقمي، من ناحية أخرى (Dafri، 2023).

FinTech هو المصطلح المستخدم للإشارة إلى حلول الفضاء المالي والتكنولوجي. وعادة ما يشير إلى الابتكارات الجديدة التي تدير أو تتصل بالخدمات المالية عبر الإنترنت، أو الأجهزة الذكية، أو تطبيقات البرامج أو الخدمات السحابية وتشمل أي شيء من الخدمات المصرفية عبر الهاتف المحمول إلى تطبيقات العملات المشفرة. وعلى الرغم من مزايا FinTech، فقد اغتنم مجرمو الإنترنت الفرصة لاستغلال نقاط الضعف في أنظمة FinTech. أصبحت هجمات التصيد الاحتيالي وبرامج الفدية واختراقات البيانات أكثر انتشاراً، وتستهدف الأفراد ومؤسسات FinTech. وقد تأثرت البحرين، التي لا تختلف عن بقية العالم، بمثل

هذه التهديدات الإلكترونية. وبالتالي، كان على شركات FinTech تعزيز تدابيرها وبروتوكولاتها لمكافحة هذه التهديدات. تركز التدابير المضادة الموجودة في الأدبيات بشكل أساسي على ممارسات وأطر الأمن السيبراني العامة، مع إيلاء اهتمام محدود للاحتياجات المحددة لصناعة FinTech. وبالتالي، هناك فجوة ملحوظة في الأدبيات فيما يتعلق بإطار عمل الأمن السيبراني المركز الذي يلبي المتطلبات الفريدة لابتكارات FinTech، وخاصة في البحرين. ولسد هذه الفجوة، يتناول هذا البحث المشكلة من خلال إجراء مراجعة شاملة لتحديات الأمن السيبراني الحالية والممارسات الشائعة ومعايير الأمن السيبراني ومن خلال مقابلات بحثية متعمقة مع المديرين التنفيذيين والخبراء وأصحاب المصلحة الآخرين في مجال التكنولوجيا المالية. وباستغلال هذه المعرفة، اقترح هذا البحث إطارًا قابلاً للتكيف يعالج المخاطر والثغرات التي تواجهها ابتكارات التكنولوجيا المالية في البحرين. من خلال المناقشات الجماعية وجلسات دلفي، قام خبراء الصناعة بتقييم الجدوى العملية للإطار والقدرة على معالجة المخاطر المحددة والتوافق مع المشهد التنظيمي الحالي للتكنولوجيا المالية. وتوضح النتائج قبولاً كبيراً للإطار المطور وتسلسل الضوء على إمكانات الإطار لتعزيز مرونة الأمن السيبراني بشكل كبير. وعلاوة على ذلك، يعترف الخبراء بالإطار المقترح باعتباره أساساً أساسياً في تأمين النظام البيئي للتكنولوجيا المالية في البحرين. تكمن أهمية هذا البحث في قدرته على تعزيز وضع الأمن السيبراني لصناعة التكنولوجيا المالية في البحرين، والتخفيف من المخاطر والثغرات المرتبطة بالتهديدات السيبرانية في هذا القطاع الحيوي (AlBenJasim, 2024).

سعت الدراسة إلى استكشاف تأثير التكنولوجيا المالية (Fintech) على الأداء المالي لمؤسسات التمويل الأصغر في البحرين. الهدف الأساسي من هذه الدراسة هو التحقيق في تأثير تبني التكنولوجيا المالية (Fintech) على الأداء المالي لمؤسسات التمويل الأصغر في البحرين. على وجه التحديد، يهدف البحث إلى تقييم مدى تأثير حلول التكنولوجيا المالية، مثل الإقراض الرقمي والخدمات المصرفية عبر الهاتف المحمول، على المؤشرات المالية الرئيسية، مثل الربحية والكفاءة التشغيلية، داخل قطاع التمويل الأصغر في البحرين. كانت الدراسة قائمة على الأدبيات. جمعت الدراسة وحللت الأبحاث والمنشورات الموجودة لاستنتاجات. أدى إدخال التكنولوجيا المالية (Fintech) في مؤسسات التمويل الأصغر في البحرين إلى تعزيز الكفاءة التشغيلية بشكل كبير، وخفض التكاليف وتسريع معالجة القروض. أدت أتمتة الخدمات المالية

ورقميتها إلى انخفاض النفقات العامة، مما أدى إلى تحسين الأداء المالي لمؤسسات التمويل الأصغر. عزز تبني التكنولوجيا المالية استراتيجيات التخفيف من المخاطر داخل مؤسسات التمويل الأصغر، مع تمكين نماذج تقييم المخاطر المتقدمة من اتخاذ قرارات إقراض أكثر دقة. ونتيجة لذلك، انخفضت معدلات التخلف عن السداد ونسب القروض المتعثرة، مما ساهم في الاستقرار المالي لهذه المؤسسات. وتؤكد النتائج أيضًا على التأثير الإيجابي للتكنولوجيا المالية على رضا العملاء وثقتهم، حيث توفر الخدمات المتاحة على مدار الساعة طوال أيام الأسبوع، والتطبيقات المحمولة، والخدمات المصرفية عبر الإنترنت تجربة أكثر ملاءمة وسهولة في الوصول. تعد العلاقات القوية مع العملاء محورية لجذب العملاء والاحتفاظ بهم، مما يعود بالنفع في نهاية المطاف على الأداء المالي الطويل الأجل لمؤسسات التمويل الأصغر. في الختام، كان تأثير التكنولوجيا المالية على الأداء المالي لمؤسسات التمويل الأصغر في البحرين إيجابيًا بشكل كبير. فقد سهلت التكنولوجيا المالية تحسين الكفاءة التشغيلية، وتخفيف المخاطر، ورضا العملاء، وكل ذلك ساهم بشكل مباشر في تعزيز الاستقرار المالي وربحية هذه المؤسسات. وللحفاظ على هذه المكاسب وتعظيمها، يجب على مؤسسات التمويل الأصغر الاستمرار في تبني ابتكارات التكنولوجيا المالية، وإعطاء الأولوية للامتثال التنظيمي، والاستثمار في الأمن السيبراني، وضمان بقائها في وضع جيد لخدمة عملائها والتكيف مع المشهد المالي المتطور باستمرار في البحرين. أوصت الدراسة بأنه ينبغي لمؤسسات التمويل الأصغر في البحرين أن تفكر في تنوع عروضها في مجال التكنولوجيا المالية لتلبية مجموعة أوسع من احتياجات العملاء، والتوسع إلى ما هو أبعد من القروض الصغيرة التقليدية إلى خدمات مثل المدفوعات الرقمية والادخار والتأمين، والتي يمكن أن تزيد من تدفقات الإيرادات وتحسن الأداء المالي. وينبغي لمؤسسات التمويل الأصغر أن تشارك بنشاط في الشراكات والتعاون داخل منظومة التكنولوجيا المالية، بما في ذلك الشركات الناشئة في مجال التكنولوجيا المالية، وشركات التكنولوجيا، والهيئات التنظيمية، للبقاء في طليعة التطورات التكنولوجية والامتثال التنظيمي، وتمكينها من الاستفادة من التكنولوجيا المالية إلى أقصى إمكاناتها لتحقيق النجاح المالي على المدى الطويل (Chuc، 2023).

لقد مكّن التقدم التكنولوجي من نقل العديد من الخدمات التقليدية إلى بيئة إلكترونية، مما أدى، من بين أمور أخرى، إلى زيادة عدد قنوات الاتصال بين المؤسسات المالية والأفراد. والنتيجة هي أن الأفراد

والكيانات مضطرون إلى مشاركة أي نوع من البيانات الشخصية تقريبًا. وفي حين تتزايد تكنولوجيا مشاركة البيانات والطلب على بيانات القطاعين العام والخاص، فإن التشريعات المتعلقة بحماية هذه البيانات لم تتمكن من النمو بنفس السرعة والنطاق. وفي حالة المملكة العربية السعودية، هناك عنصر من حماية البيانات بموجب مبادئ الشريعة الإسلامية بشكل عام، وهناك بعض اللوائح التي تعاقب على انتهاكات البيانات المحددة وفقًا للتنظيم ذي الصلة. وعلى الرغم من أن قانون حماية البيانات الشخصية الجديد قيد المراجعة من قبل مجلس الشورى، إلا أنه لم يتم قبوله بعد. وفي الوقت نفسه، في الاتحاد الأوروبي، تم اعتماد اللائحة العامة لحماية البيانات 1 (GDPR) كقانون سيغطي الاتحاد الأوروبي بأكمله ومواطنيه وشركاته في جميع أنحاء العالم. وفي حين يحمي هذا الإطار الجديد البيانات الشخصية، فإنه يفرض معايير وعقوبات معينة على جميع الأفراد والمؤسسات التي تعالج هذه البيانات. تحاول هذه الورقة تقديم تقييم للمخاطر التي يفرضها قانون حماية البيانات العامة (GDPR) على المملكة العربية السعودية ومتطلبات وجود لائحة مفصلة لحماية البيانات تتوافق مع الشريعة الإسلامية بشكل أساسي بسبب مبدأ "المصلحة" ورؤية 2030 (Polat، 2021).

## 7.1 المنطلقات النظرية للدراسة:

تستند هذه الدراسة إلى مجموعة من المنطلقات النظرية التي تشكل الإطار الفكري لفهم العلاقة بين الابتكار التكنولوجي وإدارة المخاطر السيبرانية في المؤسسات المالية السعودية. تتضمن هذه المنطلقات عددًا من النظريات التي تساهم في تفسير كيفية تأثير الابتكارات التكنولوجية على أداء المؤسسات في مجال الأمن السيبراني، وتركز على استكشاف الجوانب المختلفة لهذه العلاقة.

### 1. نظرية الابتكار التكنولوجي

تعتبر نظرية الابتكار التكنولوجي أحد المنطلقات الأساسية في هذه الدراسة، حيث تركز على كيفية تطوير وتنفيذ التقنيات الجديدة وتأثيرها على الأداء المؤسسي. وفقًا لهذه النظرية، يمثل الابتكار التكنولوجي محركًا رئيسيًا للنمو والتغيير في المؤسسات، حيث يمكن أن يساهم في تحسين الكفاءة وتعزيز القدرة

التنافسية. تفسر هذه النظرية كيف يمكن للمؤسسات المالية استخدام الابتكارات التكنولوجية لتحديث أنظمتها وعملياتها، مما يساعدها في مواجهة التهديدات السيبرانية بشكل أكثر فعالية. من خلال هذه النظرية، تعزز الدراسة أهمية الابتكار كأداة استراتيجية لتطوير حلول جديدة لمشكلات الأمن السيبراني (Wei، 2023).

## 2. نظرية إدارة المخاطر

تعتبر نظرية إدارة المخاطر إطارًا مهمًا لفهم كيفية التعامل مع التهديدات التي تواجه المؤسسات. تركز هذه النظرية على تحديد المخاطر، تقييمها، وتطوير استراتيجيات للحد منها. في سياق هذه الدراسة، يتم تطبيق هذه النظرية لفهم كيف يمكن للابتكارات التكنولوجية أن تسهم في تحسين استراتيجيات إدارة المخاطر السيبرانية. تقدم النظرية أدوات وتقنيات تساعد المؤسسات على التعرف على المخاطر المحتملة وتحليلها، مما يمكنها من اتخاذ قرارات مدروسة حول كيفية حماية بياناتها وأصولها (Kindness، 2023).

## 3. نظرية النظام المعقد

تتناول هذه النظرية كيفية تفاعل العناصر المختلفة داخل نظام معين، مما يساهم في فهم البيئة الديناميكية التي تعمل فيها المؤسسات المالية. في إطار هذه الدراسة، تعكس نظرية النظام المعقد كيف يمكن للابتكار التكنولوجي أن يتفاعل مع مكونات النظام الأمني السيبراني. إذ تشدد هذه النظرية على أن التغييرات في عنصر واحد من النظام، مثل إدخال تقنية جديدة، يمكن أن تؤثر على باقي العناصر. من خلال تحليل العلاقات بين الابتكارات التكنولوجية واستراتيجيات إدارة المخاطر، يمكن تحديد كيفية تحسين الأداء الكلي للنظام الأمني (Turner، 2019).

## 4. نظرية التغيير التنظيمي

تتناول هذه النظرية كيفية إدارة المؤسسات للتغيرات الداخلية والخارجية، خاصة في ظل الظروف المتغيرة في السوق. تلعب هذه النظرية دورًا رئيسيًا في فهم كيف يمكن للمؤسسات المالية التكيف مع الابتكارات التكنولوجية الجديدة. تعتمد هذه الدراسة على هذه النظرية لاستكشاف كيفية تأثير الثقافة

التنظيمية والهيكل الإداري على نجاح تطبيق الابتكارات التكنولوجية. من خلال تحليل مدى استعداد المؤسسات لتقبل التغيير واحتضان الابتكار، يمكن تحديد العوامل التي تؤثر على فعالية إدارة المخاطر السيبرانية (Parastuty، 2015).

## 5. نظرية القيمة المضافة

تركز هذه النظرية على كيفية زيادة القيمة الناتجة عن العمليات والممارسات المختلفة داخل المؤسسة. في سياق الدراسة، تساهم نظرية القيمة المضافة في تحليل الفوائد المحتملة التي يمكن أن تحققها المؤسسات من خلال اعتماد الابتكار التكنولوجي في إدارة المخاطر. تسلط هذه النظرية الضوء على أهمية تحقيق توازن بين التكاليف والفوائد الناتجة عن استثمار في تقنيات جديدة، مما يساعد المؤسسات على تحسين عوائدها وزيادة قدرتها على مواجهة التهديدات (Saffer، 2018).

تشكل هذه المنطلقات النظرية الإطار العام للدراسة، حيث تعزز من فهم العلاقة المعقدة بين الابتكار التكنولوجي وإدارة المخاطر السيبرانية في المؤسسات المالية السعودية. من خلال دمج هذه النظريات، تسعى الدراسة إلى تقديم رؤى عميقة تساهم في تطوير استراتيجيات فعالة لتحسين الأمان السيبراني، مما يساهم في تعزيز أداء المؤسسات واستدامتها في ظل التحديات المتزايدة.

## 8.1 المنهجية وطرق البحث:

تعتبر المنهجية الكمية من الأساليب البحثية الفعالة التي تستخدم في هذه الدراسة لتحليل تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية. تعتمد هذه المنهجية على جمع البيانات الكمية وتحليلها إحصائياً، مما يسمح بتقديم استنتاجات دقيقة تدعم النتائج التي تم التوصل إليها. وفيما يلي تفاصيل المنهجية وطرق البحث المتبعة:

### 1. تصميم الدراسة

تعتمد الدراسة على تصميم وصفي وتحليلي، حيث يهدف إلى فهم العلاقة بين الابتكار التكنولوجي وإدارة المخاطر السيبرانية. يتضمن التصميم الوصفي جمع البيانات عن الخصائص الحالية للمؤسسات

المالية والتكنولوجيا المستخدمة فيها، بينما يركز التحليل على تحديد العلاقة بين المتغيرات المدروسة. يتم استخدام استبيانات كأداة لجمع البيانات، مما يسمح بجمع معلومات دقيقة من عينة كبيرة من المشاركين.

## 2. مجتمع الدراسة

يتكون مجتمع الدراسة من المؤسسات المالية في المملكة العربية السعودية، بما في ذلك البنوك التجارية، شركات التأمين، ومؤسسات التمويل. تم اختيار هذه المؤسسات نظرًا لأهميتها الكبيرة في النظام المالي، ودورها البارز في استخدام التكنولوجيا الحديثة لإدارة المخاطر. يشمل المجتمع جميع المستويات التنظيمية، مما يسمح بالحصول على رؤى متنوعة حول الابتكارات التكنولوجية والتحديات المتعلقة بإدارة المخاطر السيبرانية.

## 3. عينة الدراسة

تم تحديد عينة الدراسة باستخدام طريقة العينة العشوائية، مما يساعد في تقليل التحيز وزيادة تمثيل العينة. سيتم اختيار عينة من الموظفين العاملين في المؤسسات المالية بمختلف المستويات الإدارية، بما في ذلك الإدارات التقنية، إدارة المخاطر، والإدارة العليا. يهدف هذا الاختيار إلى جمع آراء وتجارب متنوعة تعكس واقع الابتكار التكنولوجي في هذه المؤسسات. تم تحديد حجم العينة بناءً على قواعد العينة المناسبة للدراسات الكمية، بحيث تكون كافية لتحليل البيانات وتقديم نتائج موثوقة.

## 4. أدوات جمع البيانات

تستخدم الدراسة استبيانات كأداة رئيسية لجمع البيانات. تم تصميم الاستبيان ليشمل مجموعة من الأسئلة المغلقة والمفتوحة، بحيث تغطي جوانب متعددة تتعلق بالابتكار التكنولوجي وإدارة المخاطر السيبرانية. تشمل الأسئلة قياس مدى استخدام تقنيات معينة، تقييم فعالية استراتيجيات إدارة المخاطر، ورصد التحديات التي تواجه المؤسسات في هذا السياق. لضمان موثوقية الاستبيان، تم إعداد بناءً على مراجعة الأدبيات السابقة واستشارة خبراء في المجال.



## 5. تحليل البيانات

بعد جمع البيانات، سيتم استخدام الأساليب الإحصائية المناسبة لتحليل النتائج. تشمل هذه الأساليب التحليل الوصفي، مثل حساب المتوسطات والانحرافات المعيارية، بالإضافة إلى التحليل الاستنتاجي، مثل اختبار الفرضيات. ستستخدم تقنيات مثل تحليل الانحدار لفهم العلاقة بين الابتكار التكنولوجي وإدارة المخاطر، مما يمكن الباحثين من تحديد مدى تأثير الابتكار على فعالية استراتيجيات إدارة المخاطر السيبرانية. سيتم استخدام برنامج إحصائي مثل SPSS أو R لتحليل البيانات ومعالجة النتائج.

## 6. الضوابط الأخلاقية

تتضمن الدراسة احترام الضوابط الأخلاقية في البحث، حيث سيتم توضيح أهداف الدراسة للمشاركين والحصول على موافقتهم قبل جمع البيانات. سيتم أيضًا ضمان سرية المعلومات وعدم استخدامها لأغراض أخرى غير البحث. تعتبر هذه الخطوات ضرورية لبناء الثقة مع المشاركين وضمان شفافية العملية البحثية.

## 7. التحديات المحتملة

تتضمن المنهجية أيضًا الاعتراف بالتحديات المحتملة التي قد تواجهها الدراسة. من الممكن أن تشمل هذه التحديات مقاومة بعض المؤسسات لتقديم المعلومات، أو صعوبة الوصول إلى بعض فئات الموظفين. لتجاوز هذه التحديات، سيتم اتخاذ تدابير مثل التوضيح للجهات المعنية بفوائد المشاركة في الدراسة، وتقديم حوافز للمشاركة.

## 9.1 أدوات الدراسة:

تعتبر أدوات جمع البيانات جزءًا حيويًا من أي دراسة بحثية، حيث تساهم في توفير المعلومات الضرورية لفهم الظواهر المدروسة وتحليلها بشكل دقيق. في إطار الدراسة الحالية التي تتناول "تحليل تأثير

الابتكار التكنولوجي على إدارة المخاطر السيبرانية في المؤسسات المالية السعودية"، تم اختيار مجموعة من أدوات جمع البيانات بعناية لضمان تحقيق أهداف البحث بفعالية وموضوعية. تشمل هذه الأدوات الاستبيانات، المقابلات، والمراجعة الوثائقية، بالإضافة إلى الأدوات الإلكترونية.

#### - الاستبيانات

تعتبر الاستبيانات الأداة الأساسية لجمع البيانات في هذه الدراسة، حيث تم تصميمها بشكل منهجي لجمع معلومات شاملة من مجموعة متنوعة من المشاركين. يتكون الاستبيان من مجموعة من الأسئلة المغلقة التي تتيح للمشاركين اختيار إجابات محددة، مما يسهل جمع البيانات الكمية وتحليلها إحصائيًا. على سبيل المثال، تتناول الأسئلة المغلقة استخدام تقنيات مثل الذكاء الاصطناعي وأنظمة تحليل البيانات الكبيرة وكيفية تأثيرها على فعالية إدارة المخاطر.

#### - المقابلات

تعتبر المقابلات أيضًا أداة مهمة لجمع البيانات، حيث تتيح للباحثين الحصول على رؤى أعمق وتفصيلية حول الموضوع المدروس. يتم إجراء المقابلات مع مجموعة مختارة من الشخصيات الرئيسية في المؤسسات المالية، مثل المدراء التنفيذيين ومديري تكنولوجيا المعلومات، وذلك بهدف استكشاف آراءهم وتصوراتهم بشأن الابتكار التكنولوجي وإدارة المخاطر. تعتبر هذه المقابلات فرصة فريدة للحصول على معلومات غنية وغير متاحة في الاستبيانات، حيث يمكن للباحثين طرح أسئلة توضيحية بناءً على إجابات المشاركين، مما يسمح بعمق النقاش واستكشاف الأفكار الجديدة.

يمكن إجراء المقابلات بشكل فردي أو في مجموعات، مما يتيح تبادل الآراء والأفكار بين المشاركين. تعزز المقابلات الجماعية من فهم الديناميكيات الجماعية والتفاعلات بين أعضاء الفريق، مما يتيح رؤية شاملة حول كيفية تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية داخل المؤسسات.

## - المراجعة الوثائقية

تُعتبر المراجعة الوثائقية أداة بحثية مهمة لجمع البيانات، حيث يتم تحليل المستندات والتقارير ذات الصلة بالمؤسسات المالية وابتكاراتها التكنولوجية وإدارة المخاطر. تشمل هذه الوثائق مجموعة متنوعة من المصادر، مثل تقارير الأداء السنوية، والسياسات والإجراءات المعتمدة، والدراسات السابقة في هذا المجال. من خلال مراجعة هذه الوثائق، يمكن للباحثين الحصول على معلومات قيمة حول كيفية إدارة المؤسسات المالية للمخاطر السيبرانية وكيفية اعتماد الابتكارات التكنولوجية.

تساهم المراجعة الوثائقية في توفير السياق التاريخي والحالي لطواهر الابتكار وإدارة المخاطر، مما يعزز من فهم العلاقات والتفاعلات بين مختلف العوامل المؤثرة. كما تساعد هذه المراجعة في الكشف عن الثغرات البحثية التي يمكن أن تسعى هذه الدراسة لسدها.

## - الأدوات الإلكترونية

مع التطور التكنولوجي السريع، أصبح استخدام الأدوات الإلكترونية جزءاً لا يتجزأ من عملية جمع البيانات. يتم استخدام استبيانات إلكترونية مصممة بشكل جيد لجمع البيانات بطريقة فعالة وسريعة. هذه الاستبيانات تُرسل عبر البريد الإلكتروني أو من خلال منصات الاستطلاعات على الإنترنت، مما يسهل الوصول إلى عينة كبيرة من المشاركين ويزيد من سرعة جمع البيانات.

تتيح الأدوات الإلكترونية تحليل البيانات بشكل أكثر كفاءة، حيث يمكن استخدام برامج التحليل الإحصائي المتقدمة لتفسير النتائج واستكشاف الأنماط. تساهم هذه الأدوات في تحسين جودة البحث من خلال تمكين الباحثين من جمع وتحليل البيانات بطريقة موضوعية ودقيقة.

## 10.1 حدود الدراسة:

تعتبر حدود الدراسة جزءاً مهماً من تصميم البحث، حيث تحدد نطاق البحث وتوضح الإطار الذي سيتم فيه إجراء الدراسة. في دراسة "تحليل تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية في

المؤسسات المالية السعودية"، تم تحديد الحدود البشرية، الزمانية، والمكانية لتوفير رؤية واضحة حول نطاق الدراسة وأبعادها المختلفة.

#### - الحدود البشرية

تتعلق الحدود البشرية بالأفراد أو الفئات المستهدفة التي سيتم تضمينها في الدراسة. في هذه الدراسة، تركز العينة على الموظفين العاملين في المؤسسات المالية في المملكة العربية السعودية، بما في ذلك البنوك التجارية، وشركات التأمين، ومؤسسات التمويل. سيتم اختيار هؤلاء الموظفين من مستويات تنظيمية مختلفة، بدءاً من العاملين في أقسام تكنولوجيا المعلومات وإدارة المخاطر إلى المدراء التنفيذيين. تهدف هذه الحدود البشرية إلى ضمان تمثيل شامل لمختلف وجهات النظر والخبرات المتعلقة بالابتكار التكنولوجي وإدارة المخاطر السيبرانية. من خلال استهداف مجموعة متنوعة من المشاركين، يمكن للدراسة تقديم رؤى عميقة حول كيفية تأثير الابتكار التكنولوجي على استراتيجيات إدارة المخاطر في السياق المالي. كما سيتم اختيار المشاركين بناءً على معايير محددة، مثل سنوات الخبرة، والمجال الوظيفي، والموقع الجغرافي داخل المملكة، مما يعزز من موثوقية النتائج.

#### - الحدود الزمانية

تشير الحدود الزمانية إلى الفترة الزمنية التي تغطيها الدراسة، والتي تمتد من عام 2022 حتى عام 2024. تُعتبر هذه الفترة حاسمة نظراً للتطورات السريعة التي يشهدها الابتكار التكنولوجي في المجال المالي، وخاصةً في ظل التحولات الرقمية التي تشهدها المؤسسات المالية. تستند الدراسة إلى البيانات المجمعة خلال هذه الفترة الزمنية لتحليل تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية. من خلال التركيز على هذه السنوات، سيتمكن الباحثون من تقييم كيفية تأثير المؤسسات المالية مع التغيرات السريعة في البيئة التكنولوجية، وكيفية تأثير هذه التغيرات على استراتيجيات إدارة المخاطر. كما ستساعد هذه الحدود الزمنية في فهم التوجهات المستقبلية والاتجاهات التي قد تطرأ بعد عام 2024.

## - الحدود المكانية

تشير الحدود المكانية إلى المواقع الجغرافية التي تركز عليها الدراسة، والتي تقتصر على المؤسسات المالية في المملكة العربية السعودية. تعتبر المملكة واحدة من الأسواق المالية الأكثر تطورًا في المنطقة، حيث تشهد نموًا ملحوظًا في الابتكار التكنولوجي، مما يجعلها بيئة مثالية لدراسة تأثير هذه الابتكارات على إدارة المخاطر السيبرانية. تتضمن الحدود المكانية مجموعة متنوعة من المؤسسات المالية في مختلف المدن السعودية، مثل الرياض، جدة، والدمام، مما يضمن تنوع البيانات المجمعة. تساهم هذه الحدود في تقديم صورة شاملة عن كيفية تأثير الابتكار التكنولوجي على إدارة المخاطر السيبرانية عبر مختلف المناطق الجغرافية في المملكة. كما تعكس هذه الحدود تأثير العوامل المحلية على استراتيجيات المؤسسات في التعامل مع التهديدات السيبرانية، مما يعزز من فهم السياق الذي تعمل فيه المؤسسات المالية.

## الفصل الثاني: الإطار النظري

### المبحث الأول: الابتكار التكنولوجي

#### المقدمة

يعد الابتكار والتطوير التكنولوجي في وقتنا الحالي قضية ضرورية وأساسية داخل المنظمات اليوم، خاصة في ظل التطور التكنولوجي الحاصل، حيث أن المقدرة على الابتكار أصبحت المعيار الرئيسي للمنافسة في الدول المتقدمة، لأن المقدرة العالية على الابتكار تعد من أهم المؤشرات على صحة الاقتصاد وقدرته على المواجهة في ظل المنافسة. (عبد المجيد، 2024)

عرفت الابتكارات في الدول المتطورة، لكنها غدت موضوعاً مهماً في ظل التطور التكنولوجي للدول المتنامية، وبالتالي فإن منظمات اليوم تعيش حقبة الإستراتيجيات التي تبذل فيها أقصى ما بوسعها من طاقات التفكير والعمل من أجل التنسيق بين المتطلبات الخاصة بالعملية بين رفع جودة الأداء في ظل التطورات الحديثة وعلى جميع المستويات الإدارية والإستراتيجيات للتطوير والابتكار، وتمثل التكنولوجيا المعلوماتية انطلاقة واسعة من المكونات والعناصر المتنوعة في تخزين البيانات ومعالجتها و استرجاعها و توزيعها، إضافة إلى الدور الذي تلعبه في خلق المعرفة المطلوبة التي هي نتاج امتزاج الأنظمة المحاسبية وشبكات الاتصالات والمعرفة التكنولوجية، تتلخص أهم سمات تكنولوجيا المعلومات في تقريب المسافات اختصار الوقت، وتقسيم المهام الفكرية مع الآلات وتزايد الأنظمة الشبكية وتطور البيئة الإلكترونية فكرياً. (بيان، 2024)

أما فيما يتعلق بالبنوك الأردنية، فهي تواجه تقلبات جذرية لمواجهة المتغيرات الكبيرة التي يعيشها الاقتصاد الأردني، وقد باتت مشكلة تطوير النظام البنكي الأردني ومواكبته للمستقبل من أكبر الاهتمامات في كافة المستويات الإدارية. (دقيش، 2023)

## 1.1.2 التمييز بين المصطلحات

تعددت المفاهيم المستعملة للتعبير عن "إنتاج منتجات جديدة أو خدمات جديدة، حيث نجد المصطلحات التالية الإبداع، والابتكار، والاختراع والتجديد نظراً لكثرة الترجمات وعدم توحيدها من طرف مجمع اللغة العربية في مختلف الدول العربية، اختلفت الآراء حول الكلمات المترادفة التي تعطي المعنى الدقيق لهذه المصطلحات. (ملاوي، 2024)

## 2.1.2 الفرق بين الإبداع والابتكار

أورد أغلب الباحثين تعريفات مختلفة تميز بين الإبداع والابتكار، وفيما يلي أهم هذه الآراء:

الإبداع هو عملية تتبع الابتكار، ومنها يجب عدم الخلط بينهما، لأن الإبداع هو بداية الابتكار، كما أن الابتكار بعد عملاً فردياً بينما يعد الإبداع عملاً جماعياً يستلزم التعاون بين أفراد المجموعة. ويرى أن الابتكار يخلق الجديد الذي لم يكن موجوداً من قبل، في حين أن الإبداع يعمل على تحويل هذه الأشياء لتصبح شيئاً ملموساً كالسلع والخدمات. كما أورد أن مفهوم الابتكار يدل على العمل لإيجاد شيء جديد، ويمكن اعتباره إيجاد مورد حديث للمنظمة، بينما يرى أن الإبداع هو التكامل بين المواد المستحدثة والتسويق الجيد لها. (شهوان، 2024)

وأشار إلى تكاملية العلاقة بين الإبداع والابتكار كما هي مبينة في الشكل أدناه، حيث أن مدخلات المنظمة المبدعة تتضمن الأفكار والعاملون والتمويل، وتخلق أفكار جديدة مشتملة النمو والإبداع وذلك عن طريق التحسين المستمر في العملية الإنتاجية وتحقيق الكسب المادي. (بن علي، 2022)

وعليه فإن الحداثة هي من سمات وصفات الابتكار وهي أفكار متصلة بإيجاد حل للمشكلات وإعادة تجميع الأنماط المعرفية في نماذج ومخرجات مميزة أو يتجلى في الوصول إلى حلول خلاقة لمشكلة جديدة أو فكرة ما، أما فيما يخص الإبداع، فإنه ذو صلة بجعل هذه الفكرة المستحدثة محل التنفيذ على شكل عملية أو سلعة أو خدمة يتم تقديمها من قبل المنظمة للزبائن والمتعاملين معا

يلجأ بعض الكتاب إلى استخدام لفظي الابتكار والإبداع كمترادفين للإشارة والدلالة على معنى واحد، لكن هناك تمايز بين المفهومين لإزالة اللبس والغموض بينهما لا بد من توضيح الفرق بين الإبداع والابتكار. (عبد المجيد، 2024)

أوضحت إن كلمة ابتكار تم اشتقاقها من الكلمة اللاتينية Innovates والتي تعني تغيير أو تبديل، وهناك ترجمتين مختلفتين لهذا المعنى:

- التغيير وتعديل ما هو موجود أصلاً. (Machos، 2021)
  - التبديل وهي اختراع شيء جديد وتقديمه للوجود سواء أكانت فكرة أو منتج أو خدمة. (قداري، 2021)
- قد لا يشير الابتكار دائماً إلى استخدام أحدث التكنولوجيا المتقدمة، على العكس تماماً، بل هو أقل من أن يكون مسألة متطورة تقنياً بل هو أسلوب في التفكير وخلق حلول مبتكرة داخل المنظمة. (بيان، 2024)

يمكننا في هذا المضمون اعتبار تقنيات إدارة الابتكار على أنها مجموعة من الأدوات والمنهجيات المساعدة للمنظمات من أجل التكيف مع الوضع الراهن ومواجهة التحديات الموجودة في السوق بطريقة أكثر منهجية وأكثر تنظيم. (بن علي، 2022)

ويمكننا تعريف الابتكار بأنه القدرة الفعلية للمنظمة للتوصل إلى كل جديد يمكن أن يضيف قيمة أكبر وأكثر تميزاً من تلك التي يقدمها المنافسون في السوق بحث تكون المنظمة السبابة في مجال الابتكار عند مقارنتها مع منافسيها للتوصل إلى كل ما هو جديد من أفكار ومنتجات وأسواق. (دقيش، 2023)

و عرف الابتكار بأنه عملية التطوير و الجميع الأفكار الحديثة من قبل الموظفين، كما يعتبر الابتكار هو تلك العملية الديناميكية العقلية التي تحتاج أن يكون التفكير بما هو جديد و غير مطروح سابقاً أحد مدخلاتها وذلك لتطوير الأفكار الجديدة أو استحداث استعمالات جديدة لمنتجات موجودة أصلاً مع الأخذ بعين الاعتبار أن يكون أفضل مما كان عليه ويوضح أيضاً أن عملية الابتكار تمتاز بالعديد

من السمات منها أنها غير حتمية، وتهتم بالمعرفة، وغالباً ما تثير الجدل وحدودها تتباين كما أنها تعيد صياغة عملية الابتكار في العلاقات داخل العمل والترتيبات الموجودة في الهيكل التنظيمي. (ملاوي، 2024)

### 3.1.2 مسارات الابتكار

تقسم الدراسة الابتكار من حيث التعريف إلى ما يلي:

الابتكار كنتيجة: يقول بإن الابتكار هو الاختراع الذي تم طرحه في السوق عند وجود منتج مستحدث أو عند الاستخدام الأول أثناء عملية الإيجاد وذلك عند ابتكار العملية. كما يرى أنه عملية البناء الجديدة للربح والمنتجات وعمليات الإنتاج والخطط التسويقية، ويرى أنه أي فكرة أو شيء ما جديد يختلف من حيث النوع عن الأشكال الموجودة مسبقاً. (شهوان، 2024)

الابتكار كعملية: وهو ناتج عملية التطوير والتطبيق للأفكار الجديدة من قبل مجموعة العاملين الذي يعملون في إطار مؤسسي منظم ويرى البعض أنه العملية التي يتم فيها استقطاب الأفكار الجديدة لتقديم حلول للمشاكل الحالية، كما يعرفه آخرون بأنه تطبيق الأساليب والهيكل وممارسات العمليات بحيث تشكل الحالة الجديدة من الفن بحيث تسعى للمزيد من تحقيق أهداف تنظيمية. (عثمان، 2023)

ويوضح مستويين للابتكار وهما:

■ **المستوى الكلي:** حيث يقول بأنه المستوى الذي يوضح الكيفية والسبب لدعم التكنولوجيا للابتكار.

(Machos، 2021)

■ **المستوى الجزئي:** وهو المستوى الخاص بالمنظمة والذي يركز على التسويق وخدمات البحث والتطوير

كما ويركز على أي خدمات أخرى بحيث تكون مسؤولة عن الابتكار. (قداري، 2021)

### 4.1.2 تطور الابتكار

تطور الابتكار خلال العقود الماضية بحيث تم اعتباره تطويراً منفصلاً ناتجاً عن الدراسات التي قام بها الباحثون بشكل منفصل، أما في وقتنا الحاضر فلم يعد الابتكار نتيجة الأعمال الفردية وإنما بات

ينظر له كعملية لتقديم حلول في مشكلة معينة وهو عملية تفاعلية تتضمن علاقات تفاعلية بين المؤسسات وجميع الأطراف الفاعلة، وبدأت أيضاً عمليه متنوعة للتعليم وعمليه تتضوح على التبادل للمعرفة المقننة وللمعرفة الضمنية. (بيان، 2024)

## 5.1.2 خصائص الابتكار

يمكن توضيح خصائص الابتكار الأساسية من خلال خمس سمات رئيسية، حيث يتم من خلالها الاستجابة للابتكار أو رفضه:

- 1- **الميزة النسبية:** ويقصد بها أن تكون المنتجات والخدمات المبتكرة تفوق المنتجات والخدمات الحالية في نظر الزبائن، ويمكننا احتساب درجة الميزة النسبية اقتصادياً كنسبة الأرباح المتوقعة من خلال الرضى للزيتون والرفاهية الاجتماعية. (عبد المجيد، 2024)
- 2- **التوافق:** وهو قياس توافق الابتكار مع قيم الزبائن وتجارهم واحتياجاتهم، وهناك دراسة قام بها حيث أوضح أن جميع الخدمات المبتكرة المقترحة من جهة البنوك التايوانية بكل ما يخص الهاتف المحمول اعتمدت على التوافق الواضح للابتكار مع نمط حياة الأفراد. (عظام، 2022)
- 3- **التعقيد:** وهو مقياس لصعوبة استيعاب واستخدام الابتكار كمنتج أو كخدمة، وبالتالي نقل أو تزيد محاولة الاستجابة له. (ملاوي، 2024)
- 4- **قابلية الاختبار:** وهي إمكانية إخضاع الابتكار قبل التسويق له على عينة صغيرة، وذلك لأن الشيء المبتكر المجرب مسبقاً يكون أقل مخاطرة على صعيدي الأفراد والمنظمات. (بن علي، 2022)
- 5- **قابلية الملاحظة:** وهي انعكاس مدى وضوح ورؤية نتائج الابتكار، فكلما زاد هذا المقياس كانت هناك استجابة أسرع للمنتج أو الخدمة المبتكرة. (دقيش، 2023)

## 6.1.2 مبادئ الابتكار ومصادره

### ➤ مبادئ الابتكار

أوضح أن هناك مبادئ رئيسية للابتكار تم وضعها من قبل الكثير من مدراء المنظمات وأهم هذه الأثرء الريادية:

إعطاء الفرصة والمجال للأفكار الجديدة أن تولد إذا كانت في الاتجاه السليم. و بعد الفرد في المنظمة مصدر قوتها ، والاهتمام بتنميته يجعلها أكبر وأفضل وأكثر ابتكاراً، وعملية اتخاذ القرار هي عملية قائمة على احترام الفرد في المنظمة و تشجيعه ومشاركته في تلك العملية، وتجاوز الروتين و اللامركزية في المعاملات بين الأفراد والارتقاء بالعمل من وظيفة روتينية إلى شيء ممتع ويكون ذلك إذا قامت المنظمة بتحويل النشاط إلى مسؤولية وبالتالي المسؤولية الطموح، والارتقاء الدائم بالفكر والطروحات عن طريق خلق شعور لدى الفرد بالتكامل مع عمله، وبناءات عليه وجب على المدير خلق أساليب للتحفيز من أجل صناعة الإبداع من الأفراد وإيجاد وحدة خلاقة من مؤسسته، يعد المحرك الأساسي للحافز لدى الأفراد للعمل مبدأ التطلع إلى ما هو أفضل وكذلك السعي المستمر إلى تحقيق أهداف أبعد وذلك لضمان مسيرة فاعلة وكاملة، يتنافى الابتكار مع ما يعرف بالنسخة المكررة، بل الابتكار يعني أن تكون نسخة رائدة وفريدة، ولكي تكون كذلك يجب الانتباه للتجارب الأخرى والتمايز بين الجيد والردئ لتكون الأعمال مجموعة من الإيجابيات، فتنص الإستراتيجية الابتكارية على أن المنظمة لها إحدى الحالات التالية : قائمة أو تابعة أو نسخة مكررة إن عملية تولد أفكار جديدة هي مسألة مرتبطة بالزمن، والقدرة على تنفيذها تأتي من تكرار المناقشة، إن عملية التعلم بواسطة العمل لها أهمية كبيرة إذ تعتبر أفضل طريق لتطوير الكفاءات وتوسيع النشاط واندماج الأفراد بمهامهم ووظائفهم، لا يخلو الابتكار في ماهيته من الحذر والكثير من التحدي والشجاعة، ويحتاج دائماً إلى الحوار والنقاش. (شهوان، 2024)

## 7.1.2 مصادر الابتكار

أكد بأن بيتر دركار يشير إلى سبعة مصادر رئيسية للابتكار على أساس أنه نشاطاً منظماً وهي كالآتي:

- المصدر الفجائي (غير المتوقع وعناصره تشتمل على النجاح المفاجئ وال فشل غير المتوقع والحدث الخارجي الفجائي). (قداري، 2021)
- مصدر تعارض الواقع كما هو والواقع المفترض حيث أن هذا النوع من التعارض يشير إلى فرصة كبيرة للابتكار. (Machos، 2021)

- مصدر الوقائع الاقتصادية المتعارضة، ومن الأمثلة عليه التعارض الحاصل بين طلب متزايد في ظل غياب الربحية، والتعارض الحاصل بين القيمة المدركة والواقعية لمتلقي الخدمة أو المستهلك. (عثمان، 2023)
- مصدر الحاجة أم الاختراع، بأن الحاجة تعتبر فرصة كبيرة للابتكار. (عظام، 2022)
- البنية الخاصة بالسوق: وهي حتمية أن يتغير السوق بفعل المنافسة أو اختلاف القيمة المتوقعة من المستهلكين وهذا يعتبر من الفرص العظيمة للابتكار، وينضوي هذا المصدر على استجابة سريعة للتغيير والتنبؤ بالفرص ومؤشرات تغير الصناعة. (بيان، 2024)
- العوامل السكانية: ويعرف هذا العامل والمصدر بأنه تحولات تطرأ على حجم السكان ومتوسط أعمارهم حسب العمل ومستوى الدخل والتعليم، وهذا يعد من المصادر القوية للابتكار في عدة مجالات أهمها إيجاد قطاعات أسواق جديدة. (شهبان، 2024)
- تبدل الإدراك: ويقصد به تبدل رؤية وإدراك الأفراد في المجتمع، والتوقيت الذي يحصل فيه هذا التبدل مهم أيضاً مع أهمية أن يأتي الابتكار في الوقت المناسب. (بن علي، 2022)
- المعرفة الجديدة: إن قيام الابتكار على أسس معرفية بكل أبعادها بشكل مصدراً عظيماً للخروج بالأفكار والمنتجات والخدمات الجديدة. (ملاوي، 2024)

## 8.1.2 عناصر الابتكار

أكد على ضرورة قيام مفاهيم الابتكار على أسس منهجية وعلمية، بحيث تتخذ من العلم والتكنولوجيا والاتساع في الأفكار وارتقاء الأهداف والطموحات أساساً إستراتيجياً لخلق وضع أفضل وهذا يتطلب توفير عناصر الابتكار التالية:

أولاً: التخطيط الاستراتيجي: تواجه المنظمات السؤال الدائم (ماذا ستكون صورة العالم غداً؟) والإجابة ستكون حتماً أن الغد سيكون مختلفاً عن اليوم ولكن هذا الاختلاف إلى أي درجة، ففي عالم دائم التغيير والتطوير تتجلى وظيفة التخطيط الإستراتيجي وتصبح أكثر صعوبة. (دقيش، 2023)

ويقول إن المنظمات عموماً بحاجة إلى خطة عمل إستراتيجية يسبقها تخطيط إستراتيجي وذلك للوصول إلى تقديم خدماتها وتعزيز من وضعها التنافسي. (عبد المجيد، 2024)

وبالتالي فإن عملية التخطيط الإستراتيجي تجيب عن الأسئلة المطروحة، ما هو موقع تواجد المنظمة اليوم؟ وما هي وجهتها؟ وما هي السبل التي تمكنها من الوصول إلى وجهتها؟ وكيف يمكن أن تحقق قيمة مضافة

يعرف التخطيط الإستراتيجي على أنه عملية استشراف للمستقبل من خلال تصور ماهيته متبوعة بعمليات على أرض الواقع من تطوير للإجراءات والعمليات للوصول إلى هذا المستقبل. (Machos، 2021)

وقد بين أن عملية صياغة الإستراتيجية يتم صياغتها على ثلاثة مستويات:

(المستوى الكلي: وفيه يتم اتخاذ قرارات لتحديد التوجه العام المستوى الإداري: على صعيد الوحدات الإدارية والمستوى التشغيلي). (قداري، 2021)

وهذه المستويات تلعب دوراً أساسياً في عملية الابتكار ومنها يتضح لنا أن التخطيط الإستراتيجي عنصراً هاماً من عناصر عملية الابتكار والتي تظهر القدرة على التخطيط المستقبلي والتنبؤ بأهداف التطوير والتغيير. (عظام، 2022)

## 9.1.2 التفكير الاستراتيجي

أوضح أن عملية الابتكار تتطلب النظر للمستقبل طويل الأمد من الإدارة العليا للبنوك، مدعوماً بخطة مبنية على التفكير السليم مع الأخذ بعين الاعتبار أن الوقت المستغرق في التفكير هو نوع من الاستثمار وليس ضياعاً للمجهود. (شهوان، 2024)

عبر عن التفكير الإستراتيجي بأنه المنهجية التي تمكن قادة المنظمات من توجيه المنظمات بداية من الانتقال من العمليات الإدارية المجردة ومواجهة الأزمات إلى الوصول لمرحلة الرؤية المختلفة للعوامل

الداخلية والخارجية القادرة على تغيير البنية المحيطة بهم، بحيث تكون المرحلة الجديدة موجهة إلى المستقبل مع عدم إهمال الماضي. (عثمان، 2023)

ثالثاً: بناء الثقافة التنظيمية: وتعني قيم يشترك فيها العاملون تستند إلى احتياجاتهم مع ترسيخ قيم الأسرة الواحدة مع ضرورة الاهتمام بهم وتدريبهم وتوفير قدر من الاحترام وإفساح المجال للمشاركة. (بن علي، 2022)

### 10.1.2 خطوات الابتكار

أوضح أن أساس التفكير في عملية الابتكار ودراستها هو الفكرة، حيث أن أي فكرة أو سلعة جديدة يجب أن تقدم قيمة مضافة حقيقة للمنظمة أو السوق، مع ضرورة الانتباه إلى أن العملية لا تكتمل إلا عندما تصل إلى نقطة التطبيق وتحتاج عملية الابتكار إلى خطوات نوردها فيما يلي:

- إيجاد وخلق الفكرة: حيث أن السلع والخدمات تحتاج إلى إبداع ذاتي ومعالجة معلومات. (شهبان، 2024)
- التجربة المبدئية: وترمي هذه الخطوة إلى ضرورة فحص ما هو جديد واختيار التطبيقات الأنسب له. (بيان، 2024)
- تحديد ملائمة الفكرة: وهي تضمين المنافع والتكاليف لتبني سلعة أو خدمة جديدة.
- التطبيق: وهي عملية تسويق السلعة أو الخدمة أو عملية إطلاق للعملية الجديدة كلياً. (ملاوي، 2024)

### 11.1.2 سمات المدراء المبتكرين

أجمل أهم السمات الواجب توافرها في المدير المبتكر بأن يكون عاكفاً على البحث ويمتاز بالخيال الواسع، ولديه القدرة العالية على الإحساس بالمشكلات من حوله، ولديه المقدرة على تحسس الخلل والقصور ولديه المرونة الذهنية العالية في معالجة المشكلات، وأن يهتم بمجمل المؤشرات دون التفاصيل

ومن الضروري أن يكون على قدر عال من التمتع بأصالة التفكير وعدم التقليد وذلك يكون بفتح العقل على كل الخبرات ويتمتع بوعي كامل بأهدافه، وأن يكون موضوعياً في الحكم ومستقلاً في الرأي، ويتمتع بالثقة والإيمان بقدراته والقدرة على تجاوز الصعوبات، وأن يكون متحمساً للأفكار والأعمال الكبيرة وتكون قدرته على تنظيم الأفكار والتعبير عنها مميزة يكون ذو مستوى طموح عالي. (دقيش، 2023)

## المبحث الثاني: إدارة المخاطر السيبرانية

تركز إدارة المخاطر السيبرانية على تحديد المخاطر المحتملة وتحليلها، وتقييم المخاطر السيبرانية التي يجب التعامل معها، وتنفيذ إستراتيجيات للتعامل مع تلك المخاطر؛ حيث أن المنظمات التي تحدد المخاطر مسبقاً تكون أكثر استعداداً، وتكون أكثر قدرة وفعالية على مواجهة التحديات المختلفة من خلال استخدام العمليات والأساليب الناجعة لإدارة هذه المخاطر. (الرحماني، 2024)

### 1.2.2 مفهوم المخاطر

تناول العديد من الباحثين والكتاب تعريف الخطر، كل يعبر عن وجهة نظره، وغالباً ما تكون وجهات النظر هذه متأثرة بنوع وطبيعة الدراسة والأغراض التي يرمون لها والمدارس التي ينتمون إليها، إلا أن أغلب هذه التعريفات قد جاءت في إطار واحد، يمثل حالة من عدم التأكد من تحقق ظاهرة معينة أو موقف معين، بالنظر لما قد يترتب عليه من نتائج ضارة من عدة نواحي ومنها النواحي المالية والاقتصادية. Eladia (2024)

يستخدم مصطلح المخاطر غالباً كمرادف للخطورة أو الأخطار، ويتصف بأنه فرصة لاحتمالية وقوع حدث ما، وعادة ما يكون له دلالة سلبية، كما يرتبط بأي نشاط لفرد أو مؤسسة ارتباطاً مباشراً بأحداث غير متوقعة قد تنشأ في سياق أنشطتها وتؤدي إلى خسائر مادية. (الخريج، 2022)

ووفقاً فإن المخاطر هي احتمال نشوء خسارة من بعض الأحداث الطبيعية وأنواع مختلفة من الأنشطة الناتجة من البشر. (Metwally, 2022)

وعرفت أيضاً بأنها الضرر الذي يهدد الأفراد والمجتمع البشري، والبيئة المحيطة لكنه يحتمل أن يحدث، أو أنه حدث فعلاً، وأنه يمكن احتواؤه إن لم يتفاقم إلى درجات عالية. (Ramdani, 2024)

\*لذلك فإن جوهر المخاطر يتميز بعاملين احتمالية وقوع الحدث وتأثيره، أي احتمال وقوع الخطر خلال فترة زمنية معينة، والخسائر المترتبة على حدوثه، وبالتالي يمكن حساب قيمة المخاطرة من خلال المعادلة التالية المخاطرة - الاحتمالية  $\times$  التأثير - احتمالية حدوث المخاطر  $\times$  القيمة المالية للتأثيرات.

وقد ينظر للمخاطر على أساس الخطر والفرصة، مما يعني أن المخاطر قد تكون نتائجها إيجابية أو سلبية، ومن ثم فإن حدوث الخطر يمكن أن ينتج فرصة للاستفادة منها أو تهديد بالخسارة في تحقيق الأهداف، وقد تكون للمخاطر أسباب داخلية وخارجية، أو قد تجتمع في وقت واحد ويمثل الخطر في أي مشروع حدثاً أو ظرفاً غير مؤكدة، مما يؤدي إلى تأثير سلبي أو إيجابي على أهدافه ومبعضين. Abd-Elma (geed, 2024)

مما سبق فإن الباحث يعرف المخاطر بأنها النتائج التي تصل إليها المنظمة نتيجة لظروف وحالات عدم التأكد، والتي قد تتسبب بآثار سلبية على أداء المنظمة إذا لم يتم التصدي لها وإدارتها بالشكل الأمثل أو قد تمثل فرصة للاستفادة منها لتحقيق الأهداف. (شرف، 2023)

## 2.2.2 العلاقة بين المخاطر وعدم التأكد

\*تعكس المخاطر وعدم التأكد تغيرات غير متوقعة في البيئة وبعض السلوكيات؛ حيث تعد العلاقة بين المخاطر وعدم التأكد من المفاهيم المهمة، وذلك لأن الإدارة ترتبط ارتباطاً مباشراً بأخذ وحساب المخاطر وعدم التأكد؛ حيث أن المخاطر تعرف على أنها احتمال تعرض كيان معين لخسارة نتيجة للقرار الذي يتم اتخاذه، ويشمل عدم التأكد التغيرات التي يصعب حسابها والأحداث التي لا يمكننا تقديرها بسبب قلة المعلومات.

وعرف عدم التأكد بأنه يتعلق في غياب المعلومات أو عدم القدرة على التنبؤ بالظروف البيئية في المؤسسة بدقة بسبب نقص المعلومات أو عدم القدرة على التمييز بين البيانات ذات الصلة وغير ذات الصلة؛ حيث يدل مفهوم عدم التأكد على عدم كفاية المعلومات عن بيئة المؤسسة مما يصعب في تقييم

النتائج المرتبطة بقرارات المؤسسة، وكذلك صعوبة التنبؤ بمتغيرات البيئة، وخاصة تلك التي تؤثر على فاعلية المنظمة.(Eladia, 2024)

كما عرفه آخر بأنه ذلك الغموض الذي يتعلق في عناصر بيئة الأعمال المتغيرة والذي يحتمل أن يؤثر على أهداف المؤسسة.(Metwally, 2022)

وهناك اختلاف بين المخاطر وعدم التأكد يمكن أبارزها بالآتي:

1. يتم تعريف المخاطرة على أنها حالة الفوز أو الخسارة بشيء، أما عدم التأكد حالة لا توجد فيها معرفة بالأحداث المستقبلية.
2. يمكن قياس المخاطر وتحديد أثرها، من خلال النماذج النظرية، أما عدم التأكد على العكس من ذلك؛ حيث لا يمكن قياس عدم التأكد من الناحية الكمية، مثل الأحداث المستقبلية التي لا يمكن التنبؤ به.
3. النتائج المحتملة معروفة في الخطر، أما حالة عدم التأكد، فإن النتائج غير معروفة.
4. يمكن السيطرة على المخاطر إذا تم اتخاذ التدابير المناسبة للسيطرة عليها، أما عدم التأكد غالبا ما تكون خارجه عن سيطرة الشخص أو المؤسسة؛ حيث أن المستقبل غير مؤكد.
5. يمكن تقليل المخاطر إلى الحد الأدنى من خلال اتخاذ الاحتياطات اللازمة، أما عدم التأكد لا يمكن التقليل منه.
6. في حالة الخطر، يتم تعيين الاحتمالات لمجموعة من الظروف التي لا تكون ممكنة في حالة من عدم التأكد.

على الرغم من الاختلاف الواضح بين المخاطرة وعدم التأكد، إلا أنه يتم استخدامهما عادة لتحديد الموضوع ذاته؛ فعدم التأكد هو ظاهرة لا يمكن قياسها، في حين يسعى الجزء القابل للقياس بالمخاطر. (شرف، 2023)

وإن العنصر الأساسي في التمييز بين المخاطرة وعدم التأكد هو الاحتمال؛ حيث يشير الاحتمال إلى ظاهرة أو حدث معين يحدث في ظل ظروف محددة جيداً. (موسى، 2023)

لذا يمكن القول إن العلاقة بين المخاطر وعدم التأكد هي علاقة وثيقة؛ حيث أن المخاطر تعتمد على الاحتمالات، في حين أن عدم التأكد يتعلق بمدى توافر المعلومات لتحديد الاحتمالات. Metwally, (2022)

### 3.2.2 أنواع المخاطر

تختلف أنواع المخاطر باختلاف أسلوب التصنيف، وقد تعددت واختلفت أنواع وتصنيفات المخاطر حسب وجهات نظر الباحثون والمختصون في هذا المجال، فمنهم من صنف المخاطر وفقاً لمصادرها، ومنهم من صنف المخاطر وفقاً لآثارها، ومنهم من صنف المخاطر وفقاً لطبيعتها، ومنهم من صنفها من المنظور المالي، ومنهم من صنفها من المنظور المؤسسي، وهناك من صنفها إلى مخاطر خارجية ومخاطر داخلية حسب البيئة التي تقع فيها، ولكن بالرغم من تعدد الأنواع والتصنيفات ففي نهاية الأمر تلتقي معظم هذه التصنيفات في مساحات مشتركة. (الرحماني، 2024)

#### حيث صنفوا المخاطر إلى:

1. المخاطر الخارجية يتأثر مستوى المخاطر الخارجية بعدد كبير جداً من العوامل مثل العوامل: (السياسية والاقتصادية، والديموغرافية، والاجتماعية، والجغرافية).
2. المخاطر الداخلية يتأثر مستواها بالنشاط التجاري لإدارة المنظمة، واختيار إستراتيجية التسويق المثلى، والسياسة والتكتيكات، وما إلى ذلك من عوامل: (الإنتاج المحتمل، والأجهزة، ومستوى إنتاجية العمل، والتكنولوجيا).

## 4.2.2 مفهوم الأمن السيبراني والتهديدات السيبرانية

### ❖ تعريف الأمن السيبراني

يُعد الأمن إحدى أهم مبادئ ومرتكزات الحياة البشرية، وعرف الأمن اصطلاحاً بأنه مجموعة المعارف والتكنولوجيا والمؤسسات والأنشطة التي تحمي وتحافظ الوجود البيولوجي للحياة البشرية والسلام الجماعي والازدهار لتعزيز حرية الإنسان. (Ramdani, 2024)

ومع تطور المجتمعات والحياة الإنسانية دخلت العديد من التطورات والمتغيرات على مفهوم الأمن، ولم يجمع الباحثون على إعطاء مفهوم واحد للأمن، بل كان هنالك اتجاهين رئيسيين هما:

■ **الاتجاه الأول:** يعطي مفهوماً ضيقاً للأمن بحيث يقصره على كل ما يتعلق بالحفاظ على السيادة الوطنية وعلى الوضع القانوني الطبيعي القائم للدولة والمجتمع في حدود الإطار الإقليمي للدولة. (الطاهرات، 2023)

■ **الاتجاه الثاني:** يعطي مفهوماً أوسع للأمن؛ حيث أدى تطور الفكر الإنساني إلى تطور مفهوم الأمن، وأن هذا التطور قد وصل بفلسفة الأمن إلى درجة الإحاطة بكل جوانب الحياة الإنسانية، والدور المعاصر للمنظومة الأمنية مفاده تحقيق الأمن على المستوى الداخلي والخارجي، وهذا الاتجاه في تناوله للأمن الشامل يأخذ بتصورات وطرق عمل جديدة في تعامله مع قضايا الأمن. (الخريج، 2022)

وفكرة الأمن طرحت لأول مرة تحت أسم مركب وهو الأمن الإقليمي "تقضي هذه الفكرة أن هنالك أربع مرتكزات أساسية للأمن لابد أن تؤخذ بعين الاعتبار من قبل الباحثين عند القيام بأي محاولة لتحليل الأمن الإقليمي في أي منطقة من العالم. ويمكن تحديد هذه المستويات في النقاط التالية:

1. البيئة المحلية للأمن، والتي تشمل مقومات الدولة الداخلية مثل قوة الدولة الاقتصادية، وطبيعة نظام الحكم فيها، ومستوى الاستقرار الأمني، وعلاقة الدولة بالمواطنين، وطريقة تقسيم الثروة ومستوى النشاط الاقتصادي والتنمية الاجتماعية وغيرها.

2. يتمثل المستوى الثاني من مستويات تحليل الأمن في العلاقات بين الدول نفسها، على اعتبار أن هذه العلاقات هي التي تشكل النظام الإقليمي المستقر أو المضطرب.
3. المستوى الثالث في تحليل الأمن هو تفاعل المناطق المجاورة مع بعضها البعض، فحالة الاستقرار أو الاضطراب في مكان ضمن محيط منطقة تؤثر في الأطراف الأخرى.
4. يأتي في المستوى الرابع من تحليل الأمن دور القوى العظمى المسيطرة على النظام العالمي، والتي لها مصالح حيوية متنامية بشكل متزايد في كل أنحاء العالم، وهذا يعني أن مواقفها واستراتيجياتها الأمنية في سياستها الخارجية هي مدخلات مهمة وحاسمة في السياسة الأمنية الإقليمية.

#### ويمكن ذكر عناصر الأمن بالأبعاد التالية

- 1- الأمن الاقتصادي: هو امتلاك الفرد الوسائل المادية والمالية الكافية التي تمكنه من حياة مستقرة ومشبعة، ويتمثل الأمن الاقتصادي بشكل عام بالنسبة للكثيرين في امتلاك ما يكفيهم من النقود لإشباع حاجاتهم ومتطلباتهم الأساسية.
- 2- الأمن الغذائي: توفير الغذاء لجميع المواطنين في جميع الأوقات؛ حيث أن الملايين من الناس في العالم لا يزالون يعانون من الجوع سواء من خلال عدم توفر الغذاء، أو في أحيان كثيرة عن طريق انعدام المستحقات أو الموارد اللازمة لتأمين العيش الكريم، وهي الغذاء، والمأوى المناسب، والتعليم، والرعاية الصحية الأساسية، أي ضمان الدخل الأساسي والعيش الكريم للمواطنين والعيش، وتأمينهم بفرص العمل والموارد والحاجات الأساسية.
- 3- الأمن الصحي: يشمل تأمين العلاج الطبي لجميع المواطنين، وتحسين الظروف الصحية.
- 4- الأمن البيئي: العيش في بيئة طبيعية صحية بعيداً عن التصحر، وإزالة التهديدات البيئية التي تعرض حياة المجتمع للخطر.
- 5- الأمن الشخصي: يشمل الأمن الفردي من العنف الجسدي، وتأمين الحماية للنساء والأطفال.
- 6- أمن المجتمع: يستمد معظم الناس أمنهم من المجتمع الذي يعيشون فيه مثل: الأسرة، المجتمع، التجمع السياسي، والمجموعة العرقية، وما إلى ذلك).

7- الأمن السياسي: العيش في مجتمع يضمن حقوق الإنسان الأساسية وحرية الرأي والتعبير.

ويُعد مصطلح الأمن السيبراني من المصطلحات شائعة الاستخدام وجزء لا يتجزأ من أبعاد الأمن الشامل، وقد تعددت التعريفات التي تناولت هذا المصطلح؛ حيث يستخدم مصطلح الجرائم السيبرانية لوصف مفاهيم وأنواع مختلفة من الجرائم التي تتم عبر الإنترنت وأجهزة الحاسوب، فهناك من عرفه بأنه مجموعة من الأساليب الدفاعية التي تستخدم للكشف عن المتسللين المحتملين وإحباط عملياتهم. (الرحماني، 2024)

ويشير إلى أن الأمن السيبراني يتضمن الحد من مخاطر الهجمات الضارة على البرامج وأجهزة الحاسوب والشبكات. (Metwally, 2022)

وعرف أيضا بأنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمن والمبادئ التوجيهية، والضمانات والتقنيات التي يمكن أن تستخدم لحماية البيئة السيبرانية وأصول المنظمة. Abd- (Elma geed, 2024)

وعرفه آخر بأنه مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به. (شرف، 2023)

وأرا آخرون أن الأمن السيبراني تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني والأنظمة التي تدعم الفضاء الإلكتروني. (Eladia, 2024)

ومن المصطلحات ذات العلاقة بالأمن السيبراني الآتي

1. الفضاء السيبراني: يتعلق في التواصل من خلال الربط بين التقنيات الرقمية المختلفة؛ حيث تشمل مجموعة من العناصر المادية وغير المادية، وتتكون من البرمجيات وشبكات التواصل والتطبيقات الاجتماعية والمستخدمين سواء أكانوا مشغلين أو مستعملين.

2. الردع السيبراني: يتعلق الردع السيبراني بتوفير الحماية ومنع الأعمال التي تهدف إلى الأضرار في أصول الدولة في الفضاء السيبراني، إضافة إلى تلك التي تدعم العمليات الفضائية.

3. الهجمات السيبرانية: يقصد بها أي فعل يعرض وظائف وقدرات شبكة الحاسوب لهدف سياسي أو أمني من خلال استغلال ثغرات أمنية معينة تمكن المستهدف من التخريب، وتعرض النظام إلى الخطر.

4. الجريمة السيبرانية نشاط غير مشروع محلة معطيات الحاسوب أو كل فعل أو امتناع عن فعل مخالف للقانون صادر عن إرادة أئمة يعاقب عليه القانون.

مما سبق فإن الباحث يعرف الأمن السيبراني بأنه مجموعة من الأنشطة والتدابير التي تهدف إلى حماية الشبكات وأجهزة الكمبيوتر والأجهزة ذات الصلة والبرامج والبيانات من الهجمات والتهديدات الإلكترونية التي تهدف إلى تدميرها أو تعطيل عملها أو إضعافها. (Metwally, 2022)

#### ❖ تعريف التهديدات السيبرانية

تعرف التهديدات السيبرانية Cyber Vulnerabilities بأنها كافة الأفعال والممارسات التي تقوض من قدرات ووظائف شبكات الحاسوب والأنظمة المعلوماتية الغرض قومي أو سياسي أو اقتصادي أو مالي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام المعلوماتي. (موسى، 2023)

يشمل نطاق عمليات الأمن السيبراني حماية المعلومات والأنظمة من التهديدات السيبرانية الكبرى، وتأخذ هذه التهديدات أشكالاً مختلفة ومتنوعة، وغالبا ما تستهدف التهديدات السيبرانية الأصول السرية والسياسية والعسكرية لدولة ما، ومن التهديدات السيبرانية الشائع:

1. الإرهاب السيبراني: هو الاستخدام المبتكر لتكنولوجيا المعلومات من قبل الجماعات الإرهابية لتعزيزه أجندة سياسية، وقد اتخذ شكل هجمات على الشبكات وأنظمة الكمبيوتر والاتصالات، والبنى التحتية.

2. الحرب السيبرانية تنطوي على استخدام تكنولوجيا المعلومات لإحداث أضرار ويتم تنفيذ هجمات الحرب الإلكترونية من قبل المتسللين الذين تلقوا تدريباً على استخدام تكنولوجيا المعلومات،

والدخول إلى البيانات، وتعطيل خدمات البنية التحتية مثل وسائل النقل والخدمات الطبية، أو تعطيل التجارة.

3. التجسس السيبراني هي ممارسة استخدام تقنية المعلومات للحصول على معلومات سرية بدون إذن من أصحابها، وغالبا ما تستخدم في العمليات العسكرية والأمنية.

وتتضمن أيضا التهديدات السيبرانية اختراق نطاقات واسعة من الإنترنت، والنزاعات الجيوسياسية، والنزاعات العرقية، والتجسس، والتخريب، وغسل الأموال. (الطاهرات، 2023)

ويضيف الباحث إلى تلك التهديدات اختراق المحطات الفضائية، وعناوين البريد الإلكتروني، واختراق المواقع الإلكترونية بهدف زعزعة أمن واستقرار الدول، أو تشويه سمعتها. (Ramdani, 2024)

### أهمية الأمن السيبراني

يُعد الأمن السيبراني جزءا حيويًا من عالم رقمي آمن؛ حيث يوفر الأمن السيبراني الحماية من المتسللين ومجرمي الإنترنت والاحتيال الإلكتروني وغيرهما، وهو أحد المجالات التكنولوجية سريعة التطور، ليس فقط في قطاعات تكنولوجيا المعلومات ولكن أيضا في قطاعات الصحة والبنوك والتعليم والجيش والأمن والحكومة. (Badawy, 2021)

### ويشير إلى أهمية الأمن السيبراني بما يلي:

1. المحافظة على سرية البيانات وسلامتها، وذلك من خلال منع العبث بها، إضافة إلى ذلك جاهزية المعلومات والبيانات عند الحاجة.
2. توفير الحماية اللازمة للأجهزة والمواقع والشبكات من أية اختراقات لتحقيق منظومة الدرع الأمني الواقي للبيانات والمعلومات.
3. التعرف على الثغرات ونقاط الضعف في الأنظمة الإلكترونية، والعمل على معالجتها.
4. استغلال الوسائل والأدوات اللازمة، والعمل على تطويرها لتحقيق الغاية من الأمن السيبراني.
5. يسهم الأمن السيبراني في توفير بيئة آمنة من خلال شبكة اتصالات محصنة.

كما تكمن أهمية الأمن السيبراني في فهم المخاطر وإدارتها والتحكم في التداعيات التنظيمية والقانونية وغيرها من التداعيات المرتبطة في مخاطر الأمن السيبراني، ومواجهتها والتقليل من الآثار الناجمة عن الهجمات السيبرانية. (الخريج، 2022)

## 5.2.2 عناصر إدارة الأمن السيبراني

يُعد الأمن السيبراني وسيلة لحماية النظام والشبكات والتقنيات من الوصول غير المصرح به في ظل عصر التكنولوجيا، لذا من الضروري لأي منظمة أو مؤسسة أن يكون لديها فريق مناسب يمكنه البحث عن التهديد السيبراني والتخطيط للتعامل معه في الوقت المحدد. وتشمل عناصر إدارة الأمن السيبراني ما يلي:

1. أمان التطبيق: تلعب التطبيقات دورًا أساسيًا في المشاريع التجارية؛ لهذا السبب تحتاج الشركات التركيز على أمان تطبيقات الويب.
2. أمن المعلومات: تتضمن سجلات الأعمال والبيانات الشخصية وبيانات العملاء والملكية الفكرية، وبالتالي من الضروري أن يكون لأي مؤسسة أمن إلكتروني مناسب.
3. أمن الشبكة: يتم إجراء اختبار اختراق الشبكة لتقييم نقاط الضعف في النظام ومشكلات الأمان الأخرى التي تحدث في الخوادم والأجهزة وخدمات الشبكة.
4. تخطيط استمرارية الأعمال: يتعلق تخطيط استمرارية الأعمال حول مدى الاستعداد للتدخل أو التهديد السيبراني من خلال تحديد التهديدات التي تتعرض لها المنظمة في الوقت المحدد وتحليل كيفية تأثير العمليات وكيفية التغلب عليها.
5. أمن العمليات: يستخدم أمن العمليات لحماية وظائف المنظمة.
6. تعليم وتدريب الموظفين: لكي يتم الحفاظ على الأمن السيبراني للمؤسسة من الضروري أن تقوم المنظمة بتدريب موظفيها على الأمن السيبراني؛ بحيث يجب أن يكون كل موظف على دراية بالهجمات الإلكترونية، كذلك أن يكون لديه القدرة على التعامل مع التهديدات الإلكترونية التي قد يواجهونها.

## 6.2.2 الخلفية التاريخية لإدارة المخاطر وتطورها

ترجع البدايات الأولى لإدارة المخاطر كمصطلح على أنها فكرة متفرعة من نظرية القرار؛ حيث تعلق بالصدفة والاحتمال من الناحية الرياضية، وقد ناقشها على أنها تشير إلى مصطلح محفوف بالمخاطر في وصف مشكلة الاحتمال. ومع ذلك، فإن نظرية القرار موجودة منذ حوالي عقدين من الزمن وبالتالي يمكن أن نستنتج أن نظرية القرار بدأت في الخمسينيات من القرن الماضي. (الرحماني، 2024)

كما ذهب البعض أن فلسفة المخاطر تستمر في النمو من حيث النطاق والموقف، ومع ذلك، فإن استخدام مفهوم الخطر في الفلسفة القديمة له نطاق كبير، ومعقد للغاية للتحقيق فيه. (موسى، 2023)

إن الحديث عن إدارة المخاطر قد بدأ منذ منتصف القرن الماضي وكان تطوره عبر السنين مقترناً بمحطات هامة، ويشير أن دراسة إدارة المخاطر بدأت بعد الحرب العالمية الثانية، وأنها لطالما ارتبطت بإدارة المخاطر باستخدام تأمين السوق لحماية الأفراد والشركات من الخسائر. (Eladia, 2024)

ويشير أن تطور مفهوم إدارة المخاطر كان من خلال ما يعرف باتفاقية بازل والتي اكتسبت شهرة واسعة في القطاع المصرفي، ففي عام 1988 أصدر بنك التسويات الدولي توصيات لما يعرف بمقررات باللواتي تناولت نوعاً واحداً من المخاطر وهي مخاطر الائتمان؛ نتيجة الالتزامات التي تعرضت لها البنوك آنذاك، وفي عام 1998 تم اعتماد ما يعرف بمقررات بازل (1.5) حيث أضافت نوع آخر من المخاطر وهي المخاطر السوقية إلى جانب مخاطر الائتمان. وخلال الفترة من عام 1999 إلى عام 2007 تم إصدار ما يعرف بمقررات بازل والتي اشتملت بالإضافة إلى تعديل قواعد إدارة مخاطر الائتمان، إدخال قواعد جديدة للمخاطر التشغيلية والتي قامت ببلورتها على المستوى الدولي لجنة رعاية المنظمات (The Committee of Sponsoring Organizations) المتكامل للرقابة الداخلية (COSO)، مشيراً إلى انتقال الاهتمام بإدارة المخاطر من مجرد التركيز على الصيغ التقليدية لإدارة المخاطر المالية إلى الاهتمام بالرقابة الداخلية ومخاطر الأعمال ومبادئ الحوكمة، واتخذ هذا الاهتمام صورة إلزامية عام 2002 من خلال إصدار قانون Sarbanes Oxley في الولايات المتحدة. وفي عام 2004 أصدرت

لجنة COSO الإطار المتكامل لإدارة المخاطر المؤسسية (COSO2) والذي يعد نقطة انطلاق لتطور مفهوم إدارة المخاطر المؤسسية. (Abd-Elma geed, 2024)

## 7.2.2 تطور مفهوم إدارة المخاطر

ويرى أن معظم وظائف إدارة المخاطر كانت تمارس بشكل أو بآخر قبل ظهور مفهوم إدارة المخاطر الحديثة، وأن مفهوم إدارة المخاطر قد جاء ليجمع كل هذه الوظائف تحت عنوان واحد، وليس هذا فحسب؛ بل أن إدارة المخاطر ساهمت في تحقيق اندماج تفاعلي بين كل وظائفها، وذلك ضمن استراتيجية موحدة قائمة على موقف شامل من الأخطار التي تواجهها المنظمة. (الخريج، 2022)

ويشير إلى أن إدارة المخاطر أصبحت جزءاً لا يتجزأ من عمليات المنظمة، والتي تهتم بتحديد وتحليل المخاطر والاستجابة لها وتقييمها والتخطيط لإدارتها، وبذلت جهوداً معرفية واسعة وشاملة لتطوير مدخل تكاملي لإدارة المخاطر، حتى أصبح يعد مفهوماً منهجياً منظماً ومدخل متكامل وإطار عام لا يتجزأ من استراتيجية المنظمة بهدف حمايتها من المخاطر التي قد تتعرض لها. (Ramdani, 2024)

\*ولهذا يمكن القول إن إدارة المخاطر ارتبطت بالتطورات التاريخية المختلفة منذ عصور البداية إلى أن وصلت إلى ما هو عليه الآن.

## 8.2.2 مفهوم إدارة المخاطر السيبرانية

تم تناول مفهوم إدارة المخاطر السيبرانية بطرق مختلفة، إلا أنها ترتبط بفكرة واحدة في أن إدارة المخاطر تتعلق بالمخاطر الناتجة عن الهجمات السيبرانية على الشبكات سواء على المؤسسات الحكومية أو الخاصة؛ حيث عُرفت بأنها التقنيات والممارسات والسياسات التي تعالج التهديدات أو نقاط الضعف في الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات المتدفقة أو التي تم تمكينها عن طريق الاتصال الرقمي أو أنظمة المعلومات أو أنظمة التحكم الصناعية، بما في ذلك على سبيل المثال لا الحصر، أمن المعلومات المعلومات الضمان، وضمان الأجهزة والبرامج وعرفت بأنها منهج علمي للتعامل مع المخاطر الإلكترونية من

خلال توقع الخسارة، وتصميم وتنفيذ إجراءات من شأنها أن تخفف إمكانية حدوث الخسائر. (الطاهات، 2023)

وعرفها آخر بأنها إجراء منظم للتخطيط السليم لتحديد وتحليل الاستجابة السريعة ومتابعة المخاطر المحتملة، بما في ذلك الوسائل والإجراءات والتقنيات التي تهدف إلى تحقيق نتائج إيجابية. (Metwally, 2022)

### كما بين أن إدارة المخاطر السيبرانية تتضمن الآتي:

1. جمع المعلومات والبيانات عن الأصول الخطرة بالمنظمة.
2. تحديد التهديدات والتحديات المختلفة.
3. معرفة مواطن الضعف والخلل في التقنيات والأجهزة الإلكترونية.
4. تحديد الخسائر التي يمكن أن تتعرض لها المنظمة.
5. معرفة الوسائل والأدوات البديلة التي يمكن الاعتماد عليها لتلافي وتخفيف الخسائر.
6. تحديد الوسائل والأدوات التي سوف يتم الاعتماد عليها في إدارة المخاطر السيبرانية.

وتعتمد إدارة المخاطر السيبرانية على العديد من الآليات والأدوات التي من شأنها أن تجعل المؤسسة قادرة على حسن التعامل مع المخاطر التي يمكن أن تواجهها، مما يتيح لها حسن الاستعداد للاستجابة المناسبة لها، من خلال الاستشراف لآليات صياغة السيناريوهات المحتملة، وبالتالي صياغة الخطط المفترضة لذلك، أو تلك الطوارئ المتتبعة للمخاطر المفاجئة والتي تفترض من المؤسسة اليقظة الدائمة للتصرف في المتغيرات التي يمكن أن تنتج عن مكونات البيئة الخارجية والداخلية، فكلما كانت إدارة المخاطر السيبرانية في المؤسسة يقظة ومكتسبة للخبرة والكفاءة في التعامل الجيد مع المخاطر المحتملة والطارئة، كان تحصين الأهداف الاستراتيجية والتكتيكية والتشغيلية فيها أكثر نجاعة، بما يرفع مستوى مقدرتها على تلافي المخاطر. (Badawy, 2021)

بناءً على ما تقدم نستنتج ما يلي:

1. تتضمن إدارة المخاطر السيبرانية تنفيذ معايير الأمان في القطاعين العام والخاص في حال التعرض للهجمات السيبرانية والإلكترونية.
2. تعتمد على تحديد وتحليل المخاطر السيبرانية ودراستها بشكل منتظم.
3. منهج علمي متكامل في مواجهة المخاطر والتهديدات السيبرانية.
4. تعتمد إدارة المخاطر السيبرانية على قياس وتقييم المخاطر التي تتعرض لها المنظمة، أو من المحتمل التعرض لها، وفق إستراتيجيات تخطيطية.

## 9.2.2 أهمية إدارة المخاطر السيبرانية

تعتمد إدارة مخاطر الأمن السيبراني عادة على تحليل المخاطر الذي يحسب مخاطر الأمن السيبراني بناءً على معادلة المخاطر العامة التي تنص على ما يلي: مخاطر = عواقب الهجوم × احتمال الهجوم ويشير إلى أن أهمية إدارة المخاطر السيبرانية بما يلي:

1. تسهم إدارة المخاطر السيبرانية في صياغة رؤية واضحة للتعرض للمخاطر المحتملة عبر المؤسسة بأكملها.
2. تجنب الخسائر التي قد تتعرض لها المؤسسة من الهجمات السيبرانية، وتقليل الأثر المالي في حالة انتهاك البيانات.
3. تساعد في تعزيز ثقافة الأمن السيبراني.

ويمكن تحديد أهمية إدارة المخاطر السيبرانية بالآتي:

1. اكتشاف الخطر، والتعرف على أسبابه.
2. تقييم وتحليل أثر الأخطار على المنظمة ومعالجتها.
3. قياس الأخطار الحالية، والتنبؤ بالأخطار المستقبلية، والاستعداد والوقاية منها.
4. تفعيل الإجراءات الاحترازية والوقائية للحد من الأخطار السيبرانية، وتوفير بيئة آمنة في المنظمة.
5. إنذار المبكر وتفعيل نظام الرقابة حتى يتسنى التنبؤ بالمخاطر قبل وقوعها.

6. اختيار الطرق والأساليب المناسبة للتعامل مع الأخطار.

ذا تركز المنظمات بشكل متزايد على تحديد المخاطر السيبرانية وإدارتها قبل أن تؤثر عليها؛ حيث تساعد القدرة على إدارة المخاطر المنظمات على التصرف بثقة أكبر في اتخاذ القرارات المستقبلية، وأن معرفتهم بالمخاطر التي يواجهونها ستمنحهم خيارات مختلفة حول كيفية التعامل مع المشاكل المحتملة كما تحتاج المنظمات إلى إنشاء وتنفيذ إستراتيجية لإدارة المخاطر السيبرانية للتخفيف والقضاء على تهديدات الهجمات السيبرانية؛ حيث يمكن أن تساعد إستراتيجية إدارة المخاطر السيبرانية صانعي القرار على تحديد احتمالية التعرض لأي هجمات سيبرانية. (الخرينج، 2022)

## 10.2.2 مراحل إدارة المخاطر السيبرانية (الابعاد)

اجتهد علماء الإدارة وبعض الجهات الدولية والمهتمة بإدارة المخاطر بتقديم إطار كامل وشامل لمفهوم إدارة المخاطر، من خلال دراسة أهمية وأهداف وطبيعة ومعايير إدارة المخاطر، حيث كان هنالك شبه اتفاق على أبعاد أو مراحل إدارة المخاطر، وهنا نشير (The Committee of Sponsoring Organizations إلى لجنة رعاية المنظمات ((COSO)، والمنظمة الدولية للمعايير، ومعهد إدارة المخاطر بالإضافة إلى أهم، (The Institute of Risk Management (IR) البريطاني العلماء والباحثين الذين تناولوا المفهوم وبنيت على أساسها جميع الدراسات اللاحقة. (Elqadi, 2024)

### البعد الأول: تحديد المخاطر السيبرانية

تُعَدُّ عملية تحديد المخاطر المرحلة الأولى في إدارة المخاطر؛ لأنها القاعدة في تبني إدارة المخاطر وتؤسس لجميع المراحل اللاحقة؛ حيث تتمثل في عملية العثور والكشف عن المخاطر والتعرف عليها وتسجيلها، وذلك لتحديد ما قد يحدث أو المواقف المحتملة التي قد تؤثر في تحقيق أهداف المنظمة وفي هذه المرحلة يتم التعرف على المخاطر ذات الأهمية؛ حيث تتم عملية تقييم مخاطر المنظمة وترتيبها حسب الأولوية، وتوفر مدخلات عالية الجودة لصانعي القرار لمساعدتهم على صياغة استجابات فعالة للمخاطر، بما في ذلك معلومات حول الحالة الحالية للقدرة حول إدارة المخاطر ذات الأولوية. (Metwally, 2022)

ويرى أن عملية تحديد المخاطر يمكن أن تؤثر في تحقيق أهداف المنظمة، فالمخاطر المحتملة قد تمثل تهديداً يعيق تحقيق الأهداف، أو أنها تمثل فرصة تدعم تحقيق الأهداف، وقد تكون تهديداً أو فرصة معاً، وهنا لابد أن يتم تحديد المؤثرات من بيئة العمل الداخلية وبيئة العمل الخارجية. Abd-Elmageed, (2024)

كما لابد أن تتم عملية تحديد المخاطر بأسلوب منهجي وذلك لضمان تعريف جميع الأنشطة الهامة للمنظمة وتعريف الأخطار الناجمة عن تلك الأنشطة، كما يجب تحديد التغيرات المصاحبة لتلك الأنشطة وتصنيفها حسب أهميتها. (الرحماوي، 2024)

### ولتحديد المخاطر بشكل إيجابي يجب مراعاة ما يلي:

1. مشاركة أفراد لديهم المعارف اللازمة في المسألة، فتحديد المخاطر يتطلب معرفة السياق الداخلي والخارجي للمنظمة، وفي حال عدم إلمام فريق عمل إدارة المخاطر بهذه المعطيات يجب مشاركة خبراء لديهم المعرفة الشاملة بمعطيات بيئة العمل.
2. استمرارية عملية تحديد المخاطر؛ لتصبح نشاطاً دائماً في المسار التنظيمي للمؤسسة؛ إذ إن تحديد المخاطر لا ينتهي بمجرد إعداد خطة للمنظمة، فقد تظهر المخاطر في أي مرحلة من مراحل العمل.
3. اشتراك أعضاء الفريق في تحديد المخاطر؛ حتى يشعر كل فرد منهم بأنه مسؤول في هذه العملية.

### ويمكن التعرف على المخاطر من خلال ما يلي:

1. التحديد المعتمد على الأهداف: تهدف المنظمة من وجودها تحقيق أهداف معينة حسب خطط معينة، وأي حدث يمكن أن يعرض هذا الهدف إلى خطر سواء جزئياً أو كلياً يُعد خطورة.
2. التحديد المعتمد على السيناريو خلال عملية تحليل السيناريو يتم خلق سيناريوهات مختلفة قد تكون طرقاً بديلة لتحقيق هدف ما أو للتفاعل بين القوى وإن أي حدث يولد سيناريو مختلف عن الذي تم تصوره وغير مرغوب فيه، يعرف على أنه خطورة.
3. التحديد المعتمد على التصنيف: يتم تفصيل جميع المصادر المحتملة للمخاطر.

4. مراجعة المخاطر الشائعة في العديد من المنظمات هنالك قوائم بالمخاطر المحتملة.

وتشمل عملية تحديد المخاطر تحديد أسباب ومصدر الخطر، ويمكن أن تتضمن طرق تحديد

المخاطر ما يلي:

1. الأساليب القائمة على الأدلة مثل: قوائم التحقق مراجعة البيانات التاريخية.
2. منهج مقاربات الفريق؛ حيث يتبع الفريق عملية منهجية لتحديد الخطر من خلال مجموعة منظمة من الأسئلة أو الاستشارات.
3. تقنيات الاستقراء المنطقي؛ مثل دراسات الخطر، كما يمكن استخدام تقنيات دعم مختلفة لتحسين الدقة والاكتمال في تحديد المخاطر، بما في ذلك العصف الذهني والمسوح واستقصاء الرأي ومنهجية (الخبراء).

كما يمكن تحديد المخاطر باستخدام خطة إدارة مخاطر متكاملة منظمة كجزء من تقييم

للمخاطر، على أن تتضمن ما يلي:

1. تحديد الأفراد المشاركون في تحديد المخاطر.
2. مدى الدقة المطلوبة للأنشطة معينة لتحديد المخاطر.
3. نوع البيانات التي يتعين جمعها.
4. توثيق المخاطر التي تم تحديدها لأغراض تقييم المخاطر.

ويشير يمكن أن يختلف ويتنوع المشاركون في تحديد المخاطر، ولكن من الضروري وجود فريق الإدارة التنفيذي، الذي يكون تعامله يوميا مع سير العمل داخل المؤسسة ويحتاج إلى معلومات جديدة في أي وقت، كما أنه من الضروري تأمين المعلومات من الخبراء والجهات المعنية الخارجية فيما يتعلق بتعريف المخاطر الممكن وقوعها. (Ramdani, 2024)

ومن الأخطاء الشائعة في مرحلة تحديد المخاطر التركيز على الأهداف وليس على الأحداث التي من الممكن أن تؤدي إلى نتائج سلبية، كما تتطلب عملية تحديد المخاطر جهداً تدريبياً، وعملية إعادة من طرف

كل أفراد الفريق حتى إجاد الآليات المستوجبة، ويكون ذلك خلال برامج أنشطة أسبوعية وشهرية وسنوية لتحقيق الغرض من إدارة المخاطر. (موسى، 2023)

مما سبق يرى الباحث أن مرحلة تحديد المخاطر السيبرانية عملية منهجية مستمرة تهتم بجمع المعلومات الأساسية والتعرف على كافة المخاطر التي قد تتعرض لها الأنشطة أو الأنظمة المستخدمة داخل المنظمة، وما تتضمنه من بيانات ومعلومات، في حال وجود تهديدات أو هجمات سيبرانية، من خلال طرق وأساليب تساهم بشكل كبير في التعرف على تلك المخاطر، وأن هذه الطرق إذا أدمجت معاً ستساهم بشكل كبير في مساعدة مدراء المخاطر وفريق عمل إدارة المخاطر. (Badawy, 2021)

### البعد الثاني: تحليل المخاطر السيبرانية

تتمثل عملية تحليل المخاطر في معرفة نقاط الضعف في المنظمة، ويمكن قياس أي ثغرة أمنية من خلال بعدين يتمثلان باحتمال وقوع الخطر ودرجة أثره؛ حيث يتضمن تحليل المخاطر بشكل عام تخصيص وتصنيف شامل للمخاطر ويقصد بتحليل المخاطر درجة وحجم اتساع أثر الخطر المحتمل، أي يتم إجراء ترتيب الاخطار حسب معدل تكرارها ودرجة تأثيرها على أهداف المنظمة، كما تتضمن عملية تحليل المخاطر النظر في أسباب ومصادر الخطر واحتمال حدوث تلك الآثار، وينبغي تحديد العوامل المؤثرة في النتائج والاحتمالات، فالحدث يمكن أن تكون له آثار متعددة ويمكن أن يؤثر في أهداف متعددة. (الطاهات، 2023)

وتحتاج كل منظمة إلى فهم المخاطر المرتبطة بأنظمة المعلومات الخاصة بها الحماية أصول تكنولوجيا المعلومات الخاصة بها بفعالية وكفاءة، ويمكن لتحليل المخاطر أن يساعد المنظمة على تحسين أمنها بعدة طرق، وهي:

1. فيما يتعلق بالتأثيرات المالية والتنظيمية، فإنه يحدد ويصنف ويقارن التأثير العام للمخاطر المتعلقة بالمنظمة.
2. يساعد على تحديد الثغرات في أمن المعلومات وتحديد الخطوات التالية للقضاء على مخاطر الأمن.
3. يعزز عمليات الاتصال وصنع القرار المتعلقة بأمن المعلومات.

4. يعمل على تحسين السياسات والإجراءات الأمنية، إضافة إلى تطوير أساليب فعالة من حيث التكلفة لتنفيذ سياسات وإجراءات أمن المعلومات.

5. يزيد من وعي الموظفين بالمخاطر والتدابير الأمنية أثناء عملية تحليل المخاطر وفهم الآثار المالية للمخاطر الأمنية المحتملة.

### ويشير أن عملية تحليل المخاطر تتضمن نوعان من المهام:

1. قياس المخاطر أو تقديرها يتطلب هذا النوع دراسة وتحليل تاريخ المخاطر لتسهيل عملية تقدير أثرها المحتمل ومعدل تكرارها، ويتم القياس لأثر المخاطر ذات الطبيعة الكمية أو التي يمكن قياسها بمقياس كمي أو رقمي، أما التقدير فيختص بالمخاطر ذات الطبيعة النوعية والتي يكون أثرها رهناً بتقدير المختصين والباحثين.

2. التنبؤ بالمخاطر: يتم الاعتماد في هذا النوع على السيناريوهات التي يتم تصميمها للتعامل مع احتمالات للخسارة لم تحدث من قبل، حيث يمكن أن تساعد على بلورة حلول الأحداث لم يسبق حدوثها من قبل، ويمكن الاعتماد على أساليب ونماذج إحصائية وقياسية عديدة لتنبؤ بالمخاطر كمنهجية مونت كارل والذي يعتمد أسلوب السيناريوهات.

ويتطلب قياس الخطر وضع مقياس لكل من احتمال وقوع الخطر والأثر المتوقع ويشير تقرير وحدة التفتيش المشتركة للأمم المتحدة بجنيف (2010) أنه عند القيام بتقدير احتمال وقوع الخطر وتأثيره خلال عملية تحليل المخاطر ينبغي إجراء تقدير لكل واحد من المخاطر لتحديد مستوى أو أهمية الخطر، وأن يكون لكل من احتمال وقوع الخطر وتأثيره ومستواه فئات أو مقاييس، وذلك لاستخدامها لاحقاً في عملية تقييم المخاطر، وأنه من المهم تطبيق تلك الفئات على كل مخاطر المنظمة لكي يكون التقييم متسقاً وقابلاً للمقارنة. (الخرينج، 2022)

ويشير أن تحليل مخاطر الأمن السيبراني تتمثل في التحليل النوعي والكمي:

1. التحليل النوعي للمخاطر: تُعد عملية التحليل النوعي للمخاطر السيبرانية تقنية الإدارة أصول المنظمة؛ حيث تعطى الأولوية للمخاطر من خلال تعيين احتمالية الخطر ودرجة التأثير، وتهدف عملية التحليل النوعي للمخاطر إلى تقييم خصائص المخاطر المحددة بشكل فردي ومن ثم ترتيبها حسب الأولوية بناءً على الخصائص المتفق عليها، كما يستخدم التحليل النوعي لتحديد مدى تعرض المنظمة للمخاطر من خلال الاحتمالية  $\times$  التأثير.

2. التحليل الكمي للمخاطر: يتعلق التحليل الكمي للمخاطر السيبرانية بتقديرًا رقميًا للتأثير الكلي للمخاطر على أهداف المنظمة؛ حيث يتم تقييم احتمالية النجاح في تحقيق أهداف المنظمة، وتقدير احتياطي الطوارئ، وعادة ما ينطبق على الوقت والتكلفة، ويسهم التحليل الكمي للمخاطر السيبرانية في حساب تقديرات المخاطر الكلية للمنظمة والتي هي محور التركيز الرئيسي.

ومن الأساليب والمنهجيات الكمية التي يمكن الاعتماد عليها في قياس المخاطر منهجية وتتضمن ثلاثة أساليب لقياس الخطر أسلوب مونت كارلو، الأسلوب الإحصائي الأسلوب الحدسي، تحليل الشجرة، تحليل المجموعة الغامضة، التوزيع الطبيعي، أما أساليب والطرق النوعية فتتضمن تحليل شجرة الفشل، مصفوفة الاحتمال والتأثير، تحليل السبب والنتيجة تقنية دلفي العصف الذهني، آراء الخبراء، تحليل قوائم المراجعة وغيرها من الأساليب ونماذج، كما أنه من المستحسن بشكل كبير اتباع نهج متكامل لتحليل المخاطر، والجمع بين الأساليب الكمية والنوعية. (Abd-Elmageed, 2024)

ويرى أن تحليل المخاطر السيبرانية في أي منظمة ينطوي على:

1. توقع وتقليل تأثير النتائج الضارة الناتجة عن الهجمات السيبرانية.
2. التخطيط إلى عدم قدرة التكنولوجيا أو المعدات على مواجهة الهجمات السيبرانية.
3. تقييم ما إذا كانت المخاطر المحتملة متوازنة في عملية اتخاذ القرار.
4. تحديد تأثير المخاطر السيبرانية، والاستعداد للتغيرات البيئية في المنظمة.

ويرى الباحث أن مرحلة تحليل المخاطر السيبرانية هي عملية توفر الأساس لتقييم المخاطر والقرارات المتعلقة بمعالجة المخاطر عن طريق فهم طبيعة المخاطر وتحديد مستوى الخطر، من خلال

قياس أو تقدير احتمال وقوع الخطر وتأثيره باستخدام منهجيات وأساليب كمية ونوعية. Metwally, (2022)

### البعد الثالث: تقييم المخاطر السيبرانية

يعتبر تقييم المخاطر نهج أساسي في إدارة المخاطر السيبرانية حيث يحدد درجة ومستوى المخاطر التي قد تتعرض لها المنظمة نتيجة الهجمات والتهديدات السيبرانية، ما يسمح لها بتطوير الحلول المستخدمة للتقليل من الآثار السلبية لهذه التهديدات وبأقل التكاليف وبالتالي فإنه يتوجب لإدارة مخاطر الأمن السيبراني بشكل فعال تقييم مخاطر الأمن السيبراني والتي تعتبر جزءاً لا يتجزأ من عملية إدارة مخاطر بالمنظمة. (Ramdani, 2024)

وتهدف عملية تقييم المخاطر السيبرانية في تقدير مستوى المخاطر التي قد تتعرض لها المنظمة وتأثيرها على خدماتها وعملياتها الأساسية، كما تهدف إلى تحديد التدابير والإجراءات التي تخفف من آثارها، وذلك من خلال التخطيط لها وتصميمها ويتم تنفيذها في المنظمة لحماية أرواح الناس وتقليل الأضرار التي تلحق بالممتلكات ضد التهديدات المحتملة. (Badawy, 2021)

وتُعرف عملية تقييم المخاطر بأنها التحليل المتكامل للمخاطر التي يمكن أن تحدث، وذلك من خلال العديد من الإجراءات والمراحل، والتي تهدف للكشف المبكر عن المخاطر، وذلك لضمان الإدارة الفعالة في المستقبل. (موسى، 2023)

ويشير أن منهجية تقييم المخاطر السيبرانية هي تجميع نتائج التهديد وتقييم نقاط الضعف وتقييم الأثر وذلك لتحديد القيمة الرقمية للمخاطر لكل أصل ومجموعة. (شرف، 2023)

ويوضح تقرير وحدة التفتيش المشتركة للأمم المتحدة بجنيف (2010) أن عملية تقييم المخاطر تساعد على ترتيب المخاطر بحسب الأولوية بالنسبة للمنظمة والتوصل واتخاذ القرارات بشأن معالجة المخاطر استناداً إلى مقارنة نتائج عملية تحليل المخاطر ومعايير تقدير أثرها، وتحديد ما إذا كان الخطر يجب قبوله أو معالجته. وهنا فإنه من المهم أن تحدد المنظمات فئات لقياس احتمال وقوع المخاطر ومعايير

لتقدير أثرها، بما في ذلك الحدود القصوى لتحمل / قبول المخاطر، وتستطيع المنظمات أن تستخدم ثلاث فئات لتقييم احتمال وقوع المخاطر وتأثيرها كمستوى مرتفع أو متوسط أو منخفض وتمثيلها بمصفوفة 33، بينما قد تجد منظمات أخرى أن استخدام خمس فئات لتقييم وتمثيلها بمصفوفة 55 يعطيها تقييم أفضل، وفيما يتعلق بمستوى المخاطر، تستخدم المنظمات فئات مماثلة أو مختلفة وحسب الأنسب لطبيعة وظروف عملها؛ ومع ذلك يستحسن استخدام المزيد من الفئات في التصنيف وتحديد الأولويات، وذلك حتى لا تتركز المخاطر في فئة واحدة، الأمر الذي قد يتطلب إجراء المزيد من المراجعة وتحديد الأولويات. (Abd-Elmageed, 2024)

وتعد مصفوفة المخاطر أو خريطة الحرارة والموضحة في الشكل رقم (7) من بين أكثر الطرق شيوعاً وأبسطها لتقييم المخاطر حيث أنها توفر نوع من العرض المرئي والذي غالباً ما يعد ضروري للاتصال بالإدارة العليا، وخلالها تحدد فئات مستوى المخاطر على أنها منخفضة الخطورة أو متوسطة الخطورة أو عالية الخطورة وحسب التصنيف الأنسب للمنظمة، وتكون حصيلة التقدير أو نقطة تقاطع التأثيرات والعلامات الدالة على احتمالات. (شرف، 2023)

#### البعد الرابع: الاستجابة للمخاطر السيبرانية

تتعلق مرحلة الاستجابة للمخاطر السيبرانية في تحديد الاستجابة للمخاطر المحتملة ووضع الاستراتيجيات الممكنة، والخطط التنفيذية للحد من المخاطر المحتملة أو احتمالية حدوثها. Metwally, (2022)

وعرّفت بأنها عملية تطوير الخيارات والفرص المتاحة، وتحديد الإجراءات التي من شأنها أن تعزز الفرص وتقلل من التهديدات، وعادة يتم تعيين شخص واحد يتولى مسؤولية كل استجابة تم الاتفاق عليها وتم تمويلها لمواجهة المخاطر. (Elqadi, 2024)

وهناك خطوات أساسية للاستجابة للمخاطر تتمثل في الآتي:

1. منع المخاطر: تعني تجنب المخاطر أو تغيير في العمليات المقترحة لمنع حدوث المخاطر.

2. التحكم بالمخاطر: وتعني التخفيف من احتمالية وتأثير المخاطر، والتي تتضمن وضع الاستراتيجيات والإجراءات التي تهدف إلى التحكم والسيطرة على المخاطر في حال حدوثها، والتقليل من آثارها إلى الحد المعقول.

3. تحويل المخاطر: من خلال نقل المخاطر إلى جهات أخرى أكثر قدرة على إدارتها.

4. قبول المخاطر: أي الرغبة في قبول المخاطر ومواجهتها بالوسائل المتاحة.

#### البعد الخامس: التحكم بالنشاطات

تشمل أساليب التحكم في النشاطات، والابتعاد عن المخاطرة، إضافة إلى منع حدوث الخسائر ومجهودات الرقابة والتحكم والوقاية وعرف التحكم بالنشاطات بأنها عملية تنفيذ خطط الاستجابة للمخاطر وتعقب المخاطر التي تم اكتشافها ومراقبة المخاطر المتبقية، والتعرف على مخاطر جديدة وتقييم فعالية المخاطر في مختلف الجوانب. (الطاهات، 2023)

ويعرف عملية التحكم بالنشاطات بأنها السياسات والإجراءات التي تتخذها المنظمة على جميع المستويات والمهام للمساعدة في ضمان تنفيذ الاستجابات للمخاطر بشكل فعال. (موسى، 2023)

ويعرفها أنها مجموعة من الإجراءات والتعليمات التي يتم تنفيذها لضمان اخراج سياسات الرد على المخاطر إلى حيز الوجود، والاستعداد لمواجهة المخاطر بالشكل الأمثل والاستفادة من الفرص وتقليل التهديدات. (Metwally, 2022)

ويشير أن التحكم بالنشاطات يحقق التحكم والسيطرة على الخطر لمنع أو التقليل من آثاره من خلال معرفة سمات ومظاهر الخطر، وتقييم درجة المخاطرة ومتابعتها للتعديل والتغيير؛ حيث يؤدي تحليل المخاطر التحكم في أي مخاطر يمكنها أن تحدث أضراراً مختلفة. (الخرينج، 2022)

ويتم التحقق من قدرة التحكم بالنشاطات من خلال القيام بعمليات التقييم والقياس والأسلوب الأمثل للتحكم بالنشاطات هي التغذية الراجعة، وذلك من خلال السجلات والتقارير الدقيقة. Badawy,

(2021)

## الفصل الثالث: منهجية وإجراءات الدراسة

### مقدمة

يتناول هذا الفصل الدراسة الميدانية وذلك من خلال التعرف على منهجية الدراسة ومجتمع وعينة الدراسة وأداة الدراسة ومصادر جمع البيانات والأساليب الإحصائية المستخدمة في الدراسة وحساب الصدق والثبات لأداة الدراسة

### 1.3 منهجية البحث

نظرا لطبيعة الدراسة التي تهدف إلى التعرف على أثر الابتكار التكنولوجي على إدارة المخاطر السيبرانية تم استخدام المنهج الوصفي التحليلي حيث استخدمنا في الجانب النظري المنهج الوصفي الذي يعمل على توضيح متغيرات الدراسة، مع استخدام المنهج التحليلي في الدراسة الميدانية لأنه يعمل على التحليل والربط بين النتائج التي توصل إليها ويعمل على تفسيرها ثم إصدار الأحكام المناسبة.

### 2.3 مجتمع وعينة الدراسة

تمثل مجتمع الدراسة في جميع العاملين في المؤسسات المالية في المملكة العربية السعودية ونتيجة لصعوبة إجراء الحصر الشامل لكافة أفراد مجتمع الدراسة فقد قامت الدراسة باستخدام أسلوب العينات العشوائية البسيطة من خلال نشر الرابط الخاص بالاستبيان على كافة مواقع التواصل الاجتماعي الخاصة بأفراد مجتمع الدراسة وقد بلغ عدد أفراد عينة الدراسة 364 فرد وهم الذين أجابوا على استئلة استمارة الاستبيان.

### 3.3 مصادر جمع البيانات:

اعتمدت الدراسة على المصادر التالية في جمع البيانات والمعلومات:

- المصادر الثانوية: قام الباحث بالرجوع إلى الكتب والمراجع العربية والأجنبية ذات العلاقة، والدوريات والأدبيات والتقارير والأبحاث والدراسات السابقة التي تتناول موضوع الدراسة والبحث في مواقع الإنترنت المختلفة لتقديم الإطار النظري المتعلق بهذه الدراسة.
- المصادر الأولية: قام الباحث بإعداد استبانة كأداة رئيسية لجمع البيانات مباشرة من أفراد العينة، حيث تكونت من عدد من الفقرات بهدف التعرف على أثر الابتكار التكنولوجي على إدارة المخاطر السيبرانية بالملكة العربية السعودية

#### 4.3 الأساليب الإحصائية:

تم الاعتماد على برنامج الحزم الإحصائية (SPSS) للوصول إلى الأهداف المرسومة حيث يحتوي على مجموعة من الاختبارات الإحصائية التي تندرج تحت الإحصاء الوصفي والإحصاء الاستدلالي. وفيما يلي مجموعة من الأساليب الإحصائية التي استخدمت في الدراسة.

- ✓ التكرارات والنسب المئوية: تم استخدامها للتعرف على خصائص أفراد الدراسة
- ✓ اختبار معامل ألفا كرونباخ: تم استخدامه لتحديد ثبات أبعاد الاستبيان.
- ✓ معامل ارتباط بيرسون: تم استخدامه لتحديد مدى اتساق كل فقرة مع البنود الكمية للاستبيان والأبعاد التي ينتهي إليها (الاتساق الداخلي لأداة الاستبيان).
- ✓ المتوسط الحسابي والانحراف المعياري: وذلك لتحديد أهمية السؤال من بين الأسئلة المطروحة.
- ✓ اختبار الانحدار البسيط: تم استخدامه لتحديد تأثير المتغير المستقل على المتغير التابع.

#### 5.3 أداة الدراسة

اعتمدت الدراسة على الاستبانة كأداة لجمع البيانات وتكونت الاستبانة من ثلاث محاور على

النحو التالي:

تم العمل على الاستبانة للتناسب مع متغيرات الدراسة من خلال الاطلاع على الدراسات السابقة

المتعلقة بموضوع الدراسة، حيث تكونت من قسمين رئيسيين هما:

- **القسم الأول:** وهو الجزء الخاص بالمتغيرات الديمغرافية لأفراد عينة الدراسة والمتمثلة بـ: النوع، والعمر، والمؤهل العلمي والمسمى الوظيفي، الخبرة المهنية.
  - **القسم الثاني:** اشتمل القسم الثاني على الفقرات والأبعاد التي تقيس متغيرات الدراسة المستقل والتابع وتتضمن فقرات المتغير المستقل (الابتكار التكنولوجي) وتتضمن أربع أبعاد وهي (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) وتشتمل على 20 فقرة وفقرات المتغير التابع (إدارة المخاطر السيبرانية) ويتضمن 5 فقرات
- وتم استخدام مقياس ليكرت ذو الخمس درجات في الإجابة على أسئلة محاور الدراسة، وقد قامت الدراسة بتقسيم اتجاه موافقة أفراد عينة الدراسة على عبارات محاور الدراسة إلى مستويات.

**جدول (1) مستويات موافقة عينة الدراسة على عبارات أداة الدراسة**

| الدرجة      | المستوي    |
|-------------|------------|
| 1 – 1.79    | منخفضة جدا |
| 1.80 – 2.59 | منخفضة     |
| 2.60 – 3.39 | متوسطة     |
| 3.40 – 4.19 | مرتفعة     |
| 4.20 – 5.00 | مرتفعة جدا |

### 6.3 صدق أداة الدراسة

تم حساب صدق عبارات استمارة الاستبيان عن طريق تحديد مستوى التجانس الداخلي من خلال التعرف على الدلالة الإحصائية لمعاملات الارتباط بيرسون بين درجة العبارة والدرجة الكلية للمحور الذي تنتهي إليه العبارة وجاءت النتائج كما يلي:

#### ■ المحور الأول: الابتكار التكنولوجي

جدول (2) معاملات الارتباط لعبارات المحور الأول

| م                          | العبارة                                                                                                                         | معامل ارتباط<br>بيرسون | Sig   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------|-------|
| البنية التحتية التكنولوجية |                                                                                                                                 |                        |       |
| 1                          | تستخدم المؤسسات المالية السعودية في المملكة العربية السعودية شبكات الاتصال الإلكترونية لمتابعة وتقييم العمل اليومي              | **0.568                | 0.000 |
| 2                          | استفادت المؤسسات المالية السعودية في المملكة العربية السعودية من التقنيات الحديثة للاتصالات                                     | **0.740                | 0.000 |
| 3                          | ساهمت تكنولوجيا المعلومات في سهولة الاتصالات بين المؤسسات المالية السعودية في المملكة العربية السعودية                          | **0.624                | 0.000 |
| 4                          | تتوافر بالمؤسسات المالية السعودية في المملكة العربية السعودية المعدات والتقنيات اللازمة في مجال تكنولوجيا المعلومات             | **0.602                | 0.000 |
| 5                          | ساهمت تكنولوجيا المعلومات في زيادة قدرة المؤسسات المالية السعودية في المملكة العربية السعودية على تحقيق أهدافها                 | **0.606                | 0.000 |
| البرمجيات والتصميمات       |                                                                                                                                 |                        |       |
| 6                          | تتوافر في المؤسسات المالية السعودية في المملكة العربية السعودية أنظمة حماية آلية متطورة لحماية بياناتها                         | **0.552                | 0.000 |
| 7                          | تستخدم المؤسسات المالية السعودية في المملكة العربية السعودية البرامج والتطبيقات السياحية الإلكترونية                            | **0.654                | 0.000 |
| 8                          | تناسب البرمجيات المستخدمة في المؤسسات المالية السعودية في المملكة العربية السعودية مع نظام العمل لتقديم الخدمات السياحية بسهولة | **0.726                | 0.000 |

|                  |                                                                                                                                       |       |         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|---------|
| 9                | يوجد بالمؤسسات المالية السعودية في المملكة العربية السعودية<br>نظام رقابي إداري إلكتروني                                              | 0.000 | **0.685 |
| 10               | تمتلك المؤسسات المالية السعودية في المملكة العربية السعودية<br>ميزانية كافية لتوفير الأجهزة والمعدات التكنولوجية وتحديثها<br>باستمرار | 0.000 | **0.523 |
| الخدمات المبتكرة |                                                                                                                                       |       |         |
| 11               | تعمل المؤسسات المالية السعودية في المملكة العربية السعودية<br>على الابتكار في تقديم الخدمات للعملاء                                   | 0.000 | **0.739 |
| 12               | تحرص ادارة المؤسسات المالية السعودية العاملة في المملكة<br>العربية السعودية على تحديث تجهيزاتها والياتها باستمرار.                    | 0.000 | **0.603 |
| 13               | تحرص المؤسسات المالية السعودية العاملة في المملكة العربية<br>السعودية على أن تتلاءم التكنولوجيا المستخدمة مع متطلبات<br>العمل         | 0.000 | **0.563 |
| 14               | تحرص المؤسسات المالية السعودية العاملة في المملكة العربية<br>السعودية على تدريب العاملين على استخدام التقنيات الحديثة<br>وباستمرار.   | 0.000 | **0.509 |
| 15               | تهتم المؤسسات المالية السعودية العاملة في المملكة العربية<br>السعودية بتبني الأساليب التكنولوجية الحديثة في مجال العمل                | 0.000 | **0.459 |
| التفاعل والتواصل |                                                                                                                                       |       |         |
| 16               | تركز المؤسسات المالية السعودية العاملة في المملكة العربية<br>السعودية على التكنولوجيا الحديثة بما يتلاءم وحاجات ورغبات<br>العملاء.    | 0.000 | **0.668 |

|    |                                                                                                                                 |         |       |
|----|---------------------------------------------------------------------------------------------------------------------------------|---------|-------|
| 17 | تقوم المؤسسات المالية السعودية العاملة في المملكة العربية السعودية بإجراء تغييرات مستمرة لتطوير خدماتها في ضوء احتياجات العملاء | **0.770 | 0.000 |
| 18 | تمتلك المؤسسات المالية السعودية العاملة في المملكة العربية السعودية قدرة التركيز على العميل في كافة المستويات                   | **0.681 | 0.000 |
| 19 | تعتمد المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تقديم خدمات محددة                                       | **0.568 | 0.000 |
| 20 | تمتلك المؤسسات المالية السعودية العاملة في المملكة العربية السعودية القدرة على مواكبة التغييرات في احتياجات ورغبات العملاء      | **0.590 | 0.000 |

\*\* ذات دلالة احصائية عند 0.01

وتبين أن جميع معاملات الارتباط لجميع عبارات محور الابتكار التكنولوجي كانت ذات دلالة إحصائية عند مستوي معنوية (0.01) وهذا يعني أن عبارات محور الابتكار التكنولوجي تتمتع بصدق الاتساق الداخلي وهي صالحة لأغراض الدراسة.

#### ■ المحور الثاني: إدارة المخاطر السيبرانية

جدول (3) معاملات الارتباط لعبارات المحور الثاني

| م | العبرة                                                                                | معامل ارتباط بيرسون | Sig   |
|---|---------------------------------------------------------------------------------------|---------------------|-------|
| 1 | أعتقد أن وجود سياسة فعالة لإدارة المخاطر السيبرانية يعزز من أمان المعلومات في مؤسستي. | **0.759             | 0.000 |

|   |                                                                                                              |                |       |
|---|--------------------------------------------------------------------------------------------------------------|----------------|-------|
| 2 | أرى أن التدريب المستمر للموظفين حول المخاطر السيبرانية يساهم في تقليل الحوادث الأمنية.                       | <b>**0.738</b> | 0.000 |
| 3 | أعتبر أن استخدام تقنيات الحماية المتقدمة (مثل جدران الحماية وتشفير البيانات) ضروري لحماية المعلومات الحساسة. | <b>**0.824</b> | 0.000 |
| 4 | أؤمن بأن تقييم المخاطر السيبرانية بشكل دوري يساعد في تحسين استجابة المؤسسة للتهديدات المحتملة.               | <b>**0.719</b> | 0.000 |
| 5 | أجد أن التعاون مع جهات خارجية متخصصة في الأمن السيبراني يعزز من قدرة مؤسستي على مواجهة المخاطر.              | <b>**0.749</b> | 0.000 |

**\*\* ذات دلالة احصائية عند 0.01**

وتبين أن جميع معاملات الارتباط لجميع عبارات محور إدارة المخاطر السيبرانية كانت ذات دلالة إحصائية عند مستوى معنوية (0.01) وهذا يعني أن عبارات محور إدارة المخاطر السيبرانية تتمتع بصدق الاتساق الداخلي وهي صالحة لأغراض الدراسة.

### 7.3 ثبات أداة الدراسة:

تم حساب معامل ألفا كرونباخ لعبارات محاور الاستبيان وكانت النتائج كما يلي:

جدول (4) معامل الثبات لمحاور استمارة الاستبيان

| المحاور                  | معامل الفا كرونباخ | عدد العبارات |
|--------------------------|--------------------|--------------|
| الابتكار التكنولوجي      | 0.914              | 20           |
| إدارة المخاطر السيبرانية | 0.815              | 5            |
| إجمالي استمارة الاستبيان | 0.927              | 25           |

يتبين أن قيمة معامل الثبات Alpha أكبر من 0.7 لجميع محاور استمارة الاستبيان مما يؤكد على

صلاحية وارتباط عبارات محاور استمارة الاستبيان وارتفاع مستوى ثبات أداة الدراسة مما يسمح

باستخدام الأداة لغرض الدراسة.

## الفصل الرابع: تحليل النتائج

### مقدمة

سوف نتناول في هذا الفصل تحليل بيانات الدراسة من خلال تحليل استمارة الاستبيان والتعرف على خصائص عينة الدراسة وتحليل محاور الدراسة والاجابة عن أسئلة الدراسة من أجل تحقيق أهداف الدراسة والوصول إلى نتائج وتوصيات للدراسة.

### 1.4 أولاً: خصائص عينة الدراسة

جدول (5) توزيع عينة الدراسة وفقاً لخصائصها

| الخاصية        | الفئات                   | العدد | %    |
|----------------|--------------------------|-------|------|
| الجنس          | ذكر                      | 161   | 44.2 |
|                | أنثى                     | 203   | 55.8 |
| العمر          | أقل من 25 سنة            | 77    | 21.2 |
|                | من 25 الى أقل من 35 سنة  | 105   | 28.8 |
|                | من 35 الى اقل من 45 سنة  | 126   | 34.6 |
|                | 45 سنة فأكثر             | 56    | 15.4 |
| الدرجة العلمية | ثانوي                    | 49    | 13.5 |
|                | بكالوريوس                | 217   | 59.6 |
|                | ماجستير                  | 77    | 21.2 |
|                | دكتوراه                  | 21    | 5.8  |
| الخبرة المهنية | أقل من 5 سنوات           | 133   | 36.5 |
|                | من 5 الى اقل من 10 سنوات | 77    | 21.2 |

|      |     |                               |                |
|------|-----|-------------------------------|----------------|
| 25.0 | 91  | من 10 سنوات الى اقل من 15 سنة | المسمى الوظيفي |
| 19.2 | 70  | 15 سنة فأكثر                  |                |
| 25.0 | 91  | مدير                          |                |
| 9.6  | 35  | نائب مدير                     |                |
| 23.1 | 84  | رئيس قسم                      |                |
| 42.3 | 154 | موظف                          |                |

## 2.4 ثانياً: تحليل استمارة الاستبيان

لتحليل استمارة الاستبيان تم استخدام المتوسطات الحسابية والانحرافات المعيارية لعبارات كل

محور وللمحور ككل وجاءت النتائج كما يلي:

### ■ المحور الأول: الابتكار التكنولوجي

#### 1- البنية التحتية التكنولوجية

جدول (6) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات البنية

#### البنية التحتية التكنولوجية

| العبارة                                                                                                            | المتوسط الحسابي | الانحراف المعياري | الترتيب | مستوي الموافقة |
|--------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|---------|----------------|
| تستخدم المؤسسات المالية السعودية في المملكة العربية السعودية شبكات الاتصال الإلكترونية لمتابعة وتقييم العمل اليومي | 4.038           | 1.084             | 1       | مرتفع          |

|       |   |       |       |                                                                                                                     |
|-------|---|-------|-------|---------------------------------------------------------------------------------------------------------------------|
| مرتفع | 5 | 0.883 | 3.750 | استفادت المؤسسات المالية السعودية في المملكة العربية السعودية من التقنيات الحديثة للاتصالات                         |
| مرتفع | 2 | 0.991 | 3.865 | ساهمت تكنولوجيا المعلومات في سهولة الاتصالات بين المؤسسات المالية السعودية في المملكة العربية السعودية              |
| مرتفع | 4 | 1.067 | 3.808 | تتوافر بالمؤسسات المالية السعودية في المملكة العربية السعودية المعدات والتقنيات اللازمة في مجال تكنولوجيا المعلومات |
| مرتفع | 3 | 0.991 | 3.808 | ساهمت تكنولوجيا المعلومات في زيادة قدرة المؤسسات المالية السعودية في المملكة العربية السعودية على تحقيق أهدافها     |
| مرتفع |   | 1.003 | 3.854 | المتوسط                                                                                                             |

عند دراسة عبارات البنية التحتية التكنولوجية تبين أن جميع العبارات في مستوى الموافقة المرتفع مما يوضح ارتفاع مستوى البنية التحتية التكنولوجية كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.854 بانحراف معياري 1.003

## 2- البرمجيات والتصميمات

جدول (7) المتوسط الحسابي والانحراف المعياري والترتيب ومستوى الموافقة على عبارات البرمجيات والتصميمات

| العبارة                                                                                                                         | المتوسط الحسابي | الانحراف المعياري | الترتيب | مستوى الموافقة |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|---------|----------------|
| تتوافر في المؤسسات المالية السعودية في المملكة العربية السعودية أنظمة حماية آلية متطورة لحماية بياناتها                         | 4.231           | 0.854             | 1       | مرتفع جدا      |
| تستخدم المؤسسات المالية السعودية في المملكة العربية السعودية البرامج والتطبيقات السياحية الإلكترونية                            | 3.808           | 0.951             | 4       | مرتفع          |
| تناسب البرمجيات المستخدمة في المؤسسات المالية السعودية في المملكة العربية السعودية مع نظام العمل لتقديم الخدمات السياحية بسهولة | 3.827           | 0.964             | 3       | مرتفع          |
| يوجد بالمؤسسات المالية السعودية في المملكة العربية السعودية نظام رقابي إداري إلكتروني                                           | 3.712           | 1.109             | 5       | مرتفع          |
| تمتلك المؤسسات المالية السعودية في المملكة العربية السعودية ميزانية كافية لتوفير الأجهزة والمعدات التكنولوجية وتحديثها باستمرار | 4.058           | 1.056             | 2       | مرتفع          |
| المتوسط                                                                                                                         | 3.927           | 0.987             |         | مرتفع          |

وعند دراسة عبارات البرمجيات والتصميمات تبين أن عبارة واحدة في مستوى الموافقة المرتفع جدا وأربع عبارات في مستوى الموافقة المرتفع مما يوضح ارتفاع مستوى البرمجيات والتصميمات كأحد أبعاد

الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة

المتوسط الحسابي 3.927 بانحراف معياري 0.987

### 3- الخدمات المبتكرة

جدول (8) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات الخدمات

#### المبتكرة

| العبارة                                                                                                                       | المتوسط الحسابي | الانحراف المعياري | الترتيب | مستوي الموافقة |
|-------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|---------|----------------|
| تعمل المؤسسات المالية السعودية في المملكة العربية السعودية على الابتكار في تقديم الخدمات للعملاء                              | 3.462           | 1.196             | 4       | مرتفع          |
| تحرص ادارة المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تحديث تجهيزاتها والياتها باستمرار.               | 4.038           | 0.907             | 3       | مرتفع          |
| تحرص المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على أن تتلاءم التكنولوجيا المستخدمة مع متطلبات العمل       | 4.096           | 0.869             | 2       | مرتفع          |
| تحرص المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تدريب العاملين على استخدام التقنيات الحديثة وباستمرار. | 4.231           | 0.877             | 1       | مرتفع جدا      |
| تهتم المؤسسات المالية السعودية العاملة في المملكة العربية السعودية بتبني الأساليب التكنولوجية الحديثة في مجال العمل           | 3.038           | 1.313             | 5       | متوسط          |

|       |       |       |         |
|-------|-------|-------|---------|
| مرتفع | 1.032 | 3.773 | المتوسط |
|-------|-------|-------|---------|

وعند دراسة عبارات الخدمات المبتكرة تبين أن عبارة واحدة في مستوى الموافقة المرتفع جدا وثلاث عبارات في مستوى الموافقة المرتفع وعبارة واحدة في مستوى الموافقة المتوسط مما يوضح ارتفاع مستوى الخدمات المبتكرة كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.773 بانحراف معياري 1.032

#### 4- التفاعل والتواصل

جدول (9) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات التفاعل

#### والتواصل

| العبارة                                                                                                                         | المتوسط الحسابي | الانحراف المعياري | الترتيب | مستوي الموافقة |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|---------|----------------|
| تركز المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على التكنولوجيا الحديثة بما يتلاءم وحاجات ورغبات العملاء.    | 3.769           | 1.022             | 3       | مرتفع          |
| تقوم المؤسسات المالية السعودية العاملة في المملكة العربية السعودية بإجراء تغييرات مستمرة لتطوير خدماتها في ضوء احتياجات العملاء | 3.538           | 0.999             | 5       | مرتفع          |
| تمتلك المؤسسات المالية السعودية العاملة في المملكة العربية السعودية قدرة التركيز على العميل في كافة المستويات                   | 3.750           | 0.947             | 4       | مرتفع          |
| تعتمد المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تقديم خدمات محددة                                       | 4.019           | 0.828             | 2       | مرتفع          |

|       |   |       |       |                                                                                                                           |
|-------|---|-------|-------|---------------------------------------------------------------------------------------------------------------------------|
| مرتفع | 1 | 0.841 | 4.135 | تمتلك المؤسسات المالية السعودية العاملة في المملكة العربية السعودية القدرة على مواكبة التغيرات في احتياجات ورغبات العملاء |
| مرتفع |   | 0.927 | 3.842 | المتوسط                                                                                                                   |

وعند دراسة عبارات التفاعل والتواصل تبين أن جميع العبارات في مستوى الموافقة المرتفع مما يوضح ارتفاع مستوى التفاعل والتواصل كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.842 بانحراف معياري 0.927 يتبين مما سبق ارتفاع مستوى الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.849 بانحراف معياري 0.987

## المحور الثاني: إدارة المخاطر السيبرانية

جدول (10) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات إدارة

### المخاطر السيبرانية

| العبارة                                                                                | المتوسط الحسابي | الانحراف المعياري | الترتيب | مستوي الموافقة |
|----------------------------------------------------------------------------------------|-----------------|-------------------|---------|----------------|
| أعتقد أن وجود سياسة فعالة لإدارة المخاطر السيبرانية يعزز من أمان المعلومات في مؤسستي.  | 4.154           | 0.978             | 4       | مرتفع          |
| أرى أن التدريب المستمر للموظفين حول المخاطر السيبرانية يساهم في تقليل الحوادث الأمنية. | 4.288           | 0.825             | 1       | مرتفع جدا      |

|           |   |       |       |                                                                                                              |
|-----------|---|-------|-------|--------------------------------------------------------------------------------------------------------------|
| مرتفع     | 5 | 1.019 | 3.981 | أعتبر أن استخدام تقنيات الحماية المتقدمة (مثل جدران الحماية وتشفير البيانات) ضروري لحماية المعلومات الحساسة. |
| مرتفع جدا | 2 | 0.848 | 4.212 | أؤمن بأن تقييم المخاطر السيبرانية بشكل دوري يساعد في تحسين استجابة المؤسسة للتهديدات المحتملة.               |
| مرتفع     | 3 | 0.901 | 4.173 | أجد أن التعاون مع جهات خارجية متخصصة في الأمن السيبراني يعزز من قدرة مؤسستي على مواجهة المخاطر.              |
| مرتفع     |   | 0.914 | 4.162 | المتوسط                                                                                                      |

عند دراسة عبارات إدارة المخاطر السيبرانية تبين أن عبارتين في مستوى الموافقة المرتفع جدا وثلاث عبارات في مستوى الموافقة المرتفع مما يوضح ارتفاع مستوى إدارة المخاطر السيبرانية في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 4.162 بانحراف معياري 0.914

### 3.4 ثالثاً: اختبار فروض الدراسة

✓ الفرضية الرئيسية: لا يوجد أثر ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030

جدول (11) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الرئيسية

| P-VALUE | r     | R <sup>2</sup> | F         | t        | B     |
|---------|-------|----------------|-----------|----------|-------|
| 0.000   | 0.661 | 0.437          | 280.659** | 16.753** | 0.187 |

المصدر: نتائج التحليل الإحصائي برنامج SPSS 23

يتبين من الجدول (11) وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 حيث كانت قيمة ( $\text{Sig F}$ ) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين الابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) وإدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح ان المتغير المستقل (الابتكار التكنولوجي) يفسر 43.7 % من التغيرات التي تحدث في المتغير التابع (إدارة المخاطر السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى الابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.187% مما يبين عدم صحة الفرضية الرئيسية للدراسة

✓ الفرضية الفرعية الأولى: لا يوجد أثر ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للبنية التحتية التكنولوجية في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030

جدول (12) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الاولى

| P-VALUE | R     | R <sup>2</sup> | F         | t        | b     |
|---------|-------|----------------|-----------|----------|-------|
| 0.000   | 0.637 | 0.406          | 247.728** | 15.739** | 0.626 |

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

يتبين من الجدول (12) وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للبنية التحتية التكنولوجية في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 حيث كانت قيمة ( $\text{Sig F}$ ) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين البنية التحتية

التكنولوجية في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح ان المتغير المستقل (البنية التحتية التكنولوجية) يفسر 40.6 % من التغيرات التي تحدث في المتغير التابع (إدارة المخاطر السيبرانية بالمملكة العربية السعودية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى البنية التحتية التكنولوجية بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.626% مما يبين عدم صحة الفرضية الفرعية الأولى للدراسة

✓ الفرضية الفرعية الثانية: لا يوجد أثر ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للبرمجيات والتصميمات في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030

جدول (13) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثانية

| P-VALUE | r     | R <sup>2</sup> | F         | t        | b     |
|---------|-------|----------------|-----------|----------|-------|
| 0.000   | 0.647 | 0.419          | **261.275 | **16.164 | 0.675 |

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

يتبين من الجدول (13) وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للبرمجيات والتصميمات في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 حيث كانت قيمة ( $\text{Sig F}$ ) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين البرمجيات والتصميمات في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح ان المتغير المستقل (البرمجيات والتصميمات) يفسر 41.9 % من التغيرات التي تحدث في المتغير التابع (إدارة المخاطر السيبرانية بالمملكة العربية السعودية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى البرمجيات والتصميمات بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.675% مما يبين عدم صحة الفرضية الفرعية الثانية للدراسة

✓ الفرضية الفرعية الثالثة: لا يوجد أثر ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للخدمات

المبتكرة في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030

جدول (14) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثالثة

| P-VALUE | r     | R <sup>2</sup> | F         | t        | b     |
|---------|-------|----------------|-----------|----------|-------|
| 0.000   | 0.559 | 0.312          | **164.545 | **12.828 | 0.600 |

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

يتبين من الجدول (14) وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للخدمات المبتكرة في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين الخدمات المبتكرة في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح ان المتغير المستقل (الخدمات المبتكرة) يفسر 31.2 % من التغيرات التي تحدث في المتغير التابع (إدارة المخاطر السيبرانية بالمملكة العربية السعودية) وان باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى الخدمات المبتكرة بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.600% مما يبين عدم صحة الفرضية الفرعية الثالثة للدراسة

✓ الفرضية الفرعية الرابعة: لا يوجد أثر ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للتفاعل

والتواصل في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030

جدول (15) نتائج نموذج الانحدار الخطي البسيط لاختبار الفرضية الفرعية الرابعة

| P-VALUE | r     | R <sup>2</sup> | F         | t        | B     |
|---------|-------|----------------|-----------|----------|-------|
| 0.000   | 0.533 | 0.285          | **144.014 | **12.001 | 0.525 |

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

يتبين من الجدول (14) وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للتفاعل والتواصل في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 حيث كانت قيمة ( $\text{Sig F}$ ) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين التفاعل والتواصل في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح ان المتغير المستقل (التفاعل والتواصل) يفسر 28.5 % من التغيرات التي تحدث في المتغير التابع (إدارة المخاطر السيبرانية بالمملكة العربية السعودية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى التفاعل والتواصل بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.525% مما يبين عدم صحة الفرضية الفرعية الرابعة للدراسة

## الفصل الخامس: خلاصة النتائج والتوصيات والمقترحات

### مقدمة

سوف نتناول في هذا الفصل ملخص النتائج التي توصلت إليها الدراسة من خلال تحليل البيانات المتعلقة بمحاور الدراسة والتي تم الحصول عليها عن طريق أداة الاستبيان المتمثلة في استمارة الاستبيان الإلكتروني واختبار فروض الدراسة من أجل تحقيق أهداف الدراسة وكذلك يتناول الفصل مجموعة من التوصيات التي توصي بها الدراسة ومجموعة من المقترحات لدراسات وابحث يمكن اجراؤها في المستقبل

### 1.5 خلاصة نتائج الدراسة

- ✓ ارتفاع مستوى البنية التحتية التكنولوجية كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.854 بانحراف معياري 1.003
- ✓ ارتفاع مستوى البرمجيات والتصميمات كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.927 بانحراف معياري 0.987
- ✓ ارتفاع مستوى الخدمات المبتكرة كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.773 بانحراف معياري 1.032
- ✓ ارتفاع مستوى التفاعل والتواصل كأحد أبعاد الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.842 بانحراف معياري 0.927
- ✓ ارتفاع مستوى الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 3.849 بانحراف معياري 0.987

✓ ارتفاع مستوى إدارة المخاطر السيبرانية في المملكة العربية السعودية حيث بلغت قيمة المتوسط الحسابي 4.162 بانحراف معياري 0.914

✓ وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين الابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) وإدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 وتبين أن كلما ازداد مستوى الابتكار التكنولوجي بأبعاده (البنية التحتية التكنولوجية، البرمجيات والتصميمات، الخدمات المبتكرة، التفاعل والتواصل) بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 بمقدار 0.187% مما يبين عدم صحة الفرضية الرئيسية للدراسة وتتفق هذه النتيجة مع نتيجة دراسة (أبو المجد، 2022) ومع نتيجة دراسة (خديش، 2023) وكذلك مع نتيجة دراسة (سنوسي، 2020) ومع نتيجة دراسة (النظامي، 2021)

✓ وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للبنية التحتية التكنولوجية في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين البنية التحتية التكنولوجية في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 وتبين أن كلما ازداد مستوى البنية التحتية التكنولوجية بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 بمقدار 0.626% مما يبين عدم صحة الفرضية الفرعية الأولى للدراسة

✓ وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) للبرمجيات والتصميمات في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقاً لرؤية المملكة 2030 واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) بين البرمجيات والتصميمات في إدارة

المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 وتبين أن كلما ازداد مستوى البرمجيات والتصميمات بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.675% مما يبين عدم صحة الفرضية الفرعية الثانية للدراسة

✓ وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى  $(\alpha \leq 0.05)$  للخدمات المبتكرة في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى  $(\alpha \leq 0.05)$  بين الخدمات المبتكرة في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 وتبين أن كلما ازداد مستوى الخدمات المبتكرة بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.600% مما يبين عدم صحة الفرضية الفرعية الثالثة للدراسة

✓ وجود تأثير إيجابي ذو دلالة إحصائية عند مستوى  $(\alpha \leq 0.05)$  للتفاعل والتواصل في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية عند مستوى  $(\alpha \leq 0.05)$  بين التفاعل والتواصل في إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 وتبين أن كلما ازداد مستوى التفاعل والتواصل بمقدار 1 % ازداد مستوى إدارة المخاطر السيبرانية بالمملكة العربية السعودية وفقا لرؤية المملكة 2030 بمقدار 0.525% مما يبين عدم صحة الفرضية الفرعية الرابعة للدراسة

## 2.5 التوصيات

✓ الاهتمام بتوفير الموارد المالية والإمكانيات اللوجستية والدعم الخاص التي يمكن من خلالها الحفاظ على المستوى المتميز من تطبيق الابتكار التكنولوجي في المؤسسات المالية السعودية العاملة بالمملكة العربية السعودية

✓ العمل على توفير البيئة التحتية التي تساهم في زيادة قدرة المؤسسات المالية السعودية العاملة بالمملكة العربية السعودية على تحقيق أهدافها وفقا لرؤية المملكة 2030

- ✓ زيادة وعى العاملين في المؤسسات المالية السعودية العاملة بالمملكة العربية السعودية بضرورة العمل على تقديم أعلى مستوى ممكن من جودة الخدمات من خلال دورات وبرامج تنمية مهنية مكثفة
- ✓ الاهتمام بالعمل على الحفاظ على المستوى المتميز من إدارة المخاطر السيبرانية بالمملكة العربية السعودية من خلال توفير كافة الإمكانيات والاحتياجات والتي تساهم في تحقيق ذلك

### 3.5 المقترحات

- ✓ التوسع في إجراء الدراسات والأبحاث المتعلقة بالابتكار التكنولوجي والتعرف على أثره على مستويات الأداء والإنتاجية في الشركات والمؤسسات العاملة في المملكة العربية السعودية
- ✓ التوسع في إجراء الدراسات والأبحاث المتعلقة بإدارة المخاطر السيبرانية بالمملكة العربية السعودية والتعرف على العوامل المؤثرة عليه

## Abstract

This study aims to analyze the impact of technological innovation on cybersecurity risk management in Saudi financial institutions. A proportional stratified random sample of 364 managers from senior and middle management levels was selected. Data was collected using an electronic questionnaire and analyzed through a descriptive-analytical approach, applying a set of statistical methods.

The results of the study showed that the high level of technological infrastructure, as one of the dimensions of technological innovation, and the high level of software and designs, as another dimension of technological innovation, are present in the Saudi financial institutions operating in the Kingdom of Saudi Arabia.

Based on these results, the study recommends focusing on providing financial resources, logistical capabilities, and specific support that can maintain the outstanding level of technological innovation application in Saudi financial institutions. It also suggests working to provide the infrastructure that contributes to enhancing the ability of Saudi financial institutions to achieve their goals in alignment with Saudi Vision 2030.

**Keywords:** Technological Innovation – Cybersecurity Risk Management – Saudi Financial Institutions

## المراجع:

### أولاً: المراجع العربية

- عبد المجيد أحمد سليمان التير, & مصطفى أحمد بن حكومة. (2024). الابتكار التكنولوجي في صناعة التمويل المصرفي: نماذج جديدة وفرص استثمارية. مجلة شمال إفريقيا للنشر العلمي-110 (NAJSP), 124.
- Makhoos, D. (2021). دور الابتكار التكنولوجي في تعزيز الميزة التنافسية للمشاريع الصغيرة. Tishreen University Journal-Economic and Legal Sciences Series, 43 (3).
- بيان, محمد سعد الدين, شباط, & مهند أحمد. (2024). دور الابتكار التكنولوجي والذكاء الصناعي في تحقيق استدامة التعليم: تحليل وتوجهات للمستقبل.
- الخرينج, نواف متعب بنيه متعب, البسطويسي, مروة أحمد عبد الرحمن, و داود, ياسر إبراهيم محمد. (2022). دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي. المجلة العلمية للدراسات والبحوث المالية والإدارية, مج 13, ملحق, 1715 - 1743.
- ديقش. (2023). مساهمة التسويق بالعلاقات في تفعيل الابتكار التكنولوجي في المؤسسة الاقتصادية الجزائرية: دراسة حالة بعض المؤسسات (Doctoral dissertation).
- الرحماوي, رحاب حسني حامد. (2024). إدارة المخاطر السيبرانية في المجال الاقتصادي. مجلة الأمن القومي والإستراتيجية, مج 2, ع 4, 104 - 115.
- شرف, إبراهيم أحمد إبراهيم. (2023). إثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين: دراسة تجريبية. مجلة الإسكندرية للبحوث المحاسبية, مج 7, ع 1, 211 - 281.
- شهبان, زين الدين, & فريد زين الدين. (2024). دور الابتكار التكنولوجي في تبني استراتيجية المحيط الأزرق لتحقيق الميزة التنافسية المستدامة: دراسة تطبيقية على الشركات الصناعية المصرية. مجلة البحوث التجارية.

- الطاهات، أماني زهير خالد، و الرواشدة، هاني علي عارف. (2023). أثر إدارة المخاطر السيبرانية على جودة التدقيق الداخلي في البنوك التجارية الأردنية: الدور المعدل للحوكمة السيبرانية (رسالة ماجستير غير منشورة). جامعة جرش، جرش.
- عثمان، & رضا فولي. (2023). دراسة لاتجاه التسويق المستقبلي لروبوتات الخدمة الشخصية مع نظرة الابتكار التكنولوجي. المجلة المصرية لبحوث الرأي العام، 22(3)، 115-157.
- قداري، سليمان، باسيدي، أحمد، قويدري، & عبد الرحمان/مؤطر. (2021). دور الابتكار التكنولوجي في تحقيق الميزة التنافسية لدى المؤسسات الصغيرة والمتوسطة (Doctoral dissertation, جامعة احمد دراية-ادرا). احمد دراية-ادرا.
- ملاوي، وهيبة، ثابتي، & وليد. (2024). الذكاء الاصطناعي في المدينة الذكية: تحليل التفاعل بين الابتكار التكنولوجي والتأثير القانوني والأخلاقي.
- موسى، عمرو عادل عبدالفتاح، شاهين، عبدالحميد أحمد أحمد، شحاتة، محمد موسى علي، و البحيري، مروة أحمد عبدالرحمن. (2023). قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على قيمة المنشأة: دراسة تطبيقية. المجلة العلمية للدراسات والبحوث المالية والإدارية، مج15، عدد خاص ، 1 - 66.
- نبيل، دحمان، لحسن، & بن علي. (2022). دور الابتكار التكنولوجي في تسير النفايات-دراسة لعينة من المؤسسات مراكز الردم التقني بغرداية (Doctoral dissertation, جامعة غرداية).

## ثانيا: المراجع الأجنبية

- Adam J. Saffer. (2018). Value-Added Theory. تم الاسترداد من [https://www.researchgate.net/publication/327877299\\_Value-Added\\_Theory](https://www.researchgate.net/publication/327877299_Value-Added_Theory)
- Abd-Elmageed, M. H. (2024). The Effect of CSR on the Interrelationship among Cyber Risk, Supply Chain, and Small and Medium-Sized Enterprises Performance: An Applied Study. Scientific Journal of Economics and Trade, Vol. 4, 205-250.

- Ahmed Al-Musallam Chuc. (2023). IMPACT OF FINANCIAL TECHNOLOGY (FINTECH) ON FINANCIAL PERFORMANCE OF MICRO FINANCE INSTITUTIONS IN BAHRAIN. تم الاسترداد من <https://www.ajoeijournals.org/sys/index.php/ajoei/article/view/506>
- Ali Polat. (2021). Effects of GDPR on the financial services sector in the Kingdom of Saudi Arabia. من الاسترداد تم <https://www.ingentaconnect.com/content/hsp/jdpp/2021/00000004/00000003/art0004>
- Amar Johri. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. تم الاسترداد من <https://onlinelibrary.wiley.com/doi/10.1155/2023/2103442>
- Badawy, H. A. E. S. (2021). The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on NonProfessional Egyptian Investors' Decisions: An Experimental Study. Alexandria Journal of Accounting Research, Vol. 5, No. 3, 1-56.
- Bushra Elamin. (2016). The Impact Of Information Security Management For E- Banks Performance In Kingdom Of Sudi Arabia. من الاسترداد تم [https://www.researchgate.net/publication/310443456\\_The\\_Impact\\_Of\\_Information\\_Security\\_Management\\_For\\_E-\\_Banks\\_Performance\\_In\\_Kingdom\\_Of\\_Sudi\\_Arabia](https://www.researchgate.net/publication/310443456_The_Impact_Of_Information_Security_Management_For_E-_Banks_Performance_In_Kingdom_Of_Sudi_Arabia)
- David Kindness. (2023). Risk Management Framework (RMF): Definition and Components. من الاسترداد تم <https://www.investopedia.com/articles/professionals/021915/risk-management-framework-rmf-overview.asp>
- Elqadi, M. M. A., Mohamed, M. A., and Abdelmegeed, M. H. (2024). The Role of Risk-Based Internal Auditing on the Activation of Cybersecurity to Control Information Risk: A Field Study. Accounting Thought, Vol. 28, No. 2, 117-146.

- Florian Diener. (2021). Digital Transformation in Banking: A Managerial Perspective on Barriers to Change. تم الاسترداد من <https://www.mdpi.com/2071-1050/13/4/2032>
- Frank Cremer. (2022). Cyber risk and cybersecurity: a systematic review of data availability. تم الاسترداد من <https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/>
- Hassan Alqahtani. (2024). The effect of financial technology on the financial performance of national Saudi banks. تم الاسترداد من [https://www.researchgate.net/publication/379931144\\_The\\_effect\\_of\\_financial\\_technology\\_on\\_the\\_financial\\_performance\\_of\\_national\\_Saudi\\_banks](https://www.researchgate.net/publication/379931144_The_effect_of_financial_technology_on_the_financial_performance_of_national_Saudi_banks)
- John R. Turner. (2019). Complexity Theory: An Overview with Potential Applications for the Social Sciences. تم الاسترداد من <https://www.mdpi.com/2079-8954/7/1/4>
- Mahadih Kyambade. (2024). Technological Innovation and Commercial Banks' Financial Performance: A Mediation Analysis of Risk Management Practices. تم الاسترداد من [https://www.researchgate.net/publication/382183952\\_Technological\\_Innovation\\_and\\_Commercial\\_Banks'\\_Financial\\_Performance\\_A\\_Mediation\\_Analysis\\_of\\_Risk\\_Management\\_Practices](https://www.researchgate.net/publication/382183952_Technological_Innovation_and_Commercial_Banks'_Financial_Performance_A_Mediation_Analysis_of_Risk_Management_Practices)
- Marta Barroso. (2022). Digital transformation and the emergence of the Fintech sector: Systematic literature review. تم الاسترداد من <https://www.sciencedirect.com/science/article/pii/S2666954422000084>
- Md Hamid Uddin. (2023). Does digital transformation matter for operational risk exposure? تم الاسترداد من <https://www.sciencedirect.com/science/article/pii/S0040162523006042>
- Metwally, A. B. M., Abdelazim, S. I., and Almarji, M. T. (2022). Internal Auditors' Role In Confronting Cyber and Fraud Risks Related to Outsourcing Insurance: An Exploratory Study. Alexandria Journal of Accounting Research, Vol. 6, No. 3, 1-31.

- Mohamed Al Hammadi. (2024). Risk Management in Islamic Banking: The Impact of Financial Technologies through Empirical Insights from the UAE. تم الاسترداد من <https://www.mdpi.com/2227-9091/12/2/17>
- Muhammad Fakhru Safitra. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. تم الاسترداد من <https://www.mdpi.com/2071-1050/15/18/13369>
- Nawaf Alhalafi. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. تم الاسترداد من [https://www.researchgate.net/publication/371154328\\_Exploring\\_the\\_Challenges\\_and\\_Issues\\_in\\_Adopting\\_Cybersecurity\\_in\\_Saudi\\_Smart\\_Cities\\_Conceptualization\\_of\\_the\\_Cybersecurity-Based\\_UTAUT\\_Model](https://www.researchgate.net/publication/371154328_Exploring_the_Challenges_and_Issues_in_Adopting_Cybersecurity_in_Saudi_Smart_Cities_Conceptualization_of_the_Cybersecurity-Based_UTAUT_Model)
- Ramdani, Reem, and Al-Fahri, Zainab Al-Fassi. (2024). Cybersecurity Risks and Cyber-Resilience: The Games of Digital Transformation in the Digital Age in Morocco. Journal of Law and Business, No. 106, pp. 276-289.
- Salah AlBenjasim. (2024). Development of cybersecurity framework for FinTech innovations: Bahrain as a case study. تم الاسترداد من <https://link.springer.com/article/10.1365/s43439-024-00130-4>
- Umara Noreen. (2024). Mapping of FinTech Ecosystem to Sustainable Development Goals (SDGs): Saudi Arabia's Landscape. تم الاسترداد من <https://www.mdpi.com/2071-1050/16/21/9362>
- Wided Dafri. (2023). Challenges and opportunities to enhance digital financial transformation in crisis management. تم الاسترداد من <https://www.sciencedirect.com/science/article/pii/S259029112300267X>

- Xuan Wei. (2023). Meta theories of technological innovation based on the analysis of classic texts. من الاسترداد تم  
<https://www.sciencedirect.com/science/article/pii/S2405844023039865>
- Zulaicha Parastuty. (2015). Organizational change: a review of theoretical conceptions that explain how and why young firms change. من الاسترداد تم  
[https://www.researchgate.net/publication/270592509\\_Organizational\\_change\\_a\\_review\\_of\\_theoretical\\_conceptions\\_that\\_explain\\_how\\_and\\_why\\_young\\_firms\\_change](https://www.researchgate.net/publication/270592509_Organizational_change_a_review_of_theoretical_conceptions_that_explain_how_and_why_young_firms_change)

الملاحق

## استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس تحليل تأثير الابتكار التكنولوجي على إدارة المخاطر

السيبرانية في المؤسسات المالية السعودية

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل

الحصول منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء

رأيكم بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأثقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن

جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا

البحث، وسوف أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

## أولاً: البيانات الشخصية

- 1- النوع الاجتماعي ☐ ذكر ☐ أنثى
- 2- العمر ☐ 25 سنة فأقل ☐ من 25 – أقل من 35 سنة ☐ 35 – أقل من 45 سنة ☐ من 45 سنة فأكثر
- 3- المؤهل العلمي ☐ ثانوي ☐ بكالوريوس ☐ ماجستير ☐ دكتورة
- 4- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 5 – أقل من 10 سنوات ☐ 10 – أقل من 15 سنة ☐ أكثر من 15 سنة
- 5- المسي الوظيفي ☐ مدير ☐ نائب مدير ☐ رئيس قسم ☐ موظف

## ثانيا محاور الاستبيان

➤ المحور الأول: الابتكار التكنولوجي، ضع إشارة (√) في المربع المناسب لاختيارك:

| معارض<br>بشدة              | معارض | محايد | أوافق | أوافق<br>بشدة | البعد                                                                                                               |
|----------------------------|-------|-------|-------|---------------|---------------------------------------------------------------------------------------------------------------------|
| البنية التحتية التكنولوجية |       |       |       |               |                                                                                                                     |
|                            |       |       |       |               | تستخدم المؤسسات المالية السعودية في المملكة العربية السعودية شبكات الاتصال الإلكترونية لمتابعة وتقييم العمل اليومي  |
|                            |       |       |       |               | استفادت المؤسسات المالية السعودية في المملكة العربية السعودية من التقنيات الحديثة للاتصالات                         |
|                            |       |       |       |               | ساهمت تكنولوجيا المعلومات في سهولة الاتصالات بين المؤسسات المالية السعودية في المملكة العربية السعودية              |
|                            |       |       |       |               | تتوافر بالمؤسسات المالية السعودية في المملكة العربية السعودية المعدات والتقنيات اللازمة في مجال تكنولوجيا المعلومات |
|                            |       |       |       |               | ساهمت تكنولوجيا المعلومات في زيادة قدرة المؤسسات المالية السعودية في المملكة العربية السعودية على تحقيق أهدافها     |
| البرمجيات والتصميمات       |       |       |       |               |                                                                                                                     |

|                  |  |  |  |                                                                                                                                 |
|------------------|--|--|--|---------------------------------------------------------------------------------------------------------------------------------|
|                  |  |  |  | تتوافر في المؤسسات المالية السعودية في المملكة العربية السعودية أنظمة حماية آلية متطورة لحماية بياناتها                         |
|                  |  |  |  | تستخدم المؤسسات المالية السعودية في المملكة العربية السعودية البرامج والتطبيقات السياحية الإلكترونية                            |
|                  |  |  |  | تناسب البرمجيات المستخدمة في المؤسسات المالية السعودية في المملكة العربية السعودية مع نظام العمل لتقديم الخدمات السياحية بسهولة |
|                  |  |  |  | يوجد بالمؤسسات المالية السعودية في المملكة العربية السعودية نظام رقابي إداري إلكتروني                                           |
|                  |  |  |  | تمتلك المؤسسات المالية السعودية في المملكة العربية السعودية ميزانية كافية لتوفير الأجهزة والمعدات التكنولوجية وتحديثها باستمرار |
| الخدمات المبتكرة |  |  |  |                                                                                                                                 |
|                  |  |  |  | تعمل المؤسسات المالية السعودية في المملكة العربية السعودية على الابتكار في تقديم الخدمات للعملاء                                |
|                  |  |  |  | تحرص ادارة المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تحديث تجهيزاتها والياتها باستمرار.                 |

|                  |  |  |  |  |                                                                                                                                 |
|------------------|--|--|--|--|---------------------------------------------------------------------------------------------------------------------------------|
|                  |  |  |  |  | تحرص المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على أن تتلاءم التكنولوجيا المستخدمة مع متطلبات العمل         |
|                  |  |  |  |  | تحرص المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تدريب العاملين على استخدام التقنيات الحديثة وباستمرار.   |
|                  |  |  |  |  | تهتم المؤسسات المالية السعودية العاملة في المملكة العربية السعودية بتبني الأساليب التكنولوجية الحديثة في مجال العمل             |
| التفاعل والتواصل |  |  |  |  |                                                                                                                                 |
|                  |  |  |  |  | تركز المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على التكنولوجيا الحديثة بما يتلاءم وحاجات ورغبات العملاء.    |
|                  |  |  |  |  | تقوم المؤسسات المالية السعودية العاملة في المملكة العربية السعودية بإجراء تغييرات مستمرة لتطوير خدماتها في ضوء احتياجات العملاء |
|                  |  |  |  |  | تمتلك المؤسسات المالية السعودية العاملة في المملكة العربية السعودية قدرة التركيز على العميل في كافة المستويات                   |
|                  |  |  |  |  | تعتمد المؤسسات المالية السعودية العاملة في المملكة العربية السعودية على تقديم خدمات محددة                                       |
|                  |  |  |  |  | تمتلك المؤسسات المالية السعودية العاملة في المملكة العربية السعودية القدرة على مواكبة التغييرات في احتياجات ورغبات العملاء      |

➤ المحور الثاني: إدارة المخاطر السيبرانية، ضع إشارة (✓) في المربع المناسب لاختيارك:

| معارض<br>بشدة | معارض | محايد | أو افق | أو افق<br>بشدة | البعد                                                                                                        |
|---------------|-------|-------|--------|----------------|--------------------------------------------------------------------------------------------------------------|
|               |       |       |        |                | أعتقد أن وجود سياسة فعالة لإدارة المخاطر السيبرانية يعزز من أمان المعلومات في مؤسستي.                        |
|               |       |       |        |                | أرى أن التدريب المستمر للموظفين حول المخاطر السيبرانية يساهم في تقليل الحوادث الأمنية.                       |
|               |       |       |        |                | أعتبر أن استخدام تقنيات الحماية المتقدمة (مثل جدران الحماية وتشفير البيانات) ضروري لحماية المعلومات الحساسة. |
|               |       |       |        |                | أؤمن بأن تقييم المخاطر السيبرانية بشكل دوري يساعد في تحسين استجابة المؤسسة للتهديدات المحتملة.               |
|               |       |       |        |                | أجد أن التعاون مع جهات خارجية متخصصة في الأمن السيبراني يعزز من قدرة مؤسستي على مواجهة المخاطر.              |

مع خالص التقدير والاحترام

**Midocean University**



**Management College**

**Specialization in Risk Management**

**The Impact of Technological Innovation on Cyber Risk  
Management: An Applied Study on Saudi Financial  
Institutions**

**Student preparation/**

**Nada Rashid Abaalkheil**

**242000219**

**Supervisor/**

**Dr. Al faisal Abdelhameed Mohamed**

**Dr. Fayez Ali Jrad**

**1446 – 2025**