جامعـــــــة تعـــــــــز
نيابة الدراسات العليا والبحث العلمي
مركز الدراسات العليا
برنامج الماجستير
قسم إدارة الأعمال التنفيذي

رسالة ماجستير بعنوان:

متطلبات الأمن السيبراني وأثرها في حماية أنظمة المعلومات في البنوك اليمنية

(قدمت هذه الرسالة استكمالاً لمتطلبات نيل درجة الماجستير التنفيذي في إدارة الأعمال

مركز الدراسات العليا — جامعة تعز

إعداد الطالب:

داود عبده أحمد سعيدالشريحي

المشرف العلمي:

أ.م. د مجيب عبد الحكيم الحكيمي

أستاذ مشارك تقنية معلومات

العام الجامعي (1445هـ/2024م)


بسم الله الرحمن الرحيم

قال تعالى:

﴿قَالَ الَّذِي عِندَهُ عِلْمٌ مِّنَ الْكِتَابِ أَنَا آتِيكَ بِهِ قَبْلَ أَن يَرْتَدَّ إِلَيْكَ طَرْفُكَ ۚ فَلَمَّا رَآهُ مُسْتَقِرًّا عِندَهُ قَالَ

هَذَا مِن فَضْلِ رَبِّي لِيَبْلُوَنِي أَأَشْكُرُ أَمْ أَكْفُرُ ۖ وَمَن شَكَرَ فَإِنَّمَا يَشْكُرُ لِنَفْسِهِ ۖ وَمَن كَفَرَ

فَإِنَّ رَبِّي غَنِيٌّ كَرِيمٌ﴾ النمل (40)

الإهداء

إلى والدي الغالي ... سند الحياة، حامي الدرب ومعلم الحكمة

إلى أمي .... مصدر العطاء ونبع الحب الدافئ

لزوجتي، عوني ورفيقة دربي

إلى شموع حياتي وفلذات كبدي.. أولادي حفظهم الله..

إلى الشعب الفلسطيني المجاهد المرابط على أرض فلسطين.

إلى كل هؤلاء أهدي هذا الجهد المتواضع

داؤود الشريحي

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام على الرسول المعلم، الذي علمنا قيمة الاعتراف والتقدير والشكر لمن هم أهل الفضل حيث واليوم أقف على إتمام رسالتي، ولا يسعني الا أن أتقدم بالشكر الوافر والامتنان العميق لكل من كان له دور في هذا الإنجاز.

وأتوجه بالشكر والعرفان إلى مشرفي **الدكتور/ مجيب عبد الحكيم الحكيمي، أستاذ مشارك جامعة تعز** الذي تفضل بالإشراف والتوجيه، مانحًا إياي وقته واهتمامه، ومغذيًا عقلي بالمعلومات والأفكار النيرة. له مني كل الدعوات بأن يجزيه الله عني خير الجزاء..

واتقدم أيضا بالشكر والعرفان للجنة المناقشة الموقرة، التي ستقود بحكمتها وخبرتها العميقة مسار هذه الرسالة نحو آفاقٍ أرحب، برئاسة **الاستاذ الدكتور محمد عبد الجليل، جامعة تعز وممتحنا داخليا** وعضوية **الدكتور جميل زيد، أستاذ مساعد – جامعة الجند ممتحنا خارجيا** وأنتظر بشوقٍ وترقبٍ مساهماتهم القيمة التي ستسهم بشكل كبير في إثراء وتطوير هذا العمل.

وبنفس القدر من الامتنان، أشكر جميع أعضاء هيئة التدريس في مركز الدراسات العليا بجامعة تعز، الذين كان لهم الأثر البالغ في تذليل الصعوبات وإثراء العملية التعليمية بجهودهم الجبارة والمثمرة. كما أشكر كل الإخوة والأصدقاء الذين كانوا عوناً وسنداً في هذه الرحلة العلمية.

الباحث

قائمة المحتويات

الموضوع **رقم الصفحة**

قائمة الجداول

قائمة الأشكال

قائمة الملاحق

مُلخَّص الدراسة

متطلبات الأمن السيبراني وتأثيرها في حماية نظم المعلومات في البنوك اليمنية

هدفت هذه الدراسة إلى التعرف على أثر توافر متطلبات الأمن السيبراني (التنظيمية، الفنية، الامتثال للأطر والمعايير الدولية، المادية) في حماية نظم المعلومات في القطاع المصرفي اليمني. شمل مجتمع الدراسة (15) بنكًا يمنيًا خلال الفترة من يوليو حتى سبتمبر 2023، وتم جمع البيانات من خلال أداة الاستبيان وُزعت على عينة عشوائية مكونة من 250 موظفًا في فروع البنوك (الحكومية، والإسلامية، والتجارية) بمحافظتي تعز وعدن، واستخدمت الدراسة المنهج الوصفي مدعمًا بتحليلات إحصائية متنوعة لمعالجة البيانات.

أوضحت نتائج الدراسة وجود علاقة إيجابية معتبرة بين متطلبات الأمان السيبراني وحماية نظم المعلومات في البنوك المدروسة. كما تبينت فروق جوهرية في الإجابات بناءً على المتغيرات الديموغرافية مثل طبيعة البنك، المستوى التعليمي، والمنصب الوظيفي، وتوصي الدراسة على ضرورة تعزيز التدريب والامتثال للمعايير الدولية، وتحسين الأمن المادي، إضافة الى تحديث برامج الحماية، وإدارة كلمات المرور، وتقديم تدريبات متخصصة. كما تُشير إلى أهمية التعاون بين البنوك، تطوير خطط استجابة للحوادث السيبرانية، وإجراء تقييمات أمنية دورية.

الكلمات المفتاحية: متطلبات الأمن السيبراني، حماية أنظمة المعلومات، البنوك اليمنية

الفصل الأول:

الإطار العام للدراسة والدراسات السابقة

الفصل الأول: الإطار العام للدراسة والدراسات السابقة

يتناول هذا الفصل مقدمة عامة عن الدراسة، ومشكلتها، وأهميتها، وأهدافها، والأنموذج المعرفي لها، وفرضياتها، وحدودها، وهيكلها الدراسي، ودراسات سابقة ذات صلة بموضوعها، والتعليق عليها، والتعريفات الإجرائية للمصطلحات المستخدمة فيها.

1.1 المقدمة (Introduction):

في ضوء التطور التكنولوجي الهائل في مجال تكنولوجيا المعلومات والاتصالات واقتصاد المعرفة، والثورة الصناعية الخامسة في مختلف المجالات، وظهور تقنية الذكاء الاصطناعي أصبح نمط الحياة الحديثة معتمد بشكل متزايد على تكنولوجيا المعلومات لأنها الرابط الأساسي بين التقنية والأمن السيبراني (سمية، 2021). ومع تطور بناء المعلومات، شهدنا تعقيدًا ملحوظًا في مخاطر أمن المعلومات وفقاً لـ Ding, Wu, Tan & Jiang, (2021)، فإن بناء نظام معلومات يتمتع بمستوى عال من الأمن، سواء كان ذلك من خلال التجهيزات المادية أو البرمجية يعتبر الخطوة الأولى الأساسية في تأمين المعلومات. بالإضافة إلى ذلك، مع ظهور الثورة الصناعية الخامسة، أصبحت تكنولوجيا المعلومات عنصرًا أساسيًا ولا غنى عنها في الحياة المعاصرة، مما يزيد من أهمية وتعقيدات أمن المعلومات.

لذا أصبح الاعتماد على تقنية المعلومات والاتصالات الأساس الذي تنطلق منه الإدارات الحديثة، حين سيطر التطور الحديث في ثورة المعلومات والاتصالات على إدارة التغيير بشكل قاطع، من خلال توظيف المعلومات المتاحة لتحقيق أهداف المؤسسة (نوره، 2020).

وعلى الرغم من التطور الذي شهدته اليمن في مجال الاتصالات وتقنية المعلومات وإدخال خدمة الأنترنت في وقت مبكر 1996م، وزيادة المواقع الإلكترونية على شبكة الأنترنت، إلا أن

اليمن لم يحظ بأي اهتمام من جانب القطاع الأمني في التكنولوجيا والمعلومات الإلكترونية، حيث كشف الخبير العالمي في أمن المعلومات كريس بلاسك أن اليمن تُعد أرضية خصبة وهدفا سهلا للإرهاب الإلكتروني (العلم، 2022). وفي هذا الإطار، نشرت جمعية البنوك اليمنية تقريرًا صادرًا عن الشركة العالمية المتخصصة في الأمن السيبراني (TMI)، أشار الى أن منطقة الشرق الأوسط وشمال إفريقيا سجلت مستوى أخطار مرتفعًا قدره −0.04، مضيفا أن حوالي 76٪ من المؤسسات العالمية المشاركة في المؤتمر تتوقع تعرضها لهجمات إلكترونية في الأشهر الـ 12 المقبلة لتحقيق أهدافها (جمعية البنوك اليمنية ، 2022).

في هذا الجانب، أكد محمد (2021) أنه في ظل التداعيات الخطيرة للاختراقات والهجمات الإلكترونية، أصبح اللجوء إلى حلول أنظمة تجنب البنوك مثل هذه العواقب أمراً ضروريا، وفي السياق نفسه شدد الحميري (2021) أنه يجب على البنوك الالتزام بالمتطلبات اللازمة لحماية أنظمة المعلومات الخاصة بها والحفاظ على ثقة العملاء وأصحاب المصلحة مع ضرورة فهم ماهية الأمن السيبراني ودراسته دراسة علمية مستفيضة من مختلف جوانبه بعمق بوصفه متغيراً جديداً في العلاقات الدولية.

وعلى الرغم من الاهتمام الواسع الذي حُظي به موضوع الأمن السيبراني وحماية نظم المعلومات في الأدبيات العالمية، والتي منها دراسة Sekhar & Kumar (2023)، Zolait et al. (2008). إلا أن الدراسات المحلية والعربية لم تتطرق بعد إلى هذا الموضوع وبنفس الأبعاد على حد علم الباحث، خاصةً فيما يتعلق بالبنوك اليمنية، وهذا النقص في البحث العلمي المحلي والعربي يُبرز فجوة معرفية مهمة، ويُشير إلى ضرورة إجراء دراسات تركز على تأثير متطلبات الأمن السيبراني على حماية نظم المعلومات في هذا القطاع الحيوي، ولهذا تأتي أهمية الدراسة الحالية التي تهدف

إلى سد هذه الفجوة وتقديم إسهامات جديدة في هذا المجال، مع التركيز بشكل خاص على البنوك اليمنية.

2.1 مشكلة الدراسة (Study problem):

لقد أتاح التطور المذهل الذي شهدته صناعة التقنيات المالية الكثير من الفرص أمام المصارف نحو تعزيز مستوى الخدمات المقدمة للعملاء من خلال قنوات جديدة مبتكرة بعيداً عن القنوات التقليدية التي اعتادت عليها المصارف لتقديم الخدمات المصرفية لعملائها، مما أحدث تحولا جذريا في طريقة عمل القطاع المصرفي، فقد أسهم التطور التقني في قيام المصارف بتقديم الخدمات المصرفية من خلال المعاملات الإلكترونية، الأمر الذي أدى إلى توفير الوقت والمال والجهد من خلال تلك القنوات الجديدة المبتكرة (صندوق النقد العربي ، 2019).

ومع ظهور أنواع جديدة ومعقدة من الأجهزة المتصلة بالأنترنت وازدياد الاعتماد عليها في الأنشطة المختلفة في المجتمع الحديث، وما توفره من أرضية غنية بالإمكانيات التي تبدو غير محدودة للأنشطة الاقتصادية المهمة، أصبحت وسيلة ضرورية لمعالجة المعاملات التجارية على المستوى الدولي، ووسيلة ملائمة لتلبية احتياجات المستهلكين، التي يمكن تلبيتها بجودة عالية وتكلفة منخفضة، وفي الوقت نفسه، يمكن للمستخدم التواصل مع الآخرين في جميع أنحاء العالم وتبادل المعلومات في سرية تامة(Grandon Gill & DBA, 2018) .

وفي هذا الإطار، يجد المتسللون للأنترنت ثغرات عديدة يعملون على استغلالها في بنيته لقراءة أو حذف أو تعديل البيانات الموجودة على أجهزة الحاسوب أو المنتقلة بينها. وقد كشفت دراسة خالد (2020) عن تعرض كثير من المواقع اليمنية للاختراقات، حيث كشفت إحصائية المنتدى العربي لحوكمة الإنترنت ESCWA إلى تعرض أكثر من 86 موقعاً يمنياً للاختراق خلال

عامي 2012 – 2014 م، وأظهرت الدراسة حجم الفجوة التي تفصلنا عن كثير من البلدان في المنطقة، التي سبقتنا بخطوات في بناء قدراتها الدفاعية في مجالات الأمن السيبراني وتحدياته، وفي الوقت الذي سهلت فيه تقنية الاتصالات والمعلومات والجيل الخامس من الأنترنت الكثير في حياة الناس اليومية فإنها فرضت وتفرض العديد من التحديات في مقدمتها الجرائم السيبرانية.

ويعد افتقار البنوك اليمنية للفهم الشامل لتلك العلاقة التي تربط متطلبات الأمن السيبراني والوضع الأمني عائقا يحد من قدرة صانعي السياسات وإدارة البنوك على تطوير وتنفيذ استراتيجيات فعالة للأمن السيبراني (المسلمي، 2019 فبراير). الأمر الذي يترك البنوك عرضة للهجمات الإلكترونية، وتعرضها لخسائر مالية وإضرار بالسمعة وفقدان ثقة العملاء، وبناء على ما سبق يمكن بلورة مشكلة الدراسة في التساؤلات التالية:

السؤال الرئيس: ما أثر توافر متطلبات الأمن السيبراني بأبعادها (التنظيمية – والفنية والمادية – والامتثال للأطر والمعايير الدولية) في حماية نظم المعلومات في البنوك اليمنية ؟

ويتفرع منه التساؤلات التالية:

1- ما مدى توافر متطلبات الأمن السيبراني في البنوك اليمنية؟

2- ما مستوى حماية نظم المعلومات في البنوك اليمنية؟

3- ما أثر توافر المتطلبات التنظيمية في حماية نظم المعلومات في البنوك اليمنية؟

4- ما أثر توافر المتطلبات الفنية في حماية نظم المعلومات في البنوك اليمنية؟

5- ما أثر توافر متطلبات الامتثال للأطر والمعايير الدولية في حماية نظم المعلومات في البنوك اليمنية؟

6- ما أثر توافر المتطلبات المادية في حماية نظم المعلومات في البنوك اليمنية؟

3.1 أهمية الدراسة(Importance of the study):

تكمن أهمية هذه الدراسة من خلال تسليط الضوء على النقاط التالية:

1.3.1 الأهمية النظرية (Theoretical significance):

1. تعد هذه الدراسة ضمن الدراسات اليمنية القليلة والحديثة المتخصصة في مجال الأمن السيبراني على حد علمي التي بمقدورها الإسهام في إثراء الإنتاج الفكري والعلمي في هذا المجال.
2. تزويد صناع القرار بالمعلومات المفيدة التي تدور حول المشاكل والمعوقات التي تفرض وجود الأمن السيبراني، والعمل على تحسينها من أجل تحقيق الميزة التنافسية للبنوك، وحماية المعلومات الإلكترونية من الهجمات المتكررة، وإنشاء استراتيجيات دفاعية؛ بهدف التقليل من الهجمات الإلكترونية الجديدة.
3. تعد مرجعاً للباحثين والمهتمين في هذا المجال ورافداً للمكتبة اليمنية.

2.3.1 الأهمية التطبيقية (Applied importance):

1. تعزيز أمن أنظمة المعلومات في البنوك من خلال تقديم حلول وتوصيات حول الوضع الحالي للأمن السيبراني في البنوك وتحديد الثغرات ونقاط الضعف في التدابير الأمنية الحالية. والمساعدة في تحديد أفضل الممارسات لتعزيز أمن نظم المعلومات في البنوك .
2. تحفيز البنوك اليمنية لتطبيق المعايير واللوائح المتعلقة بالأمن السيبراني.
3. تقييم تأثير تدابير الأمن السيبراني على الأمن العام لأنظمة المعلومات في البنوك، والمساهمة في تحديد فعالية التدابير الحالية في معالجة تهديدات الأمن السيبراني الشائعة .

4. تحدد مدى تأثير التقنيات الجديدة مثل الحوسبة السحابية وإنترنت الأشياء على الأمن السيبراني لأنظمة المعلومات في البنوك، وتساعد في تحديد المخاطر المحتملة واستراتيجيات التخفيف .

5. الحد من الآثار المالية والسمعة المحتملة لخرق الأمن السيبراني على البنك، وتساعد في تحديد التدابير لتقليل هذه الآثار .

4.1 أهداف الدراسة (Objectives of the study):

الهدف الرئيس: التعرف على أثر متطلبات الأمن السيبراني بأبعادها (التنظيمية – والفنية والمادية – والامتثال للأطر والمعايير الدولية) في حماية نظم المعلومات في البنوك اليمنية، وتتفرع منه الأهداف التالية:

1. التعرف على مدى توافر متطلبات الأمن السيبراني في البنوك اليمنية.
2. التعرف على مستوى حماية نظم المعلومات في البنوك اليمنية.
3. التعرف على توافر المتطلبات التنظيمية في حماية نظم المعلومات في البنوك اليمنية.
4. التعرف على توافر المتطلبات الفنية في حماية نظم المعلومات في البنوك اليمنية.
5. التعرف على توافر متطلبات الامتثال للأطر والمعايير الدولية في حماية نظم المعلومات في البنوك اليمنية.
6. التعرف على أثر توافر المتطلبات المادية في حماية نظم المعلومات في البنوك اليمنية.

5.1.الأنموذج المعرفي للدراسة (*The cognitive model of the study*):

يتكون الأنموذج المعرفي للدراسة من المتغير المستقل (متطلبات الأمن السيبراني) والمتغير التابع (حماية نظم المعلومات)، وفيما يلي بيان هذين المتغيرين ومكوناتهما:

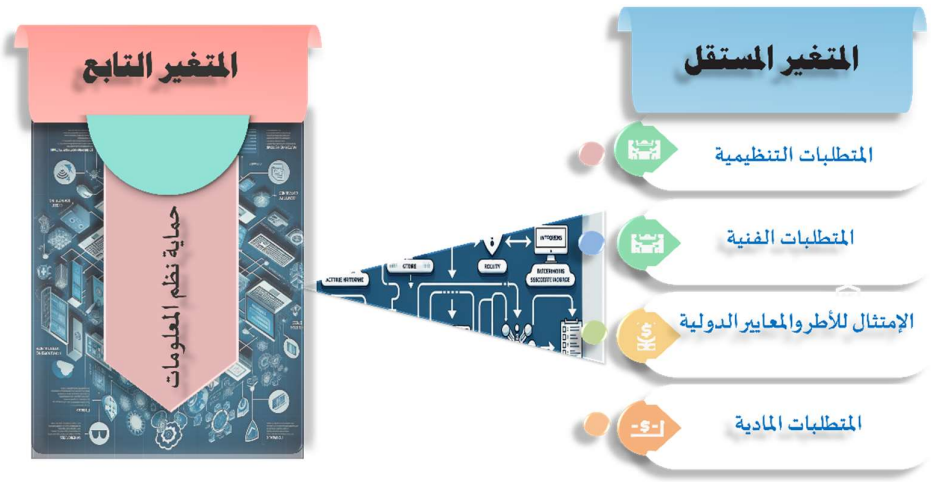
1. المتغير المستقل (متطلبات الأمن السيبراني): ويشمل المتطلبات التنظيمية، المتطلبات الفنية، المتطلبات المادية، والامتثال للمعايير الدولية، تم تحديد أبعاد هذا المتغير استنادا إلى دراسة: السرحان، (2020)، نبيلة، (2022)- (2022) ABDUALMAJED & et al ودراسة Nasser, Al-Anesi, Hazaa, & et al., (2022) ودراسة (Al-Ramadan & Hasan, (2021.

2. المتغير التابع (حماية نظم المعلومات): ويشمل الإجراءات والتدابير الضرورية لحماية نظم المعلومات وتم تحديد هذه الإجراءات والتدابير استنادا إلى دراسة Alsharabi, (2020) و Amanullah & Khan, (2019) ودراسة Gomes, Deshmukh, & Anute, (2022).

والشكل رقم (1.1) يوضح ذلك.

الشكل: 1.1

الأنموذج المعرفي للدراسة



المصدر. من إعداد الباحث بالاعتماد على الدراسات السابقة.

6.1 فرضيات الدراسة (Study hypotheses):

بناءً على أهداف الدراسة وأسئلته، تقترح الدراسة صياغة الفرضيات التالية:

1.6.1 الفرضية الرئيسية الأولى (The first main hypothesis):

وتنص على أنه "**لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($p \leq 0.05$) لمستويات توافر متطلبات الأمن السيبراني في مستويات حماية أنظمة المعلومات في البنوك اليمنية**".

وتتفرع منها الفرضيات الفرعية التالية:

1. لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($p \leq 0.05$) للمتطلبات التنظيمية للأمن السيبراني في حماية أنظمة المعلومات في البنوك اليمنية.
2. لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($p \leq 0.05$) للمتطلبات الفنية للأمن السيبراني في حماية أنظمة المعلومات في البنوك اليمنية.
3. لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($p \leq 0.05$) لمتطلبات الامتثال للأطر والمعايير للأمن السيبراني على حماية أنظمة المعلومات في البنوك اليمنية.
4. لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($p \leq 0.05$) للمتطلبات المادية للأمن السيبراني على حماية أنظمة المعلومات في البنوك اليمنية.

2.6.1 الفرضية الرئيسية الثانية (Second main hypothesis):

تنص على أنه "لا توجد فروق جوهرية بين متوسطات استجابات أفراد العينة حول مستويات توافر متطلبات الأمن السيبراني وأثرها في حماية نظم المعلومات تعزى إلى المتغيرات الديموغرافية".

7.1 حدود الدراسة (Limitations of the study):

تتمثل حدود الدراسة الحالية في الآتي:

1.7.1 الحدود الموضوعية (Objective limits): تنحصر في التعرف الى أثر متطلبات الأمن السيبراني (المتطلبات التنظيمية والفنية والامتثال للأطر والمعايير الدولية وتدابير الأمن المادي) في حماية نظم المعلومات في البنوك اليمنية.

2.7.1 الحدود البشرية (Human limits): تقتصر الدراسة الحالية على جميع موظفي البنوك اليمنية بجميع المستويات الإدارات.

3.7.1 الحدود المكانية (Spatial boundaries): تقتصر الدراسة الحالية على عينة من فروع البنوك اليمنية (الحكومية والإسلامية والتجارية) في محافظتي تعز وعدن.

4.7.1. الحدود الزمانية (Temporal limits): تم التطبيق الميداني للدراسة الحالية في العام الجامعي 2023م.

8.1 الدراسات السابقة (Previous studies):

هناك عدد من الدراسات التي تناولت موضوع الأمن السيبراني وحماية أمن المعلومات في مجالات مختلفة، وفقا من الأحداث الى الأقدم حسب منهج APA7، وأبرز تلك الدراسات الآتي:

1. **دراسة (Sekhar&Kumar,2023) بعنوان: "An Overview of Cyber Security in Digital Banking Sector"**

هدفت الدراسة إلى تقديم نظرة عامة على الأمن السيبراني في قطاع البنوك الرقمية، وتحليل الهجمات الإلكترونية في هذا القطاع وطرائق توفير الأمن السيبراني لمواجهة هذه الهجمات.

واستخدمت الدراسة منهجية نظرية وتحليلية، لاستكشاف أنواع التهديدات الإلكترونية مثل البيانات غير المشفرة والبرمجيات الخبيثة والهجمات عبر الخدمات الثالثة، وتقنيات التصيد الاحتيالي، والاستغلال عبر الأجهزة المحمولة. وتضمنت عينة الدراسة تحليل للهجمات الإلكترونية التي تعرضت لها البنوك حول العالم في عام 2021، مع التركيز على محاولات الحصول على معلومات حساسة من خلال القنوات عبر الأنترنت في عدة قطاعات.

توصلت الدراسة إلى أن هناك زيادة في جرائم السيبرانية ذات الصلة بأجهزة الصراف الآلي، وبطاقات السحب والخدمات المصرفية عبر الأنترنت، مع التركيز على أن البنوك تواجه هجمات إلكترونية أكثر بكثير مقارنة بقطاعات أخرى. أوصت الدراسة على أهمية تطبيق تقنيات الأمان السيبراني ورفع مستوى الوعي بين المستخدمين والمؤسسات المالية، بالإضافة إلى الحاجة لاستخدام تطبيقات مضادة للبرمجيات الخبيثة.

2. دراسة (Khaleefah&Al-Mashhadi,2023) بعنوان: "Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review".

هدفت الدراسة إلى استعراض منهجيات ومتطلبات وتحديات إطارات الأمن السيبراني، مع التركيز على إطارات العمل المقترحة من قبل المنظمات القياسية مثل ISO وNIST، بالإضافة إلى الإطارات الأخرى المقترحة من الباحثين. واستخدمت الدراسة المنهج التحليلي الاستعراضي، ولم تُذكر عينة محددة حيث كانت الدراسة استعراضية بطبيعتها.

توصلت الدراسة إلى أنه على الرغم من التكامل الحاصل في شبكات البيانات والنماذج الحاسوبية والبرمجيات الموزعة، فإن حلول الأمن ما تزال تشكل تحدياً كبيراً وتحتاج إلى المزيد من العمل

لتعزيز متطلبات الأمن مثل الثقة المتبادلة بين الكيانات، والتحكم في الوصول وإدارة الهوية، وحماية البيانات، والكشف عن الهجمات ومنعها أو التهديدات. وأوصت الدراسة بأن الأفكار المشتركة الموصوفة في هذه الدراسة يمكن أن تكون مفيدة لإنشاء نموذج عام لإطار العمل الأمني السيبراني.

3. دراسة (Abdualmajed, AL-Khulaidi,2023) بعنوان: " Information security gap analysis: an applied study on the Yemeni banking sector technology and innovation practices"

هدفت الدراسة إلى تحليل مستوى الامتثال لأنظمة إدارة أمن المعلومات في البنوك اليمنية مع ضوابط التكنولوجيا والابتكار، وتحديد نقاط القوة والضعف في هذه الممارسات، واقتراح حلول لسد الفجوات الأمنية الموجودة. واستخدمت الدراسة المنهج التحليلي والوصفي للفجوات بالاعتماد على دراسات سابقة واختيار أطر تقييم ونماذج نضج ملائمة، شملت عينة الدراسة 13 بنكًا محليًا في العاصمة اليمنية صنعاء، حيث تم جمع البيانات من خلال استبيانات موزعة على 26 خبيرًا.

توصلت الدراسة إلى أن مستوى النضج الأمني المعلوماتي في القطاع المصرفي يفي بالمتطلبات الرئيسية لأمن المعلومات، لكن يظل هناك فجوة بمقدار 1.1 عن المستوى المثالي المطلوب. كما وفرت الدراسة نتائج مفصلة عن مستويات النضج والضعف، ومتوسط الفجوات في ممارسات التكنولوجيا والابتكار. وبناءً على هذه النتائج، تم تحديد المؤشرات وتصنيفها وترتيبها التي تظهر الضعف التكنولوجي الأكثر احتمالية في البنوك والمستوى المتوسط للفجوات الأمنية التي يجب التقليل منها.

وقد أوصت الدراسة بأنه يجب على القطاع المصرفي تعزيز ممارساته الأمنية المعلوماتية من خلال الاستعانة بحلول مبتكرة ومعاصرة تتماشى مع ضوابط الأمن القوي في مجال التكنولوجيا

والابتكار، واعتماد استراتيجيات وسياسات وأدوات تكنولوجية ومبتكرة تغطي جميع المؤشرات التكنولوجية.

4.دراسة (Taherdoost,2022) بعنوان: "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview".

هدفت الدراسة إلى توفير نظرة شاملة وفهم متعمق لإطارات الأمن السيبراني ومعايير الأمن المعلوماتي. واستخدمت الدراسة المنهج الاستعراضي لتقديم مراجعة واسعة النطاق للمعايير والإطارات الحالية، دون الإشارة إلى عينة محددة نظرًا لطبيعة الدراسة الاستعراضية.

توصلت الدراسة إلى أن فهم الإطارات والمعايير يمكن أن يعزز من تطوير استراتيجيات الأمن السيبراني وتنفيذ الحماية المعلوماتية الفعالة في المؤسسات المختلفة.

أوصت الدراسة إلى بذل مزيد من الدراسة والتطوير في مجالات معايير الأمن المعلوماتي وتطبيقاتها، بالإضافة إلى تبني وتحديث الإطارات الأمنية لتواكب التطورات التكنولوجية والتهديدات السيبرانية المستجدة.

5.دراسة (Gomes, Deshmukh & Anute ,2022) بعنوان: "Cyber Security and Internet Banking: Issues and Preventive Measures"

هدفت الدراسة إلى استكشاف القضايا الأمنية السيبرانية في مجال الخدمات المصرفية عبر الأنترنت في الهند ومستوى وعي المستهلكين بهذه القضايا والإجراءات الوقائية التي يتخذونها. واستخدمت الدراسة المنهج الاستقصائي، حيث اعتمدت على بيانات أولية جمعت عن طريق استبانة

تم توزيعها وكانت عينة الدراسة تضم 200 مشارك، الذين تم استطلاع آرائهم بشأن معرفتهم بالتهديدات السيبرانية وتجاربهم مع الاحتيال المصرفي عبر الأنترنت.

توصلت الدراسة إلى نتائج تُظهر أن الإجراءات الأمنية السيبرانية المتبعة على مواقع البنوك لا تُحدّث بالسرعة الكافية لمواكبة التهديدات السيبرانية المتطورة، مما يُسهل سقوط المعلومات المالية السرية في أيدي أطراف ثالثة ومجرمين سيبرانيين. وعلى الرغم من وجود العديد من الإجراءات الأمنية لوقف الخروقات البيانية، ما تزال هناك ثغرات في هذه الأنظمة، وأوصت الدراسة إلى الحاجة الملحة لتحسين وعي المستهلكين بالمخاطر السيبرانية وتشجيعهم على اتخاذ إجراءات وقائية أكثر صرامة

6.دراسة (Shulha et al, 2022) بعنوان: "Banking Information Resource Cybersecurity System Modeling".

هدفت الدراسة إلى إنشاء نماذج معرفية وظيفية لتقييم مستوى حماية البنوك الإلكترونية. واستخدمت الدراسة منهج تطوير خرائط معرفية ضبابية لتحديد حالة الأمن السيبراني للبنوك. وكانت عينة الدراسة تتضمن نماذج معرفية لتحديد مستوى حماية شبكة الحاسوب ونظام أمن المعلومات، والبنية التحتية الحرجة للبنوك. حيث توصلت الدراسة إلى تطوير سيناريوهات تعكس استجابة النظام لأقصى تقليل ممكن لتأثير أهم التهديدات السيبرانية.

وأوصت الدراسة بأن تنفيذ هذه الطريقة عمليًا يوفر فرصة للتنبؤ بحالة الأمن السيبراني للبنوك، ويسهم في تنفيذ الآليات الضرورية للوقاية والحماية والتحكم في الوصول على المستويات المناسبة من بنية الشبكة التحتية.

7.دراسة (الحداد,2022) بعنوان: " متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية دراسة حالة"

هدفت الدراسة إلى التحقق من متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية والتحقق من واقع الأمن السيبراني فيها واستخدمت الدراسة المنهج الوصفي التحليلي مع استخدام أدوات المقابلة والملاحظة بالمشاركة وكانت عينة الدراسة تتكون من 8 خبراء ومتخصصين في مجال الإدارة التربوية وتكنولوجيا المعلومات من مختلف الجامعات اليمنية. وتوصلت الدراسة إلى أن الأمن السيبراني يسهم في الحفاظ على أمن البيانات وسريتها في المكتبات الجامعية، ويساعد في التصدي للهجمات الخارجية وتفادي الجرائم الإلكترونية. وأوصت الدراسة بضرورة توفير أنظمة حماية خاصة للبيانات والمعلومات، وفتح مجالات تكنولوجية مختلفة في الجامعات لدعم الأمن السيبراني.

8.دراسة (Hasan & Al-Ramadan ,2021) بعنوان "Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case".

هدفت الدراسة إلى تقييم جاهزية البنوك العراقية الخاصة لمواجهة الهجمات السيبرانية وفهم رد فعل أنظمة الأمن السيبراني تجاه تلك الهجمات، بالإضافة إلى تأثير تلك الهجمات في تحفيز البنوك لزيادة احتياطاتها لحماية قواعد البيانات والخوادم من الانتهاكات. واستخدمت الدراسة المنهج الوصفي التحليلي، وايضا الاستبانة كأداة رئيسية لجمع بيانات المستجيبين حول تجاربهم مع الهجمات السيبرانية في الأعوام السابقة على الأقل. كانت عينة الدراسة تضم مستخدمين من البنوك الخاصة العراقية الذين عانوا من هجمات سيبرانية .حيث توصلت الدراسة إلى نتائج تُظهر أن البنوك الخاصة العراقية تحافظ على مستوى معين من الأمان بغض النظر عن شدة الهجمات

السيبرانية، ومع ذلك، وبعض المستجيبين ما يزالون يحذرون من استخدام خدمات البنك عبر الأنترنت بسبب منخفض مستويات الأمان في الوصول العام لخدمات الأنترنت في العراق .وأوصت الدراسة أن البنوك يجب أن تستمر في تطوير وتعزيز إجراءات الأمان السيبراني لديها، وذلك للحفاظ على الأمان المالي والشخصي لعملائها، والحد من المخاطر المرتبطة بالهجمات السيبرانية والجرائم المعلوماتية.

9.دراسة (السرحان & المشاقبة ,2020) بعنوان: "أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية".

هدفت الدراسة إلى استكشاف أثر تطبيق سياسة الأمن السيبراني في جودة المعلومات المحاسبية في البنوك التجارية الأردنية. واستخدمت الدراسة المنهج الوصفي مع استبانة كانت أداة رئيسية لجمع البيانات من مجتمع الدراسة المكون من البنوك التجارية العاملة في الأردن. وتم تحليل البيانات باستخدام برنامج SPSS ، وكشفت نتائج الدراسة عن وجود تأثير ملموس لخصوصية بيانات العملاء، وإدارة المخاطر السيبرانية، ومعايير تحديد الجهة المالكة ونطاق التطبيق والصلاحيات في جودة المعلومات المحاسبية. بالإضافة لوجود علاقة ارتباط معنوية بين تطبيق سياسات الأمن السيبراني وتحسين جودة المعلومات المحاسبية. وبناءً على هذه النتائج، أوصت الدراسة البنوك بضرورة تعزيز الإجراءات الأمنية لحماية خصوصية بيانات العملاء والإفصاح عن جهود الأمن السيبراني في التقارير السنوية للبنوك، مع تشجيع المزيد من الدراسة في مجال الأمن السيبراني وأثره في البيئة المصرفية.

10.دراسة (Nasser, Al Ansi, & Al Sharabi ,2020) بعنوان "On The Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen".

هدفت الدراسة إلى بحث فعالية ممارسات التوحيد القياسي لعمليات أمن المعلومات في البنوك اليمنية من خلال التحقيق في المتطلبات الأساسية لتنفيذها لأداء أدوارها الأمنية بفعالية. كما سعت الدراسة إلى تحديد نقاط الضعف الرئيسية في نظم إدارة الأمن المعلوماتي (ISMS) لقطاع البنك بناءً على المعيار الأمني الدولي .ISO 27002–2013 .واستخدمت الدراسة المنهج الوصفي حيث صمم استبيانًا وزع على العاملين المسؤولين عن بيانات أمن المعلومات في 13 بنكًا تحت إشراف البنك المركزي اليمني في صنعاء. كانت عينة الدراسة تشمل العاملين في قطاع البنوك المعنيين بأمن المعلومات.

كشفت نتائج الدراسة أن مستوى النضج الفعلي لممارسات أمن المعلومات هو 3.66 من 5، مما يعني أن الممارسات الأفضل ليست متبعة باستمرار. كما تم العثور على فجوة بين مستوى النضج الفعلي لتطبيق ممارسات أمن المعلومات والمستوى القوي، وكانت 1.34، مما يعني أن نظم (ISMS) في هذا القطاع لا تمتلك معظم متطلبات الأمن الضرورية لتشغيلها العملي والقوي. تم تحديد نقطتين رئيسيتين للقوة، وثلاث نقاط ضعف ونقاط ضعف رئيسية، وأوصت الدراسة بضرورة تنفيذ خطط توجيهية مبنية على (ISO) لكل بنك.

11.دراسة (الدحياني & الصنوي , 2020) بعنوان: " متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء."

هدفت الدراسة إلى تحديد متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المتخصصين. استخدمت الدراسة المنهج الوصفي الاستقصائي، وتم تصميم استبانة تغطي أربع مجالات: المتطلبات التشريعية، البشرية، والمالية والفنية لجمع البيانات. شملت عينة الدراسة 70 متخصصاً في مجال الحاسوب، والتكنولوجيا، والذكاء الاصطناعي. وقد توصلت الدراسة إلى أن درجة الموافقة على متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية كانت مرتفعة جدًا

من وجهة نظر المتخصصين، سواء على مستوى الأداة ككل أو على مستوى كل مجال من مجالات الدراسة. وكشفت النتائج عن عدم وجود فروق ذات دلالة إحصائية في إجابات عينة الدراسة تبعًا للمتغيرات الديموغرافية كالجنس، وسنوات الخبرة العملية في هذا التخصص، سواء على مستوى الدرجة الكلية للأداة أو لكل مجال من مجالات الدراسة.

12.دراسة (Amanullah & Khan ,2019) بعنوان: "Cybersecurity Challenges of the Kingdom of Saudi Arabia: Past, Present and Future".

هدفت الدراسة إلى استعراض التحديات السيبرانية التي تواجه المملكة العربية السعودية، وتقييم الجهود المبذولة لتعزيز أمن تقنية المعلومات والاتصالات، والتعرف الى المبادرات والاستثمارات التي قامت بها الدولة لتحقيق رؤية اقتصاد مؤمن رقميًا. وتناولت الدراسة أيضًا التطورات الحالية والماضية في مجال الأمن السيبراني بالمملكة وكيف أثرت الهجمات السيبرانية في إعادة تقييم البنية التحتية لتقنية المعلومات والقدرات السيبرانية الدفاعية والهجومية. والمنهج المتبع لم يُذكر بوضوح، ولكن يُستشف أنه تحليلي استراتيجي، ولم يُذكر بوضوح كيف تم جمع البيانات أو إذا كانت هناك عينة محددة شملتها الدراسة، ولكن يبدو أن الدراسة يعتمد على تحليل للمبادرات الحالية وتقييم الأحداث السابقة.

وتوصلت الدراسة إلى أن السعودية تبذل جهودًا متواصلة لحماية البيانات والخصوصية في القطاعين العام والخاص وأن البنية التحتية السيبرانية في المملكة ما زالت في طور النمو. إضافة إلى أن الهجمات السيبرانية السابقة دفعت صانعي القرار لإعادة تقييم قدراتهم السيبرانية لمواجهة التهديدات المتزايدة والمتطورة.

وأوصت الدراسة باتخاذ إجراءات استراتيجية وتشغيلية وتكتيكية وتحسين القدرات لتمكين المملكة من تعزيز قدراتها السيبرانية، ليس بوصفها دولة، ولكن أيضًا بوصفها عضواً رائداً في جبهة الدفاع السيبراني الجماعي مع حلفائها في الشرق الأوسط.

13.دراسة (الشمالي ,2016) بعنوان: "أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن ."

هدفت الدراسة إلى تقييم أمن وسرية المعلومات وأثرهما في الأداء المصرفي في البنوك العاملة في الأردن. واستخدمت الدراسة المنهج الوصفي، حيث تم اختيار عينة طبقية عشوائية بنسبة 50% من مجتمع الدراسة المتمثل بالبنوك العاملة في الأردن. وتوصلت الدراسة إلى أن ممارسات أمن المعلومات وسريتها في البنوك الأردنية تتم بمستوى مرتفع من حيث الأهمية النسبية، وكذلك الأداء المصرفي الذي يُظهر مستويات مرتفعة من الأهمية النسبية. وكان لأمن المعلومات أثر ذو دلالة إحصائية في الأداء المصرفي في هذه البنوك. وأوصت الدراسة بضرورة قيام إدارة البنوك بنشر وتعميق ثقافة أمن وسرية المعلومات على مختلف المستويات الإدارية من خلال إعداد برامج تدريبية لجميع المستويات الإدارية، وزيادة الإنفاق على برامج أمن البرمجيات والمعلومات السرية، والسعي الى الحصول على الشهادات الدولية المطابقة للأنظمة الدولية لأمن المعلومات.

14.دراسة (Zolait et al., 2008) بعنوان: "Prospective and challenges of internet banking in Yemen: an analysis of bank websites".

هدفت الدراسة إلى قياس مدى ميل البنوك في اليمن نحو تبني الخدمات المصرفية عبر الأنترنت، وتحليل كيفية استخدام القطاع المصرفي اليمني لتقنية الأنترنت من خلال تقييم مواقع البنوك. واستخدمت الدراسة منهج تحليلي حيث تم النظر في النماذج النظرية والموديلات لتقييم

المواقع الإلكترونية، بالإضافة إلى تحليل عملي لمواقع البنوك اليمنية القائمة وفقًا لإرشادات هذه النماذج. وكانت عينة الدراسة تشمل مواقع البنوك في اليمن.

وتوصلت الدراسة إلى تصنيف تقنيات تقييم المواقع إلى ثلاث فئات هي: الاستخدام، والتفاعلية، والمحتوى، وتم استخدام هذه التقنيات في تقييم مواقع البنوك في اليمن، وأوصت الدراسة بضرورة تحسين مواقع البنوك اليمنية فيما يتعلق بالاستخدام، والتفاعلية والمحتوى لتشجيع التبني الأوسع للخدمات المصرفية عبر الأنترنت، وتوفير تجربة مستخدم أفضل للعملاء.

9.1. التعليق على الدراسات السابقة (Comment on previous studies):

بناءً على نتائج الدراسات السابقة وإجراءاتها، تم إجراء مقارنة بين أوجه التشابه والاختلاف مع الدراسة الحالية والاستفادة من الدراسات السابقة، وعلى النحو المبين في الجدول (1) الآتي:

الجدول: 1.1

أوجه التشابه والاختلاف بين الدراسات السابقة والدراسة الحالي

م	عنوان الدراسة	سنة الدراسة	البلد	المنهجية	أداة الدراسة	أهداف الدراسة	نتائج الدراسة	توصيات الدراسة	التشابه	الاختلاف	الاستفادة
.1	An Overview of Cyber Security in Digital Banking Sector	2023	غير مذكور	نظرية وتحليلية	غير مذكورة	نظرة عامة على الأمن السيبراني في البنوك الرقمية	زيادة في جرائم السيبرانية	تطبيق تقنيات الأمان السيبراني ورفع الوعي	تركيز على أمن المعلومات في القطاع المصرفي	تخصصاً في البنوك اليمنية وتستخدم منهجاً وصفياً مسحياً وارتباطياً	يمكن الاستفادة من تحليل الهجمات الإلكترونية في دراستهم
.2	Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review	2023	غير مذكور	تحليلي استعراضي	غير مذكورة	استعراض منهجيات ومتطلبات وتحديات إطارات الأمن السيبراني	التحديات الكبيرة في حلول الأمن	تطوير نموذج عام لإطار الأمن السيبراني	الاهتمام بمتطلبات الأمن السيبراني	تركيزهم على إطارات العمل ومنهجية استعراضية بينما تركز دراستك على التطبيق العملي	استلهام الأفكار حول تحديات الأمن السيبراني
.3	Information security gap analysis: an applied study on the Yemeni banking sector technology and innovation practices	2023	اليمن	تحليلي ووصفي	استبيانات	تحليل مستوى الامتثال لأنظمة أمن المعلومات	فجوة في الأمن المعلوماتي	تعزيز ممارسات الأمن المعلوماتي	تركيز على البنوك اليمنية	دراستهم تركز على تحليل الفجوات بينما تركز دراستك على التأثير والحماية	فهم الفجوات في الأمن المعلوماتي يمكن أن يساعد في تطوير استراتيجيات الأمان
.4	Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview	2022	غير مذكور	استعراضي	غير مذكورة	نظرة شاملة لإطارات الأمن السيبراني	أهمية فهم الإطارات والمعايير	تطوير وتحديث الإطارات الأمنية	الاهتمام بالأمن السيبراني والمعايير	دراستهم نظرية واستعراضية بينما تركز دراستك على التطبيق العملي	الاستفادة من فهم الإطارات والمعايير لتحسين الأمان في البنوك اليمنية
.5	Cyber Security and Internet Banking: Issues and Preventive Measures	2022	الهند	استقصائي	استبانة	استكشاف القضايا الأمنية في الخدمات المصرفية عبر الإنترنت	الإجراءات الأمنية لا تحدث بالسرعة الكافية	تحسين وعي المستهلكين بالمخاطر السيبرانية	التركيز على الأمن السيبراني في البنوك	دراستهم تركز على الهند وتستخدم منهج استقصائي بينما تركز دراستك على اليمن	استخدام نتائجهم لفهم التحديات الأمنية وتطوير الحماية
.6	Banking Information Resource Cybersecurity System Modeling	2022	غير مذكور	تطوير خرائط معرفية ضبابية	غير مذكورة	إنشاء نماذج معرفية لحماية البنوك الإلكترونية	تطوير سيناريوهات لتقليل التهديدات السيبرانية	تنفيذ الطريقة للتنبؤ بحالة الأمن السيبراني			
.7	متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية دراسة حالة	2022	اليمن	وصفي تحليلي	مقابلات وملاحظات	التحقق من متطلبات الأمن السيبراني	الأمن السيبراني يساعد في حماية البيانات	توفير أنظمة حماية خاصة للبيانات	التركيز على أمن البنوك الإلكترونية	دراستهم تستخدم نماذج معرفية ضبابية، بينما دراستك تركز على التأثيرات الواقعية للأمن السيبراني	الاستفادة من نماذجهم لتحليل وتقييم أمن البيانات
.8	Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case	2021	العراق	وصفي تحليلي	استبانة	تقييم جاهزية البنوك لمواجهة الهجمات السيبرانية	البنوك تحافظ على مستوى معين من الأمان	تطوير إجراءات الأمان السيبراني	تركيز على الأمن السيبراني في اليمن	دراستهم في المكتبات الجامعية وتستخدم مقابلات، بينما تركز دراستك على البنوك	الاستفادة من تجاربهم في تحليل متطلبات الأمن السيبراني

.9	أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية فى البنوك التجارية الأردنية	2020	الأردن	وصفي	استبانة	استكشاف أثر سياسة الأمن السيبراني	تأثير ملموس على جودة المعلومات المحاسبية	تعزيز الإجراءات الأمنية لحماية البيانات	التركيز على البنوك والأمن السيبراني	دراستهم فى العراق وتقييم الجاهزية، بينما دراستك تركز على التأثير والحماية فى اليمن	الاستفادة من تجربتهم في تقييم الجاهزية لتحسين الأمن في البنوك اليمنية
.10	On The Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen	2020	اليمن	وصفي	استبانة	بحث فعالية ممارسات التوحيد القياسي لأمن المعلومات	فجوة بين الممارسات والمستوى القوي	تنفيذ خطط توجيهية مبنية على (ISO)	التركيز على تأثير الأمن السيبراني	تركيزهم على المعلومات المحاسبية في الأردن، بينما دراستك تركز على الأمان السيبراني بشكل عام في اليمن	استخدام نتائجهم لفهم تأثير الأمان على أقسام مختلفة في البنوك
.11	متطلبات تطبيق الأمن السيبرانى فى الجامعات اليمنية من وجهة نظر الخبراء	2020	اليمن	وصفي استقصائي	استبانة	تحديد متطلبات تطبيق الأمن السيبراني	درجة موافقة مرتفعة على متطلبات التطبيق	غير متكررة	التركيز على البنوك في اليمن	دراستهم تركز على التوحيد القياسي، بينما دراستك تركز على الأمان وحماية النظم المعلوماتية	تحليل نقاط القوة والضعف في ممارسات الأمن المعلوماتي
.12	Cybersecurity Challenges of the Kingdom of Saudi Arabia: Past, Present and Future	2019	السعودية	تحليلي استراتيجي	غير متكررة	استعراض التحديات السيبرانية	جهود متواصلة لحماية البيانات والخصوصية	تحسين القدرات السيبرانية	التركيز على الأمن السيبراني في اليمن	تركيزهم على الجامعات، بينما دراستك تركز على البنوك	الاستفادة من وجهات نظر الخبراء في تطبيق الأمن السيبراني
.13	أمن وسرية المعلومات وأثرها فى الأداء المصرفى: دراسة تطبيقية على البنوك العاملة في الأردن	2016	الأردن	وصفي	عينة طبقية عشوائية	تقييم أمن وسرية المعلومات			الاهتمام بالتحديات الأمنية السيبرانية	تركيزهم على السعودية وبنية تحليلية استراتيجية، بينما دراستك تركز على البنوك اليمنية	تحليل التحديات لتحسين الأمان السيبراني في اليمن
.14	Prospective and challenges of internet banking in Yemen: an analysis of bank websites	2008	اليمن	تحليلي	تحليل لمواقع البنوك	قياس ميل البنوك نحو الخدمات المصرفية عبر الأنترنت	تصنيف تقنيات تقييم المواقع	تحسين مواقع البنوك فيما يتعلق بالاستخدام والتفاعلية والمحتوى	التركيز على البنوك والأمان	تركيزهم على البنوك الأردنية والأداء المصرفي، بينما دراستك تركز على الأمان السيبراني بشكل خاص في اليمن	استخدام نتائجهم لفهم تأثير الأمان على الأداء العام

10.1 التعريفات الإجرائية لمصطلحات الدراسة (Procedural definitions of study terms):

لتحقيق أهداف الدراسة تم تحديد التعريفات الإجرائية للمصطلحات المستخدمة في هذه الدراسة،

هي على النحو الآتي:

1.10.1 الأمن السيبراني (Cyber Security):

يعرف الأمن السيبراني في البنوك اليمنية على أنه مجموعة من التدابير والسياسات والإجراءات التي تتخذها البنوك اليمنية بهدف حماية أنظمة المعلومات والبيانات الحساسة لديها من التهديدات السيبرانية، مثل الاختراقات والاحتيال والبرمجيات الخبيثة والتجسس الإلكتروني.

2.10.1 نظم المعلومات (Information Systems):

يقصد بها في هذه الدراسة بأنها مجموعة من العناصر المترابطة والمتراكبة التي تشكل نظامًا متكاملًا لجمع وتخزين ومعالجة ونقل المعلومات وتوفيرها لاتخاذ القرارات وتنفيذ العمليات وإدارة الموارد التي تستخدمها البنوك اليمنية. وتشمل نظم المعلومات العتاد (الأجهزة والبرامج) والبرمجيات والبنية التحتية للشبكة والبيانات والإجراءات والموارد البشرية المتعلقة بإدارة واستخدام هذه النظم.

3.10.1 البنوك اليمنية (Yemeni Banks):

البنوك هي مؤسسات ماليه مرخصه من قبل البنك المركزي لتقديم حزمه من الخدمات المالية والتمويلية والحفاظ على مدخرات الأفراد والشركات والمساهمة في بناء اقتصاديات البلدان من خلال تمويل المشاريع الاستثمارية والتنمية المستدامة والتي تنعكس إيجابا على رفاهية المجتمعات.

4.10.1 متطلبات الأمان السيبراني (Cybersecurity Requirements):

تعرفها الدراسة الحالية بأنها مجموعة من المتطلبات التنظيمية والفنية والمادية والامتثال للمعايير الخاصة التي تستخدمها البنوك اليمنية لحماية الأنظمة المعلوماتية.

5.10.1 المتطلبات التنظيمية (Regulatory requirements):

يقصد بها الإطار القانوني والتشريعي الذي يحكم ممارسة الأمان السيبراني في البنوك اليمنية، وتشمل هذه المتطلبات القوانين والتشريعات المتعلقة بحماية البيانات الشخصية والتعاملات المالية،

وتأمين الشبكات والأنظمة المعلوماتية، وإجراءات الرقابة والمراقبة، وتدابير الحماية الفنية والتقنية، وتنظيم عمليات الاختبار والتقييم والاستجابة للحوادث السيبرانية.

6.10.1 المتطلبات الفنية (Technical Requirements):

يقصد بها المعايير والمبادئ الفنية التي يجب أن تتبعها البنوك اليمنية لضمان حماية نظام المعلومات الخاص بها من التهديدات السيبرانية.

7.10.1 الامتثال للأطر والمعايير (Compliance with frameworks and standards):

يعني اتباع المتطلبات والمعايير الأمنية والتشريعات المتعلقة بالأمن السيبراني، في قطاع البنوك في اليمن، وذلك من خلال اعتماد سياسات وإجراءات الأمان المناسبة وتنفيذها بشكل صحيح وفعال لحماية نظم المعلومات والبيانات الحساسة للعملاء والمؤسسة.

8.10.1 الأمن المادي (Physical Security):

ويقصد به حماية الأموال والممتلكات التي تملكها وتديرها البنوك اليمنية من أجل الوقاية من الخسائر المحتملة نتيجة للسرقة، أو الاحتيال، أو الكوارث الطبيعية، أو الأحداث السياسية المضطربة وفقاً لأفضل الممارسات والمعايير المصرفية الدولية.

الفصل الثاني:

الإطار النظري للدراسة

الفصل الثاني: الإطار النظري للدراسة

يتناول هذا الفصل دراسة الأمن السيبراني، بشكل شامل موضحا مفهومه وتعريفة، وأهدافه، وأهميته، ومراحل تطوره، ويسلط الضوء على التكنولوجيا المالية في القطاع المصرفي، مرورا بالأمن السيبراني في هذا القطاع، وصولا إلى واقع الأمن السيبراني في البنوك اليمنية.

1.2 الأمن السيبراني (Cyber Security):

أدى التطور التكنولوجي المتسارع دوراً كبيراً في تنوع وتسهيل الخدمات المصرفية وتسهيلها، هذا التطور أحدث ثغرات أمنية مما أدى إلى زيادة المخاطر في هذا القطاع، وأسهم في ظهور الحاجة إلى مفهوم الأمن السيبراني لحماية البيانات والأنظمة المصرفية. وفي الوقت ذاته، شكل هذا التطور تهديداً خطيراً على هذا القطاع من خلال تسهل عمليات الوصول للبيانات واختراق الأنظمة المصرفية من قبل جهات تنشط في هذا المجال، وتجنبا لهذه التهديدات ظهر مفهوم الأمن السيبراني الذي يشير إلى حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات (السمحان، 2020).

1.1.2 تعريف الأمن السيبراني (Definition of cybersecurity):

كلمة "سيبر" "هي مشتقة من مصطلح "السيبرنيتيكا"، والتي تشير إلى دراسة السيطرة والتواصل في الأنظمة، وخاصةً فيما يتعلق بالآلات والحواسيب. في سياق أوسع، يرتبط مصطلح "سيبر" بعالم الرقميات والتكنولوجيا"(Kolářiková, 2019, p. 266)، ويُستخدم بشكل شائع لوصف أي شيء يتعلق بالحواسيب، الإنترنت، أو الواقع الافتراضي. على سبيل المثال، تعابير مثل "الأمن السيبراني"، "الجريمة السيبرانية"، أو "التنمر السيبراني" كلها تتعلق بالقضايا والأنشطة التي تحدث

في المجال الرقمي. عموماً، يُستخدم مصطلح "سيبر" للدلالة على تقاطع التكنولوجيا والتواصل (Kolesnichenko, 2023).

وهناك العديد من التعريفات التي تناولت هذا المصطلح، حيث عرفه صالح والمجالي (2022) بأنه: "مجموعة من المفاهيم الأمنية فضلاً عن الأدوات والسياسات للوصول لضمانات الأمن من ممارسات وتقنيات وأساليب إدارة المخاطر للعمل على حماية البيئة السيبرانية التي تشمل أصول المنظمة والمستخدم، بالتالي توفر السرية والنزاهة" (ص9).

كما عرفه باندي Pandey (2021) بأنه: "عبارة عن "تقنيات منصوص عليها بشكل عام في المواد المنشورة التي تحاول حماية البيئة السيبرانية للمستخدم أو المؤسسة بحيث يدير مجموعة التقنيات المستخدمة لحفظ سلامة الشبكات والبرامج والبيانات من الوصول غير المصرح به" (p.608).

من جهته، عرف السمور، والخزعلي (2020) الأمن السيبراني بأنه: " يشير إلى حماية البيانات وجميع التقنيات المتعلقة بها من وحدات معالجة ومصادر التخزين من التهديدات المرتبطة بالفضاء السيبراني، في حين أن أمن المعلومات يعنى بحماية المعلومات من الوصول غير المصرح به" (ص24).

وأشار اليه الدحياني والصنوي (2021) بأنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"(ص98).

كما عرفه أيضا (الشمالي، 2017) بأنه: "مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحافظ على المعلومات والأجهزة والبرمجيات" (ص190).

ومما سبق يمكن القول إن الأمن السيبراني هو مجموعة السياسات والتعليمات والممارسات، التي بدورها تحافظ على سرية وتكاملية وتوافرية المعلومات والأصول التابعة للشركة من التهديدات والمخاطر في الفضاء السيبراني.

2.1.2 تطور الأمن السيبراني في القطاع المالي (Evolution of Cybersecurity in the Financial Sector):

منذ ظهور الحاسبات في الستينيات من القرن الماضي، بدأ قطاع البنوك في تبني التكنولوجيا لأتمتة عدد من العمليات مثل المعاملات المصرفية والتحويلات المالية، ولكن الثورة الحقيقية جاءت مع إطلاق الأنترنت، حيث أصبح من الممكن إجراء العمليات المصرفية عبر الأنترنت وتوفير الخدمات على مدار الساعة (Rjoub, Adebayo, & Kırıkkaleli, 2023).

وتعد التكنولوجيا المالية مجالًا يشهد تطورًا مستمرًا، وقد مر بعدة مراحل مهمة أدت إلى تبلور مفهوم الأمن السيبراني بوصفه محوراً رئيسياً في هذه الصناعة وفي فترة ما قبل الألفية الجديدة، كانت التكنولوجيا المالية تركز على تطوير الأنظمة الداخلية للمؤسسات المالية، مثل الصراف الآلي ونظم تقييم الائتمان، وهذا التركيز شهد تحولًا جذريًا مع انتشار الأنترنت، حيث تحولت الخدمات المالية إلى الفضاء الإلكتروني، مما سمح للعملاء بإجراء معاملاتهم المالية بشكل إلكتروني وأدى إلى ظهور الحاجة لتأمين هذه المعاملات (Taherdoost, 2022).

ومع ظهور عصر التكنولوجيا المحمولة والحوسبة السحابية، ازدادت حيوية التكنولوجيا المالية، حيث أسهمت هذه التقنيات في إتاحة الخدمات المالية عبر التطبيقات المحمولة والأنظمة السحابية، مما رفع من مستوى التحديات الأمنية وضرورة تعزيز بروتوكولات الأمن السيبراني (Neza, Joseph, & Joseph, 2022). وقد أدى ظهور العملات الرقمية وتكنولوجيا البلوكتشاين إلى

تسليط الضوء بشكل أكبر على قضايا الأمن السيبراني المتعلقة بحماية الأصول الرقمية ومكافحة التهديدات الإلكترونية (Gupta & Pathak, 2023) .

وفي الوقت الراهن، تقوم التحليلات الكبيرة للبيانات وتقنيات الذكاء الاصطناعي بدور محوري في صناعة التكنولوجيا المالية، ليس فقط في تخصيص الخدمات وأتمتة التجارة، بل أيضًا في تعزيز الأمن السيبراني عبر الكشف المبكر عن الأنماط المشبوهة والتنبؤ بالأنشطة الاحتيالية، ومن الضروري الإشارة إلى أن التطورات التكنولوجية المالية قد أوجبت تطبيق تشريعات وقوانين تنظيمية لضمان الأمن والنزاهة المالية، حيث تلزم هذه التشريعات المؤسسات المالية بتبني تدابير أمنية معقدة ومتقدمة لحماية البيانات الشخصية للمستهلكين (Zhang, Liu, & Jumani, 2023).

3.1.2 أهداف الأمن السيبراني (Objectives of Cybersecurity):

في عصر التقنية والإنترنت، أصبح الأمن السيبراني أمرًا بالغ الأهمية للمجتمعات والمؤسسات. حيث أصبح الأنترنت جزءًا حيويًا من حياة الأفراد، والهياكل الحكومية، والشركات، والمنظمات. ويهدف الأمن السيبراني إلى حماية المعلومات والبيانات من التهديدات السيبرانية المتزايدة، مثل عمليات الاحتيال عبر الأنترنت وسرقة الهوية، إلى جانب الحفاظ على الاستقرار المالي للأفراد والمؤسسات. إضافة لما سبق، للأمن السيبراني العديد من الأهداف التي يعمل على تحقيقها وتتضمن ما يلي: (صالح و المجالي، 2022):

1. ضمان الوصول للمعلومات فقط من قبل الأشخاص المخولين بها.
2. عدم السماح بالوصول الى المعلومات إلا للأشخاص المصرح لهم بذلك.
3. ضمان توافر النظام والمعلومات للكيانات المرخص لها فقط.
4. حماية الأنظمة التقنية والبيانات من الاختراقات الخارجية.

5. إمكانية التصدي لأي هجمات تهدد الأمن السيبراني.
6. توفير بيئة آمنة للأفراد والمؤسسات المعرضة للهجمات.
7. زيادة جاهزية البنية التحتية لمواجهة التحديات السيبرانية.
8. تقليل المخاطر والآثار السلبية للجرائم الإلكترونية.
9. تصحيح نقاط الضعف في الأنظمة لمنع الاختراقات غير المصرّح بها.
10. حماية المواطنين وتوعيتهم بأمور الأمن السيبراني.

وفي المجمل، تشير هذه الأهداف إلى الجهود الضرورية لضمان سلامة البيانات والأنظمة الرقمية. كما تعكس حجم التحديات التي تواجهها المؤسسات في مجال الأنترنت وتكنولوجيا المعلومات.

4.1.2 أهمية الأمن السيبراني في القطاع المصرفي (The Importance of Cybersecurity in the Banking Sector):

تعد المؤسسات المالية القطاع الأكثر تعرضًا لهجمات وتحديات أمن المعلومات بسبب استخدام العديد من المنصات القائمة على تكنولوجيا المعلومات في إدارة أعمالها، وينصب التركيز أكثر على التهديدات الخارجية، مع إيلاء اهتمام أقل للمخاطر الداخلية (Usman, Ayoib, & Abdulmalik, 2023) ونتيجة لذلك، هناك ضرورة قصوى لتوفير إطار حوكمة أمن المعلومات لأنظمة المعلومات المصرفية وتوظيف أفضل المعايير والممارسات على المستويات الاستراتيجية والتكتيكية والتشغيلية والتقنية لما قد تتسبب به المخاطر السيبرانية من إلحاق الضرر بسمعة المؤسسات المالية والتأثير في أصولها الأكثر أهمية. ومن ثم، تحليل المخاطر السيبرانية واتخاذ تدابير ضدها له أهمية كبيرة لمديري المؤسسات المالية (Samour & Al-Khazali, 2022).

كما أدت التقنيات الجديدة في نظم المعلومات إلى زيادة عدد الهجمات الإلكترونية، بما في ذلك: البرامج الضارة، برامج الفدية، تهديدات البريد الإلكتروني، التصيد الاحتيالي، البريد العشوائي والهجمات المستهدفة، وتهديدات الأجهزة المحمولة (Samour & Al-Khazali, 2022).

وفي هذا الجانب، ذكرت دراسة هارونا ومودوبي Haruna and Modupe (2022) أن سوق رأس المال والبنوك شهد العديد من اعتداءات طالت الرؤساء التنفيذيين في مجال صيد الحيتان التي يُنظر إليها على أنها تهدد الأمن السيبراني لهذه الصناعة وتأثرت شركات الخدمات المالية بالحوادث التي تركز على الأمن السيبراني أكثر بكثير من المنظمات في القطاعات الأخرى. وذكر Calzolari (2021) أن 33% من الهجمات الكبيرة تستهدف قطاع الخدمات المالية.

5.1.2 تهديدات الأمن السيبراني (Cybersecurity Threats):

تشمل التهديدات السيبرانية مجموعة متنوعة من الأخطار والتحديات التي تستهدف أنظمة المعلومات والشبكات الإلكترونية في قطاع البنوك، وهناك العديد من التهديدات والهجمات السيبرانية المعاصرة والمتطورة التي قد تتجاوز الأمن والخصوصية بسهولة منها:

1. الاختراق الإلكتروني(Cyber Penetration) : حيث يقوم المهاجمون بالتسلل إلى أنظمة البنوك والحصول على المعلومات الحساسة مثل بيانات العملاء والحسابات المصرفية وبيانات أخرى قد تضر بالبنك والعملاء (Dongol & Chatterjee, 2019).
2. البرمجيات الضارة (Malware): تشمل الفيروسات وبرامج التجسس وبرامج الفدية، التي تسبب أضراراً جسيمة لأنظمة البنوك، وتعرض البيانات الحساسة للخطر (البابلي، 2020). وتشمل هذه البرمجيات الآتي:

- الفيروسات (Viruses): برامج تقوم بتكاثر نسخ من نفسها وتنتشر بين الأجهزة، وتستهدف تلف البيانات أو إعاقة عمل الجهاز (Laib, 2021).
- برامج التجسس (Spyware): برامج تقوم بسرقة المعلومات والبيانات الشخصية من الأجهزة المصابة، وترسلها إلى المهاجم (Kaspersky, 2021).
- برامج الفدية (Ransomware): برامج تقوم بتشفير الملفات على الجهاز وتطلب فدية من المستخدم لفك التشفير (Mishra, Alzoubi, Gill, & Anwar, 2022).
- برامج التصيد (Phishing programs): برامج تحاول اختراق أنظمة الحماية والاستيلاء على معلومات تسجيل الدخول وكلمات المرور الخاصة بالمستخدم لغرض استخدامها (Junaido & Mua'zu, 2015).
- برامج حصان طروادة (Trojan horse programs): برامج تدعي أنها برامج آمنة ومفيدة، لكنها في الحقيقة تحتوي على برامج ضارة مخفية تلحق الضرر بملفات وبرامج المستخدم (Manisha , Jadhav, & Nalawade, 2016).
- البرمجيات الخبيثة (Malware programs): تقوم بإلحاق الضرر بالأجهزة أو البيانات، مثل تعطيل النظام أو تدمير الملفات (Kaspersky, 2021).

3. برامج التجسس الإعلاني (Ad-spay ware): تعرض إعلانات وتجمع معلومات عن تصفح المستخدم لتوجيه إعلانات مستهدفة. (RSBP for Central Asia, 2020).
4. هجمات رفض الخدمة (Denial-of-service attacks): تهدف إلى تعطيل خدمات البنوك عن طريق زيادة حجم حركة المرور على الشبكات والخوادم، مما يؤدي إلى انهيار الأنظمة وتعطيل الخدمات المصرفية (Dhatchina & Dhatchina, 2020).

5. التصيد الإلكتروني (Phishing): حيث يتم استخدام رسائل البريد الإلكتروني المزيفة والروابط الخبيثة للتلاعب بالمستخدمين والحصول على معلومات شخصية ومصرفية حساسة يستغلها المهاجمون في عملياتهم(Manisha , Jadhav, & Nalawade, 2016).
6. سرقة الهوية (Identity Theft): يتم استخدام تقنيات الاحتيال الإلكتروني لسرقة معلومات الهوية الشخصية مثل الأسماء والعناوين وأرقام الضمان الاجتماعي والبطاقات الائتمانية.
7. التجسس الصناعي (Industrial Espionage): يتم استهداف البنوك للحصول على معلومات حول استراتيجيات الأعمال والابتكارات والبحوث السرية (Laib, 2021).
8. الهجمات الموجهة (Targeted attacks): تستهدف الأفراد أو المؤسسات في قطاع البنوك للحصول على معلومات أو تعطيل الأنظمة (Dhatchina & Dhatchina, 2020).
9. استغلال الثغرات البرمجية (Exploiting software vulnerabilities): يمكن للمهاجمين استغلال الثغرات البرمجية في أنظمة البنك للوصول غير المصرح به، سرقة البيانات، أو تعطيل العمليات، ويمكن أن تكون هذه الثغرات معروفة أو غير معروفة، ولذلك يجب على البنوك تحديث وتأمين أنظمتها بشكل دوري (Dongol & Chatterjee, 2019).
10. التهديدات الداخلية (Insider threats): لا يمكن تجاهل التهديدات الداخلية التي يمكن أن تنشأ من داخل البنوك أنفسها، ويمكن للموظفين أو الأشخاص الذين لديهم وصول معتمد إلى أنظمة البنك أن يتسببوا في إحداث أضرار بالأمان سواء عن طريق الخطأ أو بقصد، مما يؤدي إلى تسريب البيانات أو وقوع حوادث إلكترونية أخرى (Buchanan, 2014).
11. الهندسة الاجتماعية (Social Engineering): تعتمد على تلاعب المجرمين الإلكترونيين بالأفراد للكشف عن المعلومات الحساسة أو منحهم وصولًا غير مصرح به إلى

أنظمة البنوك، ويمكن أن يشمل ذلك انتحال هويات موظفي البنك أو العملاء واستدراكهم بوسائل مختلفة لتقديم المعلومات المطلوبة (Haruna, Aremu, & Modupe, 2022).

ولكي يتم التصدي لهذه التهديدات، يجب على البنوك تبني سياسات وإجراءات فعّالة لحماية أنظمتها ومعلومات عملائها من تلك الهجمات.

2.2 متطلبات الأمن السيبراني في البنوك (Cybersecurity Requirements in Banks):

تحتاج البنوك إلى الخدمات الرقمية لإدارة مشاريعها، وتستفيد من منصات خدمات رقمية تنافسية تقدم الخدمات بتكلفة منخفضة. وتتضمن هذه المنصات ثغرات أمنية غير معروفة للبائع، يحاول المهاجمون الاستفادة منها من خلال الوصول إلى أنظمة البنوك المحلية المتصلة بالمنصة. تؤدي هذه الهجمات إلى تعطيل الخدمات الرقمية وتعرقل عمل البنوك، وربما تؤدي في النهاية إلى عدم رغبة العملاء في التعامل مع تلك البنوك (Anand, Duley, & Gai, 2022) .

ولتجنب هذه المخاطر، يجب على البنوك توفير مجموعة من المتطلبات الخاصة بالأمن السيبراني، فيما يلي أهم المتطلبات الأمن السيبراني:

1.2.2 المتطلبات التنظيمية (Regulatory Requirements):

عرف الحداد (2022) المتطلبات التنظيمية بأنها "مجموعة من الوسائل، والسياسات والإجراءات الأمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات مثالية وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات للمستخدمين" (ص.9). كما عرفها عبد السلام (2022) بأنها: "مجموعة من القواعد والتوجيهات التي يجب على المؤسسات والشركات الالتزام بها وتنفيذها وفقًا للقوانين واللوائح المعمول بها في القطاع المالي، وتهدف هذه

المتطلبات إلى ضمان الامتثال للقوانين والحفاظ على الأمن والحماية للعملاء والمؤسسات المالية نفسها"(ص165). وتشمل المتطلبات التنظيمية ما يلي:

1.1.2.2 التشريعات واللوائح السيبرانية: يُعد القطاع المالي من أهم القطاعات في الاقتصاد العالمي، ولهذا السبب فإن توفير الأمن السيبراني في هذا القطاع يأتي على رأس أولويات الشركات المالية، ويجب على هذه الشركات الامتثال للتشريعات واللوائح السيبرانية المحلية والعالمية لضمان الحماية الكافية لبيانات العملاء وسلامة الأنظمة المالية (de Azambuja, et al., 2023). ويأتي في مقدمة التشريعات قانون Gramm–Leach–Bliley (GLBA) ، وتوجيهات مجلس فحص المؤسسات المالية الفيدرالية(FFIEC) .

ولتحقيق الامتثال لهذه القوانين والمبادئ التوجيهية، يجب على الشركات المالية تقييم المخاطر السيبرانية بانتظام وتحليل تأثيرها المحتمل (Shejin & Sudheer, 2023) . كما يجب أن تستخدم هذه التقييمات لتحديد نقاط الضعف لديها واتخاذ التدابير اللازمة للتخفيف من المخاطر. يشمل ذلك تطبيق استراتيجيات أمنية متقدمة بما فيها إدارة الهوية ومراقبة الأمان وإدارة التهديدات. (Shejin & Sudheer, 2023). والقيام بتدريب موظفيها حول التهديدات السيبرانية وكيفية التصدي لها، بما في ذلك هجمات التصيد الاحتيالي وأمان كلمة المرور. والتشجيع على الإبلاغ عن أي نشاط مشبوه، ويجب أن تكون الدورات التدريبية والتحديثات المنتظمة جزءًا من استراتيجية التثقيف. (Mungo, 2023)

كما أن الإبلاغ الفوري عن خروقات البيانات أمر مهم للغاية، ويسهم في إبلاغ العملاء والسلطات التنظيمية بأي مخاطر محتملة، ويتيح لهم اتخاذ الإجراءات الضرورية لحماية أنفسهم (Kale, et al., 2023)، ويعد التطبيق الصارم لسياسات وإجراءات أمنية فاعلة أمرًا بالغ الأهمية

لطبيعة عمل تلك الشركات، ويجب أن تتضمن هذه السياسات إدارة الوصول والتشفير وحماية الشبكة (Kitsios, Chatzidimitriou, & Kamariotou, 2023). ويمكن لهذه الإجراءات التقليل من مخاطر الوصول غير المصرح به وخروقات البيانات.

2.1.2.2 إجراء تقييم للمخاطر السيبرانية: تقييمات المخاطر السيبرانية تُعد جزءًا أساسيًا وحيويًا من استراتيجية الأمن السيبراني في قطاع الخدمات المالية (Atnafie, Anteneh, Yimenu, & Kifle, 2021). وتؤدي هذه التقييمات دورًا كبيرًا في تحديد نقاط الضعف المحتملة والتهديدات وتقييم تأثيرها المحتمل في المؤسسة، مما يمكن الشركات المالية من وضع استراتيجيات أمنية فعالة لمواجهة التهديدات السيبرانية المحتملة والتصدي لها بكفاءة (Gavėnaitė-Sirvydienė & Miečinskienė, 2023).

للقيام بعملية التقييم، فإنه يتوجب في البداية تحديد الأصول الحيوية داخل المؤسسة التي تتطلب حماية خاصة، وتشمل هذه الأصول بيانات العملاء وأنظمة المعاملات المالية ومعلومات الموظفين والبيانات الحساسة الأخرى (Logan & Clarkson, 2020) ، ثم القيام بتحديد التهديدات المحتملة التي يمكن أن تستغل نقاط الضعف في أنظمة المؤسسة وبنيتها التحتية، مثل: محاولات القرصنة وهجمات البرامج الضارة والتصيد الاحتيالي والتهديدات الداخلية والانتهاكات المادية (Tekleselase, 2019).

يأتي بعد ذلك عملية تقييم نقاط الضعف المحتملة داخل أنظمة المؤسسة وعملياتها وبنيتها التحتية التي يمكن أن تستغلها التهديدات السيبرانية كالبرامج القديمة وكلمات المرور الضعيفة ونقص التشفير وعدم كفاية ضوابط الوصول (Alawadhi & Awad, 2023)، يتضمن تقييم المخاطر الذي يتضمن تقدير تأثير كل تهديد ونقطة ضعف محددين على المنظمة. يجب تقييم

احتمالية حدوث هجوم والعواقب المحتملة في حال حدوث ذلك (Gurgun, Bayhan, Polat, & Turkoglu, 2018) مع تحديد أولويات المخاطر المحددة استنادًا إلى تأثيرها المحتمل واحتمالية حدوثها، وهذا يساعد في توجيه الموارد بشكل فعال لمعالجة المخاطر الأكثر خطورة أولاً (Gurgun, Bayhan, Polat, & Turkoglu, 2018).

على ضوء ما سبق، يتم تطوير استراتيجيات للتخفيف من المخاطر المحتملة، وتنفيذ الضوابط والتدابير اللازمة لمعالجة هذه المخاطر، بما فيها تطبيق جدران الحماية وأنظمة كشف التسلل وعناصر التحكم في الوصول والتشفير وتحديثات النظام المستمرة. علاوة على ذلك، يجب على الشركات مراقبة ومراجعة الضوابط المنفذة بشكل مستمر لضمان فعاليتها، وتقييم المخاطر وفقًا للتطورات الجديدة.

3.1.2.2 تطوير استراتيجية أمنية شاملة في القطاع المالي: يشتمل تطوير استراتيجية أمنية متكاملة في القطاع المالي على عناصر رئيسية تُعد أساسية لضمان الحماية الفعّالة، وهذه العناصر هي:

- **إدارة الهوية:** تتضمن ممارسات قوية لإدارة الهوية ومراجعة امتيازات الوصول وتحديث حسابات المستخدم بانتظام (Tolossa, 2023).
- **المراقبة الأمنية:** تشمل كشف التسلل ومنعه ومراقبة حركة مرور الشبكة (Mishra S. , 2023).
- **إدارة التهديدات:** يجب إجراء تقييمات منتظمة للتهديدات وتنفيذ الضوابط الأمنية المناسبة.
- **تدريب الموظفين وتوعيتهم:** يتعين تثقيف الموظفين حول التهديدات السيبرانية وتقنيات الهندسة الاجتماعية (Alawadhi & Awad, 2023).

- **الإبلاغ عن خرق البيانات:** من الضروري أن تلتزم الشركات المالية بإخطار الجهات التنظيمية عند وقوع خروقات البيانات في الإطار الزمني المنصوص عليه قانونًا، وذلك للحفاظ على سلامة النظام المالي وحماية المستهلكين، وتساعد البلاغات الفورية في تقليل تأثير الخروقات وتحجيم الضرر (Choi, Kim, & Na, 2023); (Strahilevitz & Liu, 2022).
- **السياسات والإجراءات الأمنية:** تحتاج الشركات المالية إلى تنفيذ سياسات وإجراءات أمنية متقدمة لحماية بيانات العملاء والشبكات من التهديدات السيبرانية، ويشمل ذلك استخدام تقنيات مثل التشفير وأنظمة الكشف عن الاختراقات، والتدريب المستمر للموظفين على أفضل الممارسات الأمنية (Tuteja & Shanker, 2022) ; (Silvers, 2007).
- **أمن الطرف الثالث:** يُعد تقييم مقدمي الخدمات الخارجيين والتأكد من استيفائهم للمعايير الأمنية من الخطوات المهمة للحد من المخاطر المصاحبة لخرق البيانات وغيرها من الحوادث الأمنية. وتتضمن هذه العملية إجراء تقييمات شاملة، التحقق من الامتثال لمعايير الصناعة، وتطوير خطط استجابة للتعامل مع الخروقات الأمنية (Silvers, 2007).
- **التدريب للموظفين في مجال الأمن السيبراني:** يجب أن يغطي التدريب مجالات الأمن السيبراني مثل هجمات التصيد الاحتيالي والبرامج الضارة والهندسة الاجتماعية وأمان كلمة المرور، وتدريبهم عن كيفية التعرف على الأنشطة المشبوهة والإبلاغ عنها. إضافة لذلك، تعزيز ثقافة الأمن السيبراني داخل المنظمة من خلال تزويد الموظفين بانتظام بالسياسات والإجراءات الأمنية، وتشجيع مشاركتهم النشطة في الحفاظ على بيئة آمنة، وفهم العواقب المحتملة لأفعالهم وتزويدهم بشكل منتظم بمعلومات متعلقة بأحدث تهديدات الأمن السيبراني والاتجاهات من خلال النشرات الإخبارية وقنوات الاتصال الداخلية وورش العمل وغيرها.

4.1.2.2 إدارة التكوين لأمن المعلومات: تشكل إدارة التكوين الأمن عنصرا محوريا لأمن المعلومات في القطاع المالي. تتضمن هذه العملية إنشاء وصيانة مستمرة لتكوينات الأمان للأنظمة والشبكات والأجهزة في المؤسسات المالية. يواجه القطاع تحديات أمنية كبيرة، نظرًا للبيانات الحساسة التي يتعامل معها. (Inayat, Zia, Mahmood, Berghout, & Benbouzid, 2022) لذا، يجب إنشاء ممارسات قوية لإدارة التكوين للتخفيف من المخاطر وحماية المؤسسات من التهديدات السيبرانية (Nowikowska, 2021).

وتشمل العناصر الرئيسية لإدارة التكوين الأمن التالي (Lankton, Price, & Karim, 2021): التوحيد القياسي لإنشاء معايير وتكوينات الأمان الموحدة؛ تحديث الأنظمة والأجهزة بانتظام؛ تنفيذ ضوابط الوصول الصارمة؛ إدارة التغيير وتوثيق التعديلات؛ إدارة الثغرات الأمنية ومعالجتها؛ المراقبة والتسجيل للكشف عن التغييرات غير المصرح بها؛ وتوعية الموظفين بسياسات الأمان من خلال برامج التدريب.

5.1.2.2 الامتثال لمعايير السلامة الصناعية: يمكن للشركات المالية تحقيق الامتثال لمعايير السلامة الصناعية من خلال التالي:

- تطبيق معايير ISO 27001: حتى تتمكن للشركات المالية من تقييم مخاطرها الأمنية وتحديد الضوابط اللازمة لحماية معلوماتها الحساسة (Paganini, et al., 2023) .
- مراجعة وتحديث سياساتها وإجراءاتها الأمنية بانتظام وتحديثها وفقًا لأحدث التهديدات والتحديات الأمنية (Sell & Dupuis, 2023) وكذلك إجراء عمليات التدقيق الدورية لتقييم فعالية الضوابط الأمنية المتبعة وتحديد أي ثغرات أمنية ومعالجتها بشكل فعال (Leonard & Eugenia, 2020).

- توفير التدريب المستمر للموظفين حول ممارسات الأمان والتحديثات الأمنية الجديدة والتهديدات المحتملة (Paganini, et al., 2023).
- تطوير خطط استجابة للحوادث للتعامل مع الخروقات الأمنية والاستجابة بشكل فعال للحد من التأثيرات السلبية، والإبلاغ عن الخروقات الأمنية إلى السلطات التنظيمية المعنية والنسيق بانتظام مع مقدمي الخدمات الثالثين بشأن المواضيع الأمنية (Santos, Galang, & Amon, 2023).

6.1.2.2 تقديم التقارير إلى السلطات التنظيمية:

يتعين على الشركات الإبلاغ عن أي انتهاكات كبيرة للأمن إلى السلطات التنظيمية ذات الصلة، وهذا الإبلاغ يسمح للشركات باتخاذ الإجراءات المناسبة للتحقيق في الانتهاك وتقليل الضرر المحتمل وإمكانية منع الانتهاكات المستقبلية. وقد تقوم السلطات التنظيمية بتقديم التوجيه والدعم للشركة المتأثرة في التعامل مع الانتهاك وعواقبه. يمكن أن يؤدي عدم الإبلاغ عن الانتهاكات الكبيرة إلى عقوبات وعواقب قانونية على الشركة المالية (Davis, et al., 2023).

2.2.2 المتطلبات الفنية للأمن السيبراني (Technical Requirements for Cybersecurity):

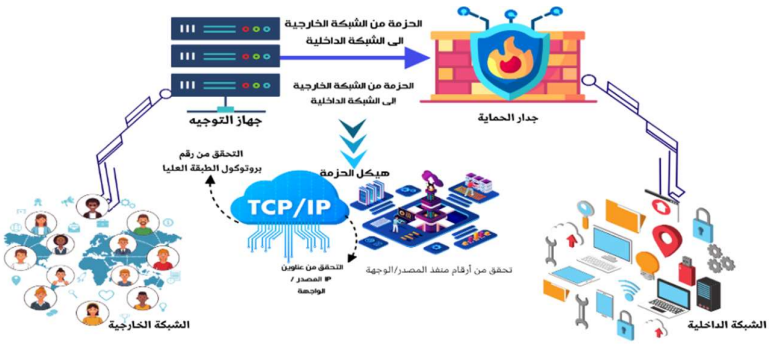
تتعلق المتطلبات الفنية للأمن السيبراني بالضمانات والتدابير الدقيقة التي يجب على المؤسسات استخدامها لحماية أنظمة الحاسوب والشبكات والبيانات الخاصة بها من الوصول غير المصرح به أو الاستخدام، أو الكشف، أو التعطيل، أو التعديل، أو التدمير. هذه المتطلبات ضرورية للحفاظ على سرية المعلومات وسلامتها وتوافرها ودرء التهديدات السيبرانية. تشمل المتطلبات الفنية الهامة للأمن السيبراني ما يلي:

1.2.2.2 جـــدران الحمايـــة (Firewalls): تمثـل جـدران الحمايـة أجهـزة أمـان الشـبكة التـي تشـرف علـى حركـة مـرور الشـبكة الـواردة والصـادرة وتـتحكم فيهـا، أي إنهـا تعمـل حـاجزاً بـين الشـبكات الداخليـة والخارجيـة، وتصـفية حركـة المـرور التـي يحتمـل أن تكـون ضـارة والـدفاع ضـد الوصـول غيـر المصـرح بـه (Ren, Ma, & Liu, 2023). فـي القطـاع المصـرفي، يـتم اسـتخدام عـدة أنـواع مـن جـدران الحمايـة بشـكل روتينـي لحمايـة البنيـة التحتيـة للشـبكة والبيانـات الحساسـة، وهنـاك عـدة أنـواع مـن جـدران الحمايـة التـي يمكن استخدامها في البيئات المالية:

1. **جدار الحماية على مستوى الشبكة (Network–Level Firewall):** يعمل على مستوى طبقات الشبكة السفلى، مثل طبقة الشبكة وطبقة النقل، ويتحكم في حركة البيانات بناءً على عناوين IP وأرقام المنافذ (Hedlund, 2013). ويوضح الشكل (1.2) جدار الحماية على الشبكة.

الشكل: 1.2

جدار الحماية على مستوى الشبكة

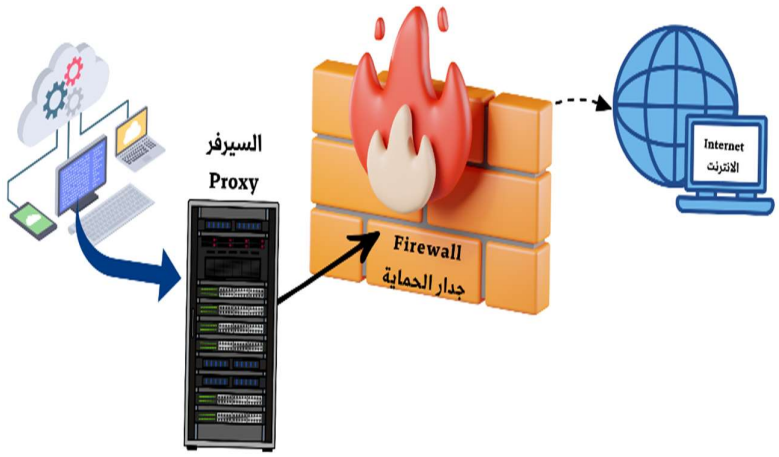


Source.Nest level firewall.From: What is a distributed firewall?.by B. Hedlund, 2013, July 9. https://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html/

2. جدار الحماية على مستوى التطبيق (Application-Level Firewall): يعمل على طبقة التطبيق ويمكنه فحص وتصفية البيانات الواردة والصادرة على مستوى التطبيقات، مثل HTTPو FTP (Liang & Kim, 2022). ويوضح الشكل (2.2) جدران الحماية على مستوى التطبيق.

الشكل: 2.2

جدار الحماية على مستوى التطبيق

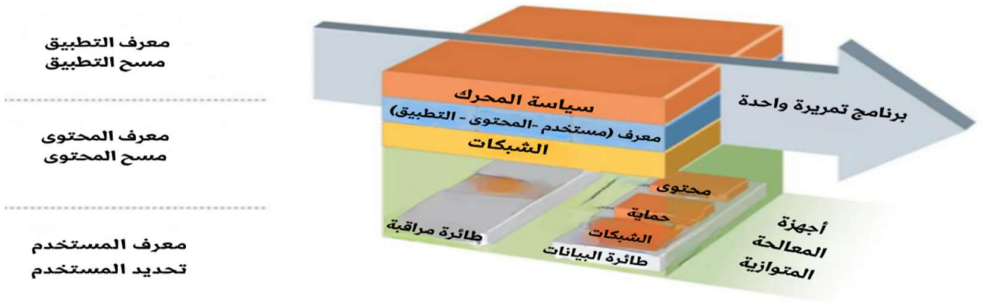


Source. App level firewall, from*:* Roll of Distributed Firewalls in Local Network for Data Security.by R. H. Rathod,2013.doi:ID: 39173224.

3. جدار الحماية المتقدم (Next-Generation Firewall - NGFW): يجمع بين خصائص جدار الحماية التقليدي والتحكم الإضافي في التطبيقات، بالإضافة إلى تقديم ميزات مثل التفتيش العميق للحزم (Deep Packet Inspection) والوقاية من الاختراق (Liang & Kim, 2022) (Intrusion Prevention Systems). ويوضح الشكل (3.2) جدار الحماية المتقدم.

الشكل: 3.2

جدار الحماية المتقدم

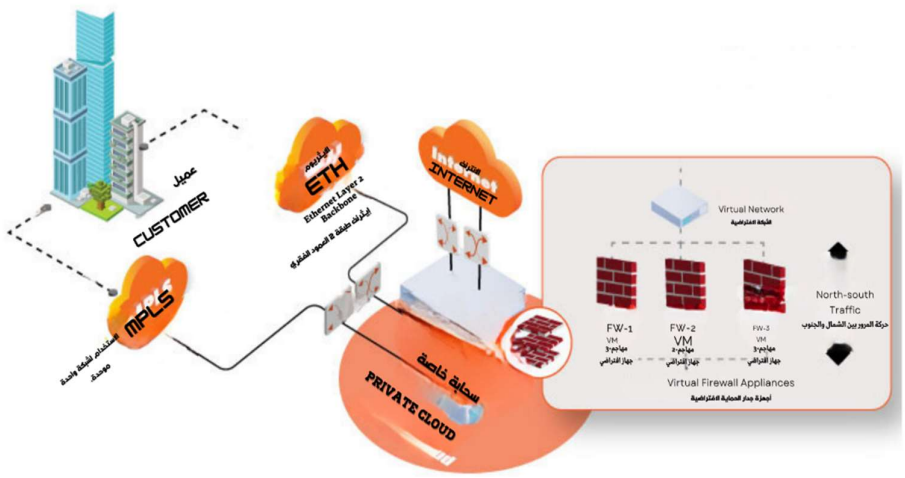


Source.Nest level firewall.From: What is a distributed firewall?.by B. Hedlund, 2013, July 9. https://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html/

4. جدار الحماية المستند إلى الحوسبة السحابية (Cloud–Based Firewall): يتم تنفيذه وإدارته في بيئة سحابية، ويوفر حماية مرنة وقابلة للتوسعة للشبكات المتصلة بالسحابة. (Singh & Govindarasu, 2020). يوضح الشكل رقم (4.2) جدار الحماية المستند إلى الحوسبة السحابية.

الشكل: 4.2

جدار الحماية المستند إلى الحوسبة السحابية

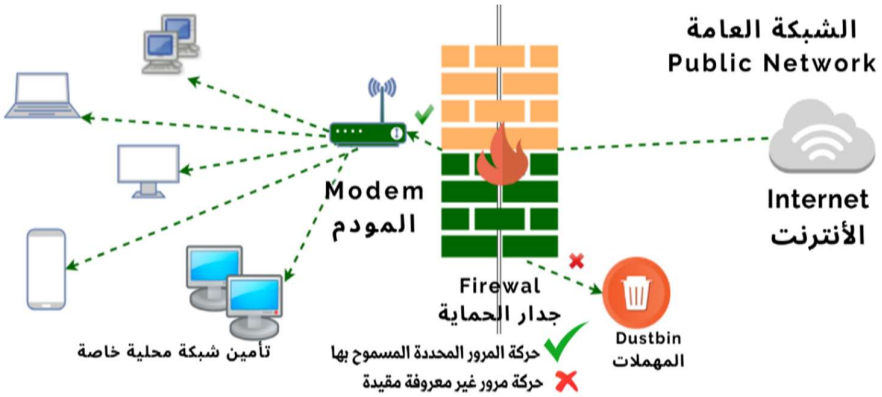


Source.Nest level firewall.From: What is a distributed firewall?.by B. Hedlund, 2013, July 9. https://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html/

5. جدار الحماية للشبكات الافتراضية الخاصة (VPN Firewall): يوفر حماية لشبكات VPN ويضمن أمان تبادل البيانات عبر شبكاتVPN (George & George, 2021). يوضح الشكل رقم (5.2) جدار الحماية للشبكات الافتراضية الخاصة.

الشكل: 5.2

جدار الحماية للشبكات الافتراضية الخاصة

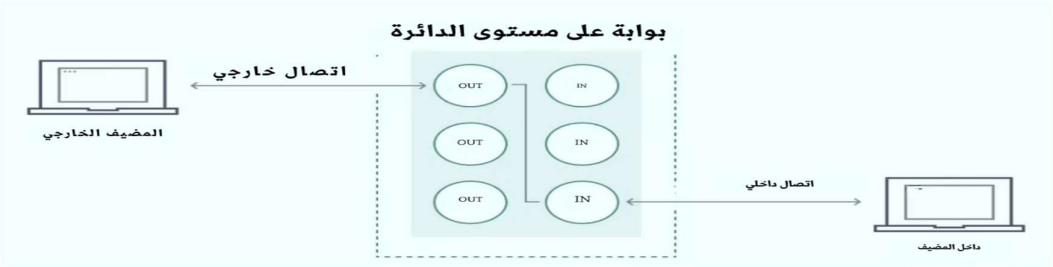


Source. Firewall for special virtual networks(p.35), From: A brief study on the evolution of next generation firewall and Web aplication firewall. By George, A., & George, A., 2021, https://doi.org/10.5281/zenodo.7027397

6. **جدار الحماية المدمج (Unified Threat Management – UTM):** يجمع بين وظائف جدار الحماية التقليدية ومجموعة من خدمات الأمان الأخرى مثل مكافحة الفيروسات، والتحكم في الوصول، والوقاية من الاختراق (Singh & Govindarasu, 2020). ويوضح الشكل رقم (6.2) جدار الحماية المدمج.

الشكل: 6.2

جدار الحماية المدمج



Source.Built-in firewall.From:What is a distributed firewall?.by B. Hedlund, 2013, July9. https://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html/

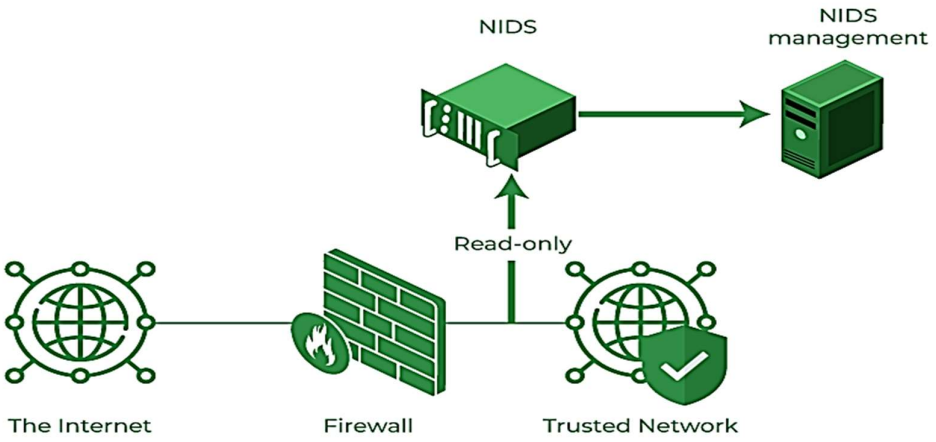
ويعتمد اختيار نوع جدار الحماية المناسب على متطلبات الأمان الخاصة بكل مؤسسة مالية، حجمها، وطبيعة البيانات التي تتعامل معها. مع الأخذ بعين الاعتبار مستويات الأداء المطلوبة والقدرة على التكامل مع الأنظمة الأمنية الأخرى في المؤسسة.

2.2.2.2 أنظمة كشف التسلل والوقاية منه (IDPS): هناك العديد من الأنظمة التي تؤدي أدوار مختلفة في مجال مكافحة وكشف التسلل منها:

- **نظام كشف التسلل القائم على الشبكة (NIDS):** يراقب حركة مرور الشبكة ويحللها لتحديد الأنشطة الضارة (Taherdoost, 2022)، الشكل رقم (7.2) يوضح نظام كشف التسلل القائم على الشبكة.

الشكل: 7.2

نظام كشف التسلل القائم على الشبكة (NIDS)

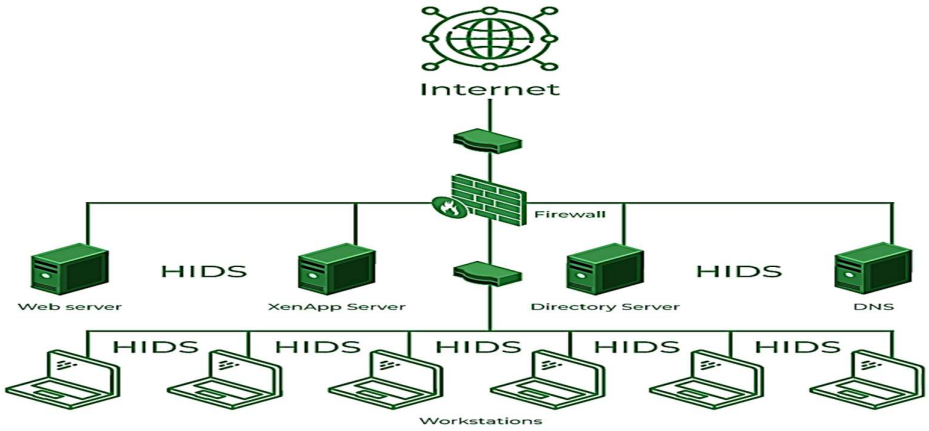


Source.NIDS, From:Understanding cybersecurity frameworks and information security standards:A review and comprehensive. by Taherdoost H., 2022 https://doi.org/10.3390/electronics11142181

- **نظـام كشـف التسـلل القـائم علـى المضـيف (HIDS):** يراقـب أجهـزة الحاسـوب والخـوادم داخـل الشـبكة لتحديـد التهديـدات (Chen & Chou, 2014). الشـكل رقـم (8.2) يوضح نظام كشف التسلل القائم على المضيف.

الشكل: 8.2

نظام كشف التسلل القائم على المضيف

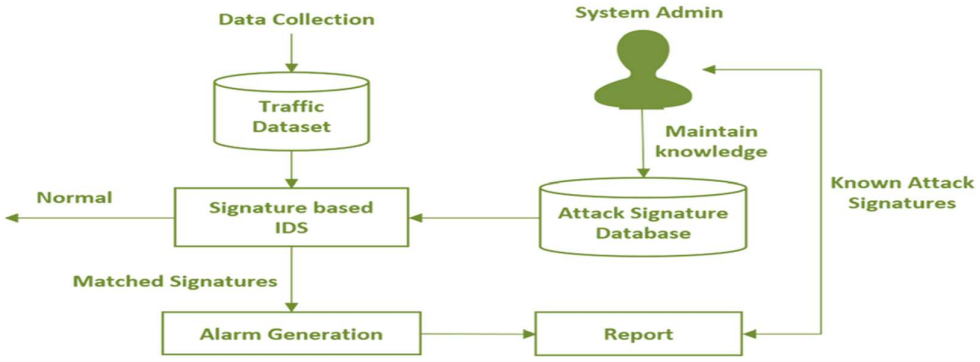


Source. ID-Based Certificateless Electronic Cash on Smart Card. From: Protection against Identity Theft and Financial Card Fraud. By Chen, Y., & Chou, J., 2014.

- **نظـام كشـف التسـلل القـائم علـى التوقيـع:** يسـتخدم قاعـدة بيانـات لتحديـد التهديـدات المعروفة (Kafi & Akter, 2023) كما في الشكل (9.2).

الشكل: 9.2

نظام كشف التسلل القائم على التوقيع

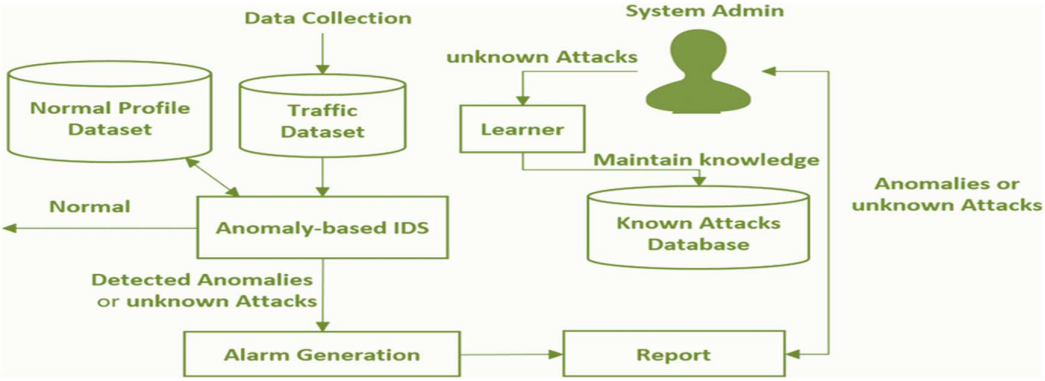


Source. A hybrid machine learning model for intrusion detection in VANET, by Bangui, Hind & Ge, Mouzhi & Unnova, Barbora., 2022. Doi. 10.1007/s00607-021-01001-0

- **نظـام كشـف التسـلل القـائم علـى الشـذوذ:** يقـوم بتحليـل حركـة المـرور بحثـا عـن أي انحرافـات عـن السـلوك الطبيعـي يوضـح الشـكل رقـم (10.2) نظـام كشـف التسـلل القائم على الشذوذ.

الشكل: 10.2

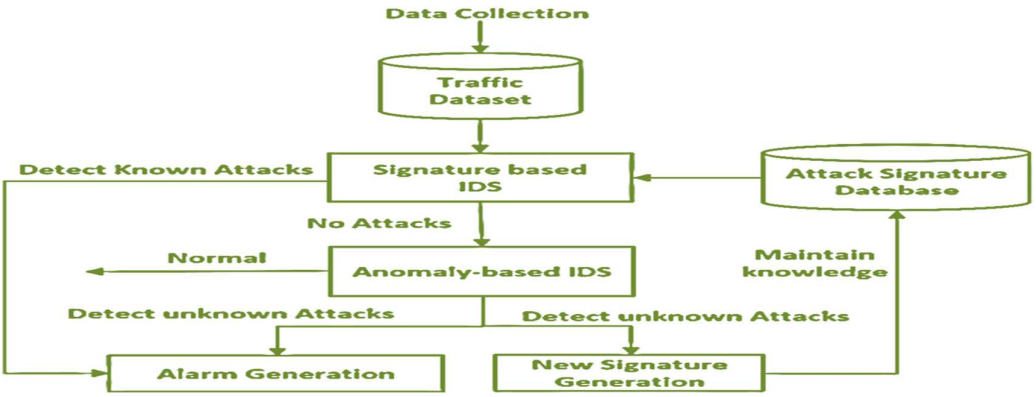
نظام كشف التسلل القائم على الشذوذ



Source. A hybrid machine learning model for intrusion detection in VANET, by Bangui, Hind & Ge, Mouzhi & Unnova, Barbora., 2022. Doi. 10.1007/s00607-021-01001-0

نظـام كشـف التسـلل الهجـين: يجمـع بـين منهجيـات الكشـف القائمـة علـى التوقيـع والقائمـة علـى الشـذوذ (Dodge, Fisk, Burruss, Moule, & Jaynes, 2023) . وهـذه الأنظمـة تسـاعد فـي اكتشـاف ومنـع التهديـدات السـيبرانية فـي المؤسسـات المصـرفية، الشكل رقم (11.2) يوضح نظام كشف التسلل الهجين.

الشكل: 11.2



Source. A hybrid machine learning model for intrusion detection in VANET, by Bangui, Hind & Ge, Mouzhi & Unnova, Barbora., 2022. Doi. 10.1007/s00607-021-.01001-0

3.2.2.2 التشـفير (Encryption): التشـفير هـو عمليـة تحويـل البيانـات إلـى تنسـيق غيـر قابـل للفهـم إلا بواسـطة مفتـاح فـك التشـفير (Li,2023). ويسـتخدم التشـفير لحمايـة البيانـات الحساسـة مـن الوصـول غيـر المصـرح بـه (طـارق، 2023) ، وتـتم عمليـة التشـفير عـن طريـق تحويـل الـنص العـادي إلـى نـص مشـفر باسـتخدام خوارزميـات معينـة. يمكـن فـك تشـفير الـنص المشـفر باسـتخدام مفتـاح سـري (Ikram&Madkour,2020). ويسـتخدم التشـفير فـي العديـد مـن المجـالات مثـل الخـدمات المصـرفية عبـر الأنترنـت والتجـارة الإلكترونيـة والرسـائل الأمنـة. بالإضـافة إلـى لـوائح حمايـة البيانـات مثـل GDPR و PCI DSS (Atnafie, Anteneh, Yimenu, & Kifle, 2021).

4.2.2.2 النسخ الاحتياطي المنتظم والتعافي من الكوارث للبنوك: يُعد النسخ الاحتياطي المنتظم والتعافي من الكوارث أمرًا حاسمًا في الأمن السيبراني للبنوك والمؤسسات المالية الأخرى. وتشمل النسخ الاحتياطية إنشاء نسخ من البيانات وتخزينها في مكان آمن لضمان استردادها في حالة فشل النظام أو التعرض لهجوم سيبراني (Mishra, Alzoubi, Gill, & Anwar, 2022). وتُحدّد خُطط التعافي من الكوارث الإجراءات التي يجب اتخاذها في حالة حدوث انقطاع كبير، بنافيها

أنظمة وبنية تحتية زائدة للحفاظ على استمرارية العمليات. يجب أيضًا تنفيذ تدريبات وبرامج توعية للموظفين لضمان التزامهم بالنسخ الاحتياطي وخطط التعافي لتقليل مخاطر فقدان البيانات وحماية المعلومات السرية للعملاء (Haruna, Aremu, & Modupe, 2022).

5.2.2.2 إدارة الحوادث الأمنية والأحداث (SIEM) للقطاع المالي: إدارة الحوادث والأحداث الأمنية (SIEM) تؤدي دورًا حاسمًا في القطاع المالي في تعزيز الأمن السيبراني. يتم تصميم أنظمة SIEM لجمع وفحص سجلات الأحداث الأمنية من مصادر متعددة داخل البنية التحتية لشبكة المؤسسة (Karakaya&Sevina,2022) وتشمل هذه المصادر جدران الحماية وأنظمة كشف التسلل والخوادم وقواعد البيانات وأجهزة الأمان الأخرى، والهدف الرئيسي لنظم SIEM هو توفير رؤية في الوقت الفعلي للأحداث الأمنية والتهديدات المحتملة والاستجابة الفورية لها.

وتوفر أنظمة SIEM ميزات عديدة مثل: جمع السجلات وربطها، واكتشاف التهديدات والاستجابة للحوادث، وتقارير الامتثال، وبالنسبة للقطاع المالي، يُعد SIEM أمرًا حيويًا لحماية البيانات المالية والاستجابة للتهديدات الإلكترونية (Silvers, 2007) . ومن المهم أن تكون أنظمة SIEM مكونة بشكل صحيح ومحدثة بانتظام ومتكاملة مع أدوات الأمان الأخرى (Hema, 2022) .

3.2.2 المتطلبات المادية للأمن السيبراني(Physical Requirements for Cybersecurity):

تشمل المتطلبات المادية للأمن السيبراني مزيجا من البنية التحتية والتدابير التشغيلية لحماية البيانات الحساسة. تم وضع هذه التدابير للحماية من التهديدات المادية مثل الوصول غير المصرح به أو السرقة أو التلف أو تدمير الأجهزة والبيانات وتتضمن هذه المتطلبات التالي:

1.3.2.2 عناصر التحكم في الوصول Access controls: تهدف عناصر التحكم في

الوصول إلى إدارة وتنظيم الوصول إلى المعلومات والموارد والبيانات داخل المنظمة (Dongol & Chatterjee, 2019) ، وتتضمن عناصر التحكم في الوصول المادية والمنطقية، والإدارية، والشبكية، والبيانات، وتهدف هذه العناصر إلى منع الوصول غير المصرح به وحماية البيانات الحساسة وتقليل مخاطر الاختراقات والتهديدات الداخلية، ومن المهم أن تقوم المؤسسات بمراجعة وتحديث هذه العناصر بانتظام لمواجهة التهديدات (Haruna, Aremu, & Modupe, 2022).

2.3.2.2 أمن مركز البيانات Data Center Security: تتضمن التدابير الأمنية

التقنية تنفيذ بروتوكولات الشبكة الأمنة مثل جدران الحماية وأنظمة كشف التسلل والتشفير لمنع الوصول غير المصرح به وحماية البيانات من الاختراق والبرامج الضارة، وبالإضافة إلى ذلك تتضمن التدابير الإدارية وضع السياسات والإجراءات التي تنظم الوصول إلى المركز وإدارة ومراقبة التدابير الأمنية كما يجب مراجعة هذه الإجراءات وتحديثها بانتظام لمواكبة التهديدات والتقنيات المتطورة والحفاظ على أمن المعلومات وثقة العملاء (Shejin & Sudheer, 2023).

3.3.2.2 إدارة الأصول المادية: إدارة الأصول المادية تؤدي دوراً مهماً في الأمن السيبراني للبنوك، حيث تتضمن تحديد جميع الأصول المادية وتتبعها وإدارتها داخل

البنيــة التحتيــة للبنــك، مثــل الخــوادم وأجهــزة التوجيــه ومحــولات البيانــات ومحطــات العمــل والأجهزة المحمولة وغيرها (Tekleselase, 2019) .

ولتحقيق إدارة فعالة للأصول المادية، يجب على البنوك تنفيذ جرد دقيق للأصول وتتبع حركتها وتخلص من الأصول القديمة بطرق آمنة، كما يجب تنفيذ عناصر التحكم في الوصول لتقييد الوصول إلى المناطق الحساسة، وصيانة الأصول بشكل دوري، وإدارة دورة حياة الأصول بطريقة فاعلة، بالإضافة إلى دمج إدارة الأصول المادية مع تدابير الأمن السيبراني الأخرى، وتقليل مخاطر الوصول غير المصرح به (Ben Naseir, Dogan, & Apeh, 2020).

4.3.2.2 الضوابط البيئية Staff awareness and training: تُعد الضوابط البيئية مثل التحكم في درجة الحرارة والرطوبة في مركز البيانات أمرا حيويا للحفاظ على الأداء الأمثل لخوادم البنك والأجهزة الاخرى(Nykänen & Kärkkäinen, 2014) . حيث يؤدي ارتفاع درجة الحرارة ومستويات الرطوبة العالية إلى تعطل المعدات وفقدان البيانات. وتعد الضوابط البيئية جانبا حاسما من تدابير الأمن المادي (Snopkov, Nasser, & Nasser, 2020).

5.3.2.2 إدارة آمنة للأصول: إدارة الأصول تؤدي دورا حاسما في المشهد الأمني للبنوك، حيث تتضمن تحديد وتتبع وإدارة جميع الأصول المادية داخل بنية البنك، بما في ذلك الخوادم والموجهات والمفاتيح ومحطات العمل والأجهزة المحمولة والأجهزة الأخرى التي تخزن أو تعالج البيانات الحساسة (البابلي، 2020).

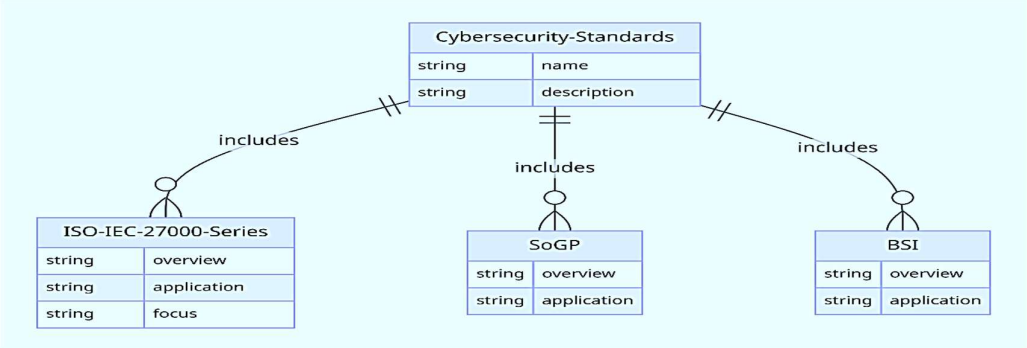
لضمان إدارة فعالة للأصول، يجب على البنوك تنفيذ التدابير التالية: جرد الأصول، تتبع الأصول، والتخلص من الأصول، وضوابط الأمان المادية، وصيانة الأصول، وإدارة دورة حياة الأصول (Jenifa & Ambika, 2020).

4.2.2 الأطر والمعايير الدولية للأمن السيبراني(International Frameworks and Standards for Cybersecurity):

الأطر والمعايير الدولية للأمن السيبراني أمر بالغ الأهمية خاصة في القطاع المالي. تعمل هذه الأطر والمعايير الأمنية على حماية بيانات العملاء والمعلومات الحساسة والحد من التهديدات السيبرانية (Lankton, Price, & Karim, 2021). وتشمل 1-الأمن السيبراني للمستخدمين 2- والبنية التحتية للشبكة، 3- البرامج والأجهزة والعمليات 4- وسائط تخزين النظام. يوصي خبراء الأمن بتنفيذ هذه المعايير كجزء من أفضل الممارسات لحماية المؤسسات من تهديدات الأمن السيبراني (Bleier, Langer, Skopik, & Smith, 2013).

الشكل: 12.2

معايير الأمن السيبراني-معايير أمن المعلومات



***Source**. A hybrid machine learning model for intrusion detection in VANET, by Bangui, Hind & Ge, Mouzhi & Unnova, Barbora., 2022. Doi. 10.1007/s00607-021-01001*

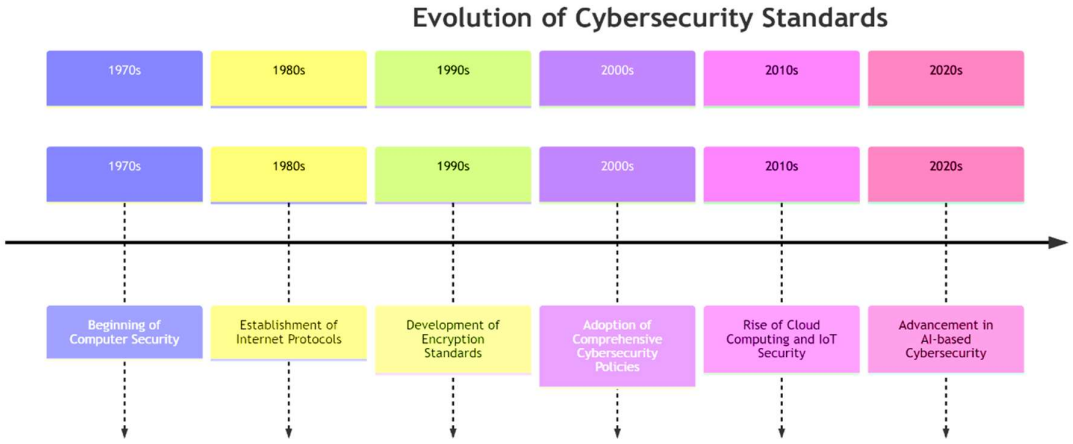
1.4.2.2 معايير الأمن السيبراني وأمن المعلومات:

يتم تطبيق معايير الأمن السيبراني الأكثر شيوعا، بما في ذلك سلسلة ISO 27000 وSoGP وBSI، لتقديم نظرة عامة وتسهيل عملية صنع القرار في الشركات المالية، وتشمل هذه المعايير الآتي:

1. **سلسلة ISO / IEC 27000**: تركز معايير ISO/IEC 27000 على أمن إدارة أنظمة المعلومات ويتم نشرها بواسطة ISO وIEC. يوفر ISO 27001 وصفًا مفصلًا للأساليب والممارسات لضمان تنفيذ فعال لأمن المعلومات(Disterer, 2013)، حيث تركز السلسلة على توفير تبادل آمن وموثوق للبيانات وقنوات الاتصال وتأكيد نهج المخاطر. ومع ذلك، لم يتم إثبات فعالية سلسلة ISO 27000 كإدارة كاملة لأنظمة المعلومات، ولذلك تستخدم في أنظمة أكبر. تشمل معايير الأمن السيبراني الأكثر شيوعًا سلسلة ISO 27000 و SoGP و BSIوتسهل عملية صنع القرار (Alexei, 2021)، الشكل (13.2) يوضح الجدول الزمني لتطور معايير الأمن السيبراني.

الشكل: 13.2

الجدول الزمني لتطور معايير الأمن السيبراني



Source. *Cloud Computing and Security (p.475), From Lecture Notes in Computer Science. By Long, Y., & Liu, Y., 2018. Springer.*

2. **سلسلة (ISO/IEC27000)**: تركز على إدارة أمن المعلومات وتنشرها منظمة ISO ولجنة IEC. تشمل السلسلة معايير مثل ISO/27001، التي توفر وصفًا مفصلاً للطرق والممارسات لضمان تنفيذ فعال لأمن المعلومات في المؤسسات، ويركز (ISO/IEC27001) على إدارة المخاطر، ومع ذلك لم يتم إثباتها كحل إداري شامل لأنظمة أمن المعلومات، غالبا يتم دمجها في أنظمة أكبر، وتشمل معايير الأمان السيبراني الأخرى SoGP وBSI (Kitsios, Chatzidimitriou, & Kamariotou, 2023).

3. **معيار (ISO/IEC27001)**: معيار معترف به دوليا لتنفيذ نظام إدارة أمن المعلومات (ISMS) في الشركات، ويتألف من سبعة عناصر رئيسية، بما في ذلك مواصفات التركيب والأداء والتشغيل والتحكم والمراقبة والمراجعة والصيانة وتحسين النظام (Ariza-López, et al., 2015). ويتضمن المعيار أيضا المتطلبات العامة لمعالجة وتقييم المخاطر في نظام معلومات المنظمة، بغض النظر عن حجمها أو طبيعتها، ويشيع استخدام (ISO/IEC27000) جنبا إلى جنب مع (ISO/IEC27001)، الذي يوفر أهدافا وتوصيات لضوابط الأمان، ويساعد استخدام (ISO/IEC27001) المؤسسات على إدارة وحماية المعلومات القيمة للموظفين والعملاء، وإدارة مخاطر المعلومات، وحماية علاماتهم التجارية وتطويرها (Nykänen & Kärkkäinen, 2014).

4. **معيار (ISO/IEC27002)**: هي مدونة قواعد الممارسة لضوابط أمن المعلومات التي تسرد سلسلة منظمة من ضوابط أمن المعلومات للامتثال (Taherdoost, 2022)، ويتم توفير توصيات أفضل الممارسات لاستخدامها من قبل الأفراد المسؤولين عند محاولتهم تنفيذ إدارة

أمن المعلومات في هذا المعيار، ويشمل ذلك إدارة الأصول في المؤسسة، وتأمين الموارد البشرية، وإدارة العمليات والاتصالات، وتأمين الجوانب البيئية والمادية، وإدارة استمرارية الأعمال، وغيرها (Nykänen & Kärkkäinen, 2014).

5. **معيار (ISO/IEC27005)**: يدعم المفاهيم والمتطلبات المدرجة على وجه التحديد في معيار (ISO/IEC27001). ولتنفيذ نظام معلومات مرض قائم على المخاطر في المؤسسات من مختلف الأحجام والقطاعات (Putri & Hakim, 2021)، ويتم استخدام عملية إدارة مخاطر المعلومات التي تتكون من ستة عناصر رئيسية، بما في ذلك تثبيت السياق، وتقييم المخاطر، ومعالجة المخاطر، وقبول المخاطر، والإبلاغ عن المخاطر، واستشارة المخاطر (Semin, Grigoreva, & Ilyina, 2016).

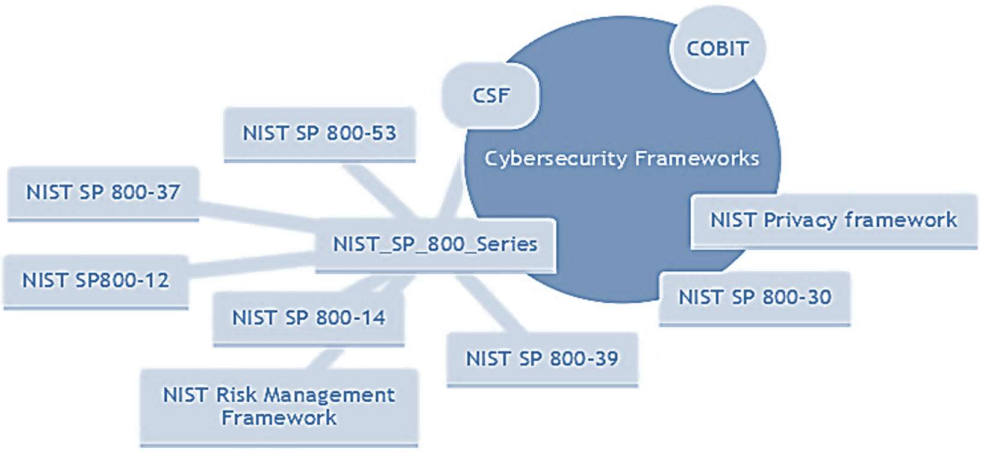
6. **معيار (ISO/IEC27006)**: الغرض من هذا المعيار هو تحديد العمليات والمتطلبات الرسمية التي يجب احترامها من قبل هيئات الطرف الثالث التي تقدم خدمات تدقيق أمن المعلومات، وإصدار الشهادات للمؤسسات الأخرى (García Araque, 2017) ، ويساعد استخدام هذا المعيار الهيئات على الاعتراف والثقة كجهات موثوقة ومنظمة لإدارة وتنفيذ عمليات شهادة نظام إدارة أمان المعلومات (ISMS) داخل المنظمات.

7. **إطار عمل NIST للأمن السيبراني (CSF)**: يقدم إطار الأمن السيبراني NIST (CSF) للمؤسسات الأدوات والهياكل اللازمة لتعزيز تدابير الأمن السيبراني الخاصة بها (Udroiu, Dumitrache, & Sandu, 2022). ويجمع هذا الإطار أفضل الممارسات والمعايير والتوصيات للأمن السيبراني، ويوفر هيكلاً تنظيميًا شاملاً للنهج المختلفة في هذا المجال. ومن ثم، يمكن استخدامه اساساً لتحسين برامج الأمان السيبراني الحالية في المؤسسات، والكشف عن الثغرات في ممارسات الأمن السيبراني وتحديد المتطلبات الفعالة للأمن السيبراني

(Abohatem, Al-Khulaidi, & Ba-Alwi, 2023). يوضح الشكل رقم (14.2) نموذج لأطر الأمن السيبراني.

الشكل: 14.2

أطر الأمن السيبراني – أطر أمن المعلومات



Source.NIDS, From:Understanding cybersecurity frameworks and information security standards:A review and comprehensive. by Taherdoost, H., 2022 .https://doi.org/10.3390/electronics11142181

- **إطار إدارة المخاطر NIST (RMF):** لإدارة مخاطر الخصوصية وأمن المعلومات، يجب على المؤسسة تنفيذ سلسلة من الخطوات وهي: (الإعداد، التصنيف، الاختيار، التنفيذ، التقييم التفويض، والمراقبة). ويتم تصميم هذه العملية لتكون عملية شاملة وقابلة للقياس والتكرار. ويمكن استخدامه في البيئات القائمة على إنترنت الأشياء لمواجهة تحديات الخصوصية والأمان' (Paoletti, Haut, Tao, Plaza, & Plaza, 2020).
- **إطار عمل خصوصية NIST** : يركز على معالجة مخاوف المؤسسات لاكتشاف التهديدات المتعلقة بالخصوصية والاستجابة لها، وإنشاء خدمات ومنتجات مبتكرة مع مراعاة الخصوصية

الفردية، ويستند هذا الإطار إلى خمس وظائف رئيسية تشمل: (تحديد الهوية، الحكم، التحكم، والتواصل، والحماية). يمكن أن يساعد هذا الإطار أيضا المديرين على معالجة التهديدات المتعلقة بمخاوف الخصوصية في البيئات القائمة على إنترنت الأشياء (Zhyvylo & Shevchenko, 2022). ويتضمن إطار عمل الخصوصية الآتي:

1. **NIST SP800-12:** يتم تغطية المبادئ الأساسية للأمن السيبراني بالتفصيل في SP800-12، حيث يغطي الدليل اعتبارات التكلفة، والمفاهيم المهمة، والعلاقة بين الضوابط الأمنية المختلفة، مما يوفر حلولا لضمان أمان الموارد(Johnson, 2005) .
2. **NIST ST800-53:** يركز هذا المعيار بشكل أساسي على الخصوصية والضوابط في أنظمة المعلومات والمؤسسات التي تهدف إلى تأمين الأصول والأفراد والعمليات في المؤسسات من التهديدات السيبرانية المختلفة، بما في ذلك الخطأ البشري والهجمات العدائية والفشل في الهيكل والكوارث الطبيعية ومخاطر الخصوصية والتهديدات من كيانات الاستخبارات الأجنبية (Force, 2020).
3. **NIST ST800-30:** يركز هذا المعيار بشكل أساسي على تقديم إرشادات لتطوير تقييم مخاطر نظم المعلومات، ويسهل هذا المعيار فهم المخاطر السيبرانية لصانعي القرار في المنظمة (Pambudi & Ramli, 2023).
4. **NIST ST800-37:** يركز هذا المعيار بشكل أساسي على توفير إرشادات لتطبيق إطار إدارة المخاطر في نظم المعلومات والمنظمات. ويقدم إرشادات للمؤسسات لتنفيذ وإدارة مخاطر الخصوصية والأمن فيما يتعلق بأفضل الممارسات في أنظمة المعلومات. وتكون الإدارة العليا مسؤولة عن إدارة الخصوصية والأمان (Putra & Soewito, 2023) .

5. **NIST SP 800-39**: يركز هذا المعيار بشكل أساسي على توجيه المنظمات لتطوير برنامج متكامل بهدف إدارة مخاطر أمن المعلومات فيما يتعلق بالمهمة التنظيمية والعمليات والسمعة والوظائف والأفراد والصورة والأصول التنظيمية (Initiative, 2021).
6. **NIST SP 800-14**: يزود المؤسسات بالمتطلبات التي يجب عليها اتباعها لتأمين موارد تكنولوجيا المعلومات، وضمان تقديم الحلول لأمن تكنولوجيا المعلومات في حالة التهديدات السيبرانية (Amiruddin, Afiansyah, & Nugroho, 2021).

3.2 نظم المعلومات في البنوك (Information Systems in Banks):

هناك العديد من النظم التي يستخدمها القطاع المصرفي، وتعمل على مساعدة ودعم المسؤولين وصناع القرار على اتخاذ القرارات الملائمة، وتتمثل هذه النظم بالآتي:

1.3.2 أمن المعلومات في البنوك(Information Security in Banks):

إن مفهوم أمن المعلومات هو مجموعة من الإجراءات والترتيبات الوقائية المستخدمة لحماية المعلومات ومنع المتسللين من الوصول إلى المعلومات الأساسية المهمة (Samour & Al-Khazali, 2022) ، وطبقا للمعيار الدولي ISO/IEC 27002، يقصد بأمن المعلومات بالحفاظ على سريتها وسلامتها وتوافرها (Culot, Nassimbeni, Podrecca, & Sartor, 2005).

بينما عرفه Rao (2023) بأنه "حماية المعلومات وعناصرها المهمة، بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها ونقلها"(p.48). من جانبه، أشار بورجيوس وآخرون Bourgeois, et al., (2019) لأمن المعلومات على أنه مجموعة من المكونات المترابطة التي تجمع المعلومات وتعالجها وتخزنها وتوزعها لدعم عملية صنع القرار والتحكم فيه. يهدف أمن

المعلومات إلى ضمان استمرارية الأعمال وتقليل الأضرار التجارية عن طريق الحد من تأثير الحوادث الأمنية.

2.3.2 أنواع نظم المعلومات في البنوك (Types of Information Systems in Banks):

هناك عدة أنواع من أنظمة المعلومات التي تستخدمها البنوك لإدارة عملياتها وتخزين واسترجاع المعلومات، منها:

1. ***نظام إدارة المعلومات البنكية (Banking Information System)***: يُعد النظام الأساسي لإدارة العمليات المصرفية كإدارة الحسابات والمعاملات والتحقق من الهوية والمراجعة الداخلية(Berdyugin & Revenkov, 2019; Berdyugin & Revenkov, 2019).
2. ***نظام إدارة علاقة العملاء (Customer Relationship Management System):*** يستخدم لتتبع وإدارة المعلومات المتعلقة بالعملاء، مثل تفاصيل الحسابات والمعاملات السابقة والتواصل مع العملاء (Talabi, Longe, Muhammad, & Olusanya, 2021).
3. ***نظام إدارة المخاطر (Risk Management System):*** يساعد هذا النظام في تحليل وتقييم المخاطر المالية والتأكد من الامتثال للقوانين واللوائح المالية. (Talabi, Longe, Muhammad, & Olusanya, 2021).
4. ***نظام إدارة المخزون (Inventory Management System):*** يستخدم لتتبع وإدارة الموارد المالية في البنوك، مثل النقد والأوراق المالية (Ecubay & Kilimvi, 2023).
5. ***نظام إدارة الشبكة الداخلية(Internal Network Management System):*** يساعد في إدارة الشبكة الداخلية وضمان أمان وسرية المعلومات (Ecubay & Kilimvi,).

2023) ويعد ضمان الأمن السيبراني لهذه الأنظمة أمر بالغ الأهمية لحماية البيانات الحساسة، والحفاظ على سلامة العمليات المصرفية، ومنع الخسائر المالية الناجمة عن الهجمات السيبرانية. لذا يجب على البنوك الاستثمار بشكل مستمر في التقنيات الأمنية المتقدمة واعتماد أفضل الممارسات لحماية أنظمة المعلومات الخاصة بها والتخفيف من المخاطر السيبرانية.

4.2 التكنولوجيا المالية (Financial Technology):

أدت التكنولوجيا دورا فعالاً ومتطوراً في المجال المالي والمصرفي، حيث ظهر مفهوم التكنولوجيا المالية، في السنوات الأخيرة، بوصفه مجالاً يهتم بالتعاملات المالية عن طريق تسخير منتجات التكنولوجيا كالتجارة الإلكترونية وشبكات الاتصالات والهواتف الذكية والعملات الرقمية بهدف تسهيل المعاملات المالية على نحو واسع وسهل الاستخدام.

1.4.2 تعريف التكنولوجيا المالية (Definition of Financial Technology):

تعرف الأدبيات السابقة التكنولوجيا المالية بأنها: "مجال يركز على بناء أنظمة تتيح نمذجة وتقييم ومعالجة المنتجات والأدوات المالية مثل الأسهم والسندات والأموال والعقود" (Friedman, 2006,65)، بينما عرفها سكوفيل Schoeffel (2016) على أنها: "صناعة مالية جديدة تعمل على تطبيق التكنولوجيا لتحسين الأنشطة المالية" وهذا التعريف جاء بعد تحليل أكثر من 200 دراسة علمية خلال الأربعين عاماً الأخير"(p.32)، ومن جهته عرف مجلس الاستقرار المالي التكنولوجيا المالية بأنها: "ابتكارات مالية باستخدام التكنولوجية الحديثة، إذ يمكنها من استحداث نماذج العمل والتطبيقات، وكذا العمليات والمنتجات، ولها أثر مادي ملموس على الأسواق

والمؤسسات المالية، عبر إضافاتها في الخدمات المالية" (بن ساسي، دحو& و إسحاق، 2023، ص 1002).

كما يمثل هذا القطاع نقطة التقاء بين المالية والتكنولوجيا، بما في ذلك الأنظمة المالية الجديدة والمتقدمة، والتي تتيح الفرص لتحسين الخدمات المالية وجعلها أكثر فعالية وشمولية، يستمد منها القطاع المالي قوته وتطوره.

2.4.2 أهمية التكنولوجيا المالية في البنوك(The Importance of Financial Technology in Banks):

تُعد التكنولوجيا المالية (Fintech) إحدى أبرز التطورات الرائدة في ميدان الخدمات المالية، حيث تشهد توسعاً متسارعاً بفضل التطورات المستمرة في مجال تقنية المعلومات، الاقتصاد التعاوني، والتشريعات الداعمة (Lee & Shin, 2018). وتعمل أنظمة (Fintech) على استحداث تقنيات متقدمة لابتكار نماذج أعمال جديدة ومبتكرة كالتمويل الجماعي، والتمويل الفردي المتبادل (P2P)، والتمويل بين الشركات (B2B). وينطوي هذا التوجه على تحديات جسيمة للنموذج التقليدي للمؤسسات المصرفية نظرًا للمزايا التي تقدمها (Fintech) فيما يخص انخفاض التكاليف، والارتقاء بالجودة، وتعزيز البيئة المالية لتصبح أكثر تنوعًا واستقرارًا، بما يبرر وصف الظاهرة بأنها ثورة التكنولوجيا المالية (Fintech).

3.4.2 مراحل تطور التكنولوجيا المالية في البنوك (Stages of Evolution of Financial Technology in Banks (Fintech):

التكنولوجيا المالية مجال يشهد تطورًا مستمرًا، وقد مرت بثلاث مراحل رئيسية منذ ظهورها في القرن التاسع عشر أدت إلى تبلور مفهوم الأمن السيبراني بوصفه محوراً رئيسياً في هذه الصناعة ، وهذه المراحل هي:

المرحلة الأولى تطبيق التكنولوجيا الرقمية في الخدمات المالية: تم استخدام الأنترنت والتكنولوجيا الرقمية لتسهيل العمليات المالية والمصرفية وتطوير خدمات مالية متعددة مثل: الخدمات المصرفية عبر الأنترنت، والدفع الإلكتروني والتحويلات المالية عبر الهاتف المحمول، والمحافظ الرقمية وغيرها، وقد أسهمت هذه التقنيات في تسهيل وتسريع العمليات المالية وتوفير الوقت والجهد للعملاء، ومع تزايد استخدام الهواتف الذكية والتطبيقات المصرفية المحمولة، أصبحت الخدمات المالية المبتكرة أكثر توافراً وملاءمة للعملاء في أي وقت ومن أي مكان (مؤمن، 2019).

المرحلة الثانية انتشار الخدمات المصرفية الرقمية: ظهور الخدمات المصرفية عبر الأنترنت وتطبيقات الهواتف الذكية، فقد شهدت انتشارا واسعا للاستخدامات التكنولوجية في القطاع المصرفي، حيث بات بإمكان العملاء إجراء المعاملات المصرفية وإدارة حساباتهم عبر الأنترنت دون الحاجة إلى زيارة الفروع البنكية (عطياني، الخرابشة، نور، و البستنجي، 2022). وقد أتاحت التكنولوجيا المالية هذه الفرصة للمستخدمين للوصول إلى الخدمات المصرفية بشكل أسرع وأكثر سهولة، وكذلك توفير العديد من الخدمات الجديدة مثل التحويلات الفورية والدفع الإلكتروني للفواتير (Olusolade, Fadare, & Mat Aji, 2020).

المرحلة الثالثة الابتكارات التكنولوجية المتقدمة: تركز على الابتكارات المتقدمة في تكنولوجيا المعلومات والاتصالات، مثل تقنيات الذكاء الاصطناعي والتعلم الآلي والبلوكتشين، وتتيح هذه التكنولوجيا الجديدة للبنوك والشركات المالية تقديم خدمات متقدمة ومبتكرة للعملاء، مثل التمويل التشاركي والتحويلات المالية عبر الحدود بشكل سريع وآمن. (الصويلح، 2023) وتتميز هذه المرحلة بظهور العملات المشفرة والخدمات المصرفية عبر الهاتف المحمول (Arner , Barberis , & Buckley , 2015) وقد أحدث التطور التكنولوجي تغييرات جذرية في قطاع الخدمات المالية والمصرفية، من حيث طرائق تقديم المنتجات والتفاعل مع العملاء (Hsu , 2021).

ومما سبق، تُعد التكنولوجيا المالية (Fintech) ثورة في قطاع الخدمات المالية والمصرفية، حيث تطورت عبر مراحل متعددة من تسهيل العمليات المالية باستخدام التكنولوجيا الرقمية إلى ابتكارات متقدمة مثل الذكاء الاصطناعي والبلوكتشين، مما أحدث تغييرات جذرية في طرق تقديم الخدمات والتفاعل مع العملاء.

5.2 العلاقة بين متطلبات الأمن السيبراني وحماية أنظمة المعلومات في القطاع المالي (*The Relationship Between Cybersecurity Requirements and the Protection of Information Systems in the Financial Sector*):

توجد علاقة وثيقة بين متطلبات الأمن السيبراني وحماية أنظمة المعلومات خصوصا في المؤسسات المالية، ويعد الأمن السيبراني من الموضوعات الضرورية للبنوك، حيث تحتوي على البيانات والمعلومات الحساسة للعملاء والشركات. وتعامل تلك البنوك مع الخدمات المصرفية الإلكترونية، يجعلها هدفًا للهجمات السيبرانية (Alamri, Crowley, & Richardson, 2022;Taherdoost, 2022) ويساعد تعزيز الأمن السيبراني في البنوك في حماية البيانات

الشخصية والمالية للعملاء، ويحمي البنية التحتية التكنولوجية للبنك من هجمات الاحتيال والتجسس والتعطيل.

وتشمل متطلبات الأمن السيبراني في البنوك الآتي (Chen & Chou, 2014):

1. *تأمين الشبكات والأنظمة*: يجب تطبيق تدابير أمنية قوية لحماية شبكات البنوك وأنظمتها من الاختراق والوصول غير المصرح به، ويتضمن ذلك 1- استخدام جدران الحماية النارية 2- أنظمة الكشف عن التسلل 3- تشفير البيانات.
2. *إدارة الهوية والوصول*: يجب تنفيذ سياسات صارمة لإدارة الهوية والوصول لضمان أن يتم منح الوصول إلى المعلومات الحساسة فقط للأشخاص المصرح لهم، ويشمل ذلك استخدام كلمات المرور القوية والمصادقة المتعددة العوامل.
3. *التحقق والرصد*: يجب تنفيذ أنظمة للتحقق والرصد المستمر للأنشطة غير المشروعة والتهديدات السيبرانية، ويساعد ذلك في اكتشاف الاختراقات المحتملة واتخاذ إجراءات فورية لمواجهتها(Asutosh , Kumar , Sattar , & Ranjan , 2023) .
4. *التدريب والتوعية*: يجب توفير التدريب والتوعية المستمرة للموظفين حول ممارسات الأمان السيبراني وكيفية التعامل مع التهديدات السيبرانية، ويساعد ذلك في خلق ثقافة أمنية داخل البنك وتعزيز التنبه للهجمات المحتملة (Kafi & Akter, 2023).

لذا، فإن تعزيز الأمن السيبراني في البنوك يساعد في حماية البيانات والمعلومات الحساسة والقيمة وضمان استمرارية خدمات المصرفية الإلكترونية بشكل آمن.

6.2 تجارب البنوك الدولية في تطبيق الأمن السيبراني(International Banking Experiences in Implementing Cybersecurity):

هناك العديد من الأمثلة الناجحة لتطبيق ممارسات الأمن السيبراني في البنوك الدولية منها:

1. **بنك جيه بي مورجان (الولايات المتحدة الأمريكية)** :يُعتبر هذا البنك الأمريكي من أكبر البنوك العالمية، وقد طور نظامًا شاملاً للأمن السيبراني يشمل تحليل الأمان، الكشف المبكر عن التهديدات، والتدقيق الأمني الدوري، بالإضافة إلى توفير تدريب مكثف لموظفيه حول مخاطر الأمان السيبراني (Herrera, Pereira, Volochen, & Zárate Moreno, 2023).
2. **بنك الرياض (المملكة العربية السعودية)** :يُعد بنك الرياض من البنوك الرائدة في السعودية، وقد اتخذ تدابير قوية لتعزيز الأمن السيبراني، متضمنًا تطبيق سياسات وإجراءات صارمة لحماية البيانات وتأمين الشبكة المصرفية، واعتماد تقنيات متقدمة للكشف المبكر عن التهديدات (Lewis, Connelly, Henkin, Leibovich, & Akavia, 2022).
3. **بنك HSBC المملكة المتحدة** :(يُعتبر بنكHSBC ، وهو بنك بريطاني، من أكبر البنوك العالمية، وقد أولى اهتمامًا كبيرًا للأمن السيبراني، معتمدًا على تكنولوجيا متقدمة لحماية البيانات وتأمين الشبكة، بما في ذلك استخدام الحواجز النارية ونظام الكشف عن التسلل (Nowikowska, 2021).
4. **بنك الإمارات دبي الوطني (الإمارات العربية المتحدة)** :يُعد هذا البنك الإماراتي من أكبر البنوك في الإمارات، ويضع الأمن السيبراني في صلب استراتيجيته، مستخدمًا نظامًا متكاملاً للحماية السيبرانية يشمل تقنيات التشفير والتحقق الثنائي (Nguyen, Koblandin, Suleymanova, & Volokh, 2021).

5. **بنك سيتي (الولايات المتحدة الأمريكية)** :يُعتبر بنك سيتي الأمريكي رائدًا في مجال الأمان السيبراني، حيث يستخدم تقنيات مثل الذكاء الاصطناعي وتحليل البيانات للكشف المبكر عن التهديدات والاحتيال السيبراني، وينفذ إجراءات صارمة لحماية بيانات العملاء (Adak, Pradhan, & Shukla, 2022).

6. **بنك هسبند (جنسية غير محددة)** :يُعتبر بنك هسبند من البنوك الدولية الرائدة في مجال الأمن السيبراني، ويستخدم تقنيات متطورة مثل الاعتماد على الهوية المتعددة وتشفير البيانات لحماية العمليات المصرفية الإلكترونية(Sawant, et al., 2023).

7. **بنك أوف أمريكا (الولايات المتحدة الأمريكية)** :يُعد هذا البنك الأمريكي من البنوك الكبرى في الولايات المتحدة، وقد طور برامج متخصصة للحماية من الهجمات السيبرانية، متضمنًا استخدام تقنيات التشفير المتقدمة وإجراءات صارمة للمصادقة والتحقق من الهوية (Efijemue, Ejimofor, & Owolabi, 2023) .

7.2 البنوك اليمنية ومدى تطبيقها للأمن السيبراني(Yemeni Banks and the Extent of Their Cybersecurity Implementation):

في ظل القرية الكونية الصغيرة التي صنعها التقدم التكنولوجي والتوجه العالمي الرامي إلى توحيد الجهود، وتوحيد السياسات والمعايير في السوق المالي، وجدت اليمن نفسها في إطار هذا التجمع العالمي الصغير، وأصبح من الضروري للبنوك مواكبة كل التطورات في مجال الأمن السيبراني تجنبا للوقوع في دائرة الاستهداف من قبل المهاجمين السيبرانيين.

بالرغم من وضع اليمن كإحدى الدول النامية، إلا أنها تسجل تقدمًا في مجال التكنولوجيا نتيجة لتطور تقنيات المعلومات والاتصالات وتوسع البنية التحتية الوطنية، لذا كان ظهور الأمن

السيبراني بوصفه تهديداً أمنياً جديداً في اليمن ناتج عن هذه التطورات وتعدد الاستخدام لهذه التكنولوجيا. وهناك العديد من الدراسات التي تناولت هذا الجانب، حيث ركزت دراسة حميد (Humied, 2023) على قضايا الأمن السيبراني في اليمن، وتناولت فكرة الأمن السيبراني ضمن إطار نظري للأمن من خلال تسليط الضوء على استهداف هاكرز صينيين للولايات المتحدة وما نجم عن ذلك من آثار هائلة. استنادًا إلى ذلك، تم تقييم بيئة الأمن السيبراني في اليمن، كما شملت الدراسة استطلاعات إحصائية أخرى تصنف البلد ضمن أصعب البلدان تأثرًا بالهجمات السيبرانية في العالم.

وقد أدت دراسة Humied إلى العمل على مسودة قانون الوقاية من الجرائم السيبرانية وجرائم تقنية المعلومات. كما تم إطلاق مناقشات حول استراتيجية الأمن السيبراني الوطنية في العام 2022م، ولكن حتى الآن لم يتم تشريع أية قوانين سيبرانية ملموسة. ذكرت الدراسة أن البلد يعاني من ضعف الأنترنت بسبب نقص المهارات والخبرة السيبرانية. وقدمت العديد من التوصيات حول كيفية تحسين استراتيجية الأمن السيبراني الشاملة في اليمن.

وفي دراسة أجراها (Al-Khulaidi, et al., 2022) كشف وجود مستويات متفاوتة من الالتزام بضوابط ومجالات ISRM بين الأنظمة المصرفية المختلفة، وبينت نقاط الضعف والثغرات في بعض البنوك اليمنية، لا سيما في مجالات مراجعة المخاطر والتعامل معها وتحديثها. ورجحت الدراسة أن سبب افتقارها لعمليات مراجعة منتظمة لخطط استمرارية الأعمال يعود لعدم استعدادها لحالات الكوارث والأزمات، مما قد يكون له آثار كبيرة في سيناريوهات العالم الحقيقي.

من جانب آخر، ذكرت الدراسة أنه على الرغم من وجود أمثله لبعض الأنظمة في القطاع المصرفي تطبق ممارسات إدارة الأمن المعلوماتي والمخاطر القوية، إلا أن التباين في جميع المجالات يشير

إلى الحاجة إلى نهج أكثر توحيدا وتنفيذ أفضل الممارسات في جميع الأنظمة المصرفية. وسد هذه الفجوة ضروريا للبنوك والنظام المالي بشكل أوسع (Al-Khulaidi, et al., 2022).

وفي السياق نفسه، كشفت دراسة أجراها الخليدي وآخرون(Al-Khulaidi, et al., (2022 تحديد نقاط القوة والضعف في ممارسات إدارة مخاطر الأمن السيبراني (ISRM) في القطاع المصرفي اليمني العديد من النتائج أهمها:

- أن أنظمة إدارة مخاطر الأمن السيبراني في القطاع المصرفي اليمني تلبي فقط متطلبات المستوى الرابع من نضج ممارسات إدارة مخاطر الأمن السيبراني ISRM بالنسبة لجميع مؤشرات إدارة مخاطر الأمن السيبراني وأبعاده، مع متوسطات تراوحت بين 3.58 و4.08 ومؤشر عام لا يتجاوز 3.84.
- أن إجراءات النسخ الاحتياطي لعمليات إدارة المخاطر هي أبرز نقطة قوة في أنظمة إدارة الأمن السيبراني، بينما كانت عمليات تقييم المخاطر والتعامل معها من أبرز نقاط الضعف.
- أن نظام إدارة مخاطر الأمن السيبراني في بنك TB هو الأكثر امتثالاً لمتطلبات إدارة المخاطر، تلته أنظمة البنوكRDB ، SB، QNB، NBY، SIB، YCB، IBY، وCAC، مع فجوة تطبيق تبلغ مستوى واحد، ومن ناحية أخرى، كان نظام إدارة مخاطر الأمن السيبراني في بنك YKBهو الأقل امتثالاً لمتطلبات إدارة المخاطر.

8.2 التدابير التي تطبقها البنوك اليمنية لمواجهة التهديدات السيبرانية (Measures Adopted by Yemeni Banks to Counter Cybersecurity Threats):

في الوقت الراهن، تواجه البنوك اليمنية تحديات كبيرة في مواجهة التهديدات السيبرانية، ونتيجة للظروف الصعبة التي تمر بها اليمن، يعد الأمن السيبراني للبنوك ضروريا لضمان استمرارية الخدمات المصرفية(Islam, Madavarapu, Sarker, & Rahman, 2022) .

وتعتمد البنوك اليمنية على تنفيذ بعض الإجراءات الأمنية الاحترازية للتصدي للتهديدات السيبرانية، وتتضمن هذه الإجراءات التالي:

- تطوير برامج تدريبية للموظفين والعاملين في البنوك لرفع مستوى الوعي الأمني وتعريفهم بالتهديدات السيبرانية وكيفية التصدي لها(Ansari, 2022) .
- استخدام أنظمة حماية أمنية متقدمة، مثل: جدران الحماية النارية وبرامج مكافحة الفيروسات والبرمجيات الخبيثة(Oprea, Li, Norris, & Bowers, 2018) .
- يتم وضع خطط وإجراءات استجابة للأزمات للتصدي للهجمات السيبرانية واحتمالية حدوث انقطاع في الخدمات المصرفية.
- تتعاون البنوك اليمنية مع الجهات الحكومية والمؤسسات الأمنية الأخرى لتبادل المعلومات والخبرات في مجال الأمن السيبراني والتصدي للتهديدات المشتركة(Górka, 2023) .

ومع ذلك. فإن بعض البنوك اليمنية قد اتخذت إجراءات لتعزيز أمنها السيبراني، على سبيل المثال، قامت بتطوير وتنفيذ سياسات وإجراءات أمنية قوية، مثل تحديث أنظمة الحماية وتكنولوجيا المعلومات وتكثيف التدريب والتوعية للموظفين بشأن التهديدات السيبرانية (Grasmick & Reichwald, 2015) .

ومما سبق تظل التهديدات السيبرانية تشكل تحديًا كبيرًا للبنوك اليمنية نظرًا للقيود الموجودة في البنية التحتية الرقمية والموارد المحدودة. ويتطلب تعزيز الأمن السيبراني في البنوك اليمنية استثمارات إضافية وتعاوناً مستمراً مع الجهات المعنية لتعزيز القدرة على التصدي للتهديدات المستمرة، وفي السياق نفسه تُعد تجارب البنوك اليمنية في مواجهة التهديدات السيبرانية تحديًا كبيرًا نظرًا للظروف الأمنية الصعبة التي تمر بها البلاد.

9.2 قانون الجرائم الإلكترونية وأمان المعلومات في اليمن(Cybercrime Legislation and Information Security in Yemen):

في عام 2020م، أصدرت الحكومة اليمنية مشروع قانون الجرائم الإلكترونية وأمان المعلومات، يوفر هذا المشروع أساسًا لضمان أن الحكومة تتعامل مع عناصر متنوعة تتعلق بأمان البلاد السيبراني، وينص ملخص المشروع الأولي على ما يلي: تنظيم الجرائم وفرض عقوبات تؤثر في الجريمة الإلكترونية، وتنظيم اختصاص المحاكم، وتنظيم صلاحيات التحقيق والدراسة والوصول أو الاستيلاء، وتنظيم جوانب التعاون الدولي في التحقيق في الجريمة الإلكترونية (Humied, 2023).

ورغم ذلك، لم يخل مشروع القانون من الانتقادات منذ إصداره، وقد تعرض لانتقادات حادة، حيث أعربت وسائل الإعلام والمواطنون لعدة أسباب رئيسية، وهي تتضمن الآتي: (Ismail, 2023)

1. **القيود على حرية التعبير** :تتضمن بعض قوانين الجرائم الإلكترونية بنودًا تحد من حرية التعبير على الإنترنت، حيث يمكن أن تُستخدم لمعاقبة الأفراد على التعبير عن آرائهم أو انتقاداتهم، خاصةً تلك التي توجه إلى الحكومات أو الأشخاص في مناصب السلطة.

2. **الغموض وعدم الوضوح** :قد تكون الصياغة في بعض بنود هذه القوانين غامضة أو غير واضحة، مما يجعل من الصعب على الأفراد تحديد ما يُعتبر سلوكًا مخالفًا. هذا الغموض يمكن أن يؤدي إلى سوء الاستخدام أو التطبيق التعسفي للقانون.

3. **انتهاك الخصوصية** :قد تمنح بعض قوانين الجرائم الإلكترونية السلطات الحكومية صلاحيات واسعة للمراقبة الاتصالات الرقمية وجمع البيانات الشخصية، مما يثير مخاوف بشأن انتهاك الخصوصية والرقابة على الإنترنت.

4. **تأثير على الحقوق الأساسية** :في بعض الحالات، يمكن أن تؤدي هذه القوانين إلى تقييد الحقوق الأساسية مثل حرية التجمع والرأي، خاصةً عند استخدامها لتجريم أنواع معينة من التعبير الرقمي أو النشاط الاجتماعي.

5. **استخدام كأداة للقمع السياسي** :في بعض الأنظمة، يتم استخدام قوانين الجرائم الإلكترونية كأداة للقمع السياسي، حيث تُستخدم لتكميم أفواه المعارضين السياسيين أو النشطاء.

6. **التأثير على حرية الصحافة** :قد تؤدي هذه القوانين أيضًا إلى تقييد حرية الصحافة، حيث يمكن استخدامها لمعاقبة الصحفيين على نشر معلومات تُعتبر حساسة أو ناقدة للحكومة.

7. **عدم التوافق مع المعايير الدولية:** في كثير من الحالات، تُعتبر هذه القوانين مخالفة للمعايير الدولية المتعلقة بحقوق الإنسان، بما في ذلك تلك المتعلقة بحرية التعبير والخصوصية.

8. **العقوبات القاسية** :غالبًا ما تتضمن قوانين الجرائم الإلكترونية عقوبات قاسية وغير متناسبة، بما في ذلك الغرامات الكبيرة والسجن لفترات طويلة، لأفعال قد تعتبر في سياقات أخرى مجرد مخالفات بسيطة.

9. **تقييد الابتكار والإبداع** :قد تؤدي هذه القوانين أيضًا إلى خلق بيئة تثبط الابتكار والإبداع في مجال التكنولوجيا والإعلام الرقمي، خاصةً عندما يخشى الأفراد من مخالفة القوانين بشكل غير مقصود.

هذه الأسباب تجعل قوانين الجرائم الإلكترونية موضوعًا مثيرًا للجدل ومحط انتقاد من قبل الجماعات الحقوقية، الإعلامية، والمواطنين على حد سواء

الفصل الثالث:

المنهجية والإجراءات المستخدمة بالدراسة

الفصل الثالث: المنهجية وإجراءات الدراسة

بعد التطرق لأهم المفاهيم النظرية المتعلقة بمتغيري الدراسة وعرض الدراسات السابقة في الموضوع، يتناول هذا الفصل محاولة الاطلاع على الواقع الحقيقي لتلك المفاهيم وذلك بإسقاط الجانب النظري على الجانب التطبيقي من خلال دراسة مدى تطبيق و أثر متطلبات الأمن السيبراني في حماية نظم المعلومات في البنوك اليمنية بحيث يتناول وصفاً للإجراءات التي اتبعت لغرض تحقيق أهداف الدراسة، من خلال وصف المنهج ، مصادر جمع البيانات والمعلومات، مجتمعها وعينتها، وأداة الدراسة وصدقها وثباتها بالاعتماد على الأساليب الاحصائية الملائمة من خلال برامج التحليل الاحصائي المستخدمة.

1.3 منهج الدراسة:

لتحقيق أهداف الدراسة تم الاعتماد على المنهج الوصفي بنوعيه المسحي والارتباطي، حيث تم استخدام المنهج الوصفي المسحي لتشخيص مدى توافر متطلبات الأمن السيبراني (التنظيمية، الفنية، الامتثال للأطر والمعايير الدولية، المادية)، وكذا مستوى حماية نظم المعلومات في البنوك اليمنية، بينما تم استخدام المنهج الوصفي الارتباطي للتعرف على أثر توافر متطلبات الأمن السيبراني على حماية نظم المعلومات في البنوك اليمنية.

2.3 مصادر جمع بيانات الدراسة:

اعتُمد في جمع البيانات على المصادر الأولية والثانوية على النحو الآتي:

المصادر الثانوية: اعتمد على مصادر البيانات الثانوية التي تتمثل في الكتب والأبحاث المنشورة والرسائل العلمية.

المصادر الأولية: وهي البيانات التي جمعت من أفراد العيِّنة من الموظفين في البنوك اليمنية بواسطة استمارة الاستبانة التي طُوِّرت لأغراض هذه الدراسة.

3.3 مجتمع الدراسة وعينتها:

مجتمع الدراسة يتكون من العاملين في فروع البنوك اليمنية (الحكومية، الإسلامية، والتجارية) في محافظتي عدن وتعز، بإجمالي يبلغ 15 بنكًا يمنيًا، وعدد الموظفين يقارب 356 موظفًا في مختلف المستويات الإدارية وفقًا لبيانات إدارات الموارد البشرية في هذه البنوك.

وباستخدام طريقة الحصر الشامل لاختيار المفردات، تمت دعوة جميع الـ 356 موظفًا للمشاركة في الدراسة، حيث تم توزيع رابط الاستبيان عبر مجموعات البنوك على موقع التواصل الاجتماعي (الواتساب)، وتم الحصول على استجابة من 250 موظفًا، ما يمثل معدل استجابة 70% من المجتمع الدراسي الكلي. يُظهر الجدول (3-1) حجم العينة المعتمد للتحليل، وتم إجراء اختبار KMO and Bartlett's Test لتحليل مدى كفاية حجم العينة المعتمدة وصلاحيتها لتنفيذ التحليل العاملي.

الجدول: 3-1

حجم عينة الدراسة المعتمدة في التحليل

عدد الاستبانات	التوزيع	العائد	المفقود	المستبعد	النهائي
المجموع	342	250	0	0	250
النسبة	96%	73%	0%	0%	73%
	KMO and Bartlett's Test				
	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.				0.969
	Bartlett's Test of Sphericity			Approx. Chi-Square	12560.316
				Df	1378
				Sig.	0.000

المصدر. إعداد الباحث استناد الى نتائج تحليل SPSS.

يتبين من الجدول (3-1) أن قيمة مؤشر KMO لدرجة التجانس لعينة الدراسة التي تشير إلى مدى كفاية حجمها وملائمتها لكل متغير من متغيرات الدراسة تساوي 97%، وهي أكبر من المدى المقبول للمؤشر الذي يجب ألا يقل عن 50%، كما تشير الدلالة الإحصائية لاختبار Bartlett's إلى معنوية النموذج العاملي عند مستوى دلالة (0.05). وقد توزعت مفردات العينة بحسب البنوك التي تنتمي إليها كما في الجدول (3-2) والشكل (1.3).

الجدول: 3-2

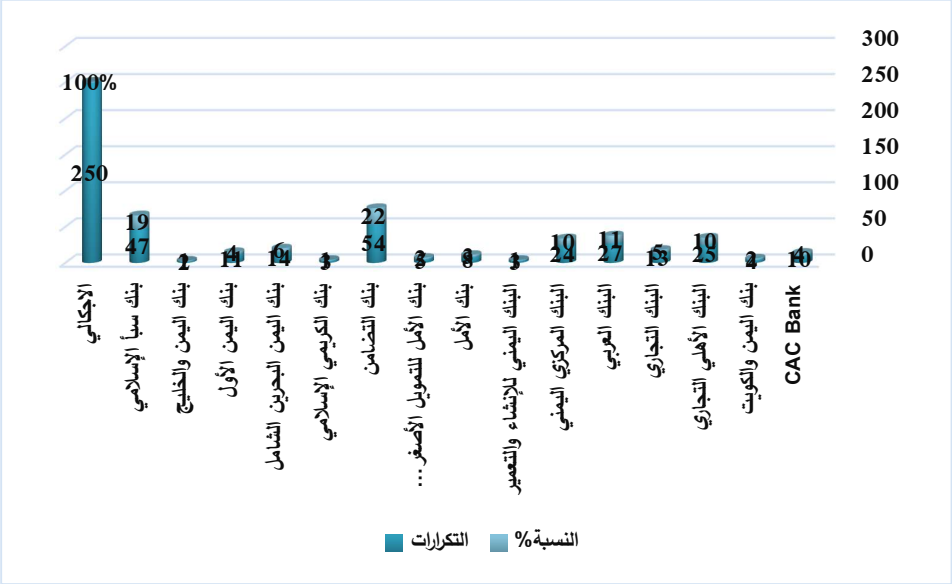
توزيع مفردات العينة حسب البنك

		التكرارات	النسبة%
1	CAC Bank	10	4
2	بنك اليمن والكويت	4	2
3	البنك الأهلي التجاري	25	10
4	البنك التجاري	13	5
5	البنك العربي	27	11
6	البنك المركزي اليمني	24	10
7	البنك اليمني للإنشاء والتعمير	3	1
8	بنك الأمل	8	3
9	بنك الأمل للتمويل الأصغر الإسلامي	5	2
10	بنك التضامن	54	22
11	بنك الكريمي الإسلامي	3	1
12	بنك اليمن البحرين الشامل	14	6
13	بنك اليمن الأول	11	4
14	بنك اليمن والخليج	2	1
15	بنك سبأ الإسلامي	47	19
	الإجمالـــي	250	%100

المصدر. إعداد الباحث استنادا الى بيانات إدارة الموارد البشرية للبنوك.

الشكل:(1.3)

التوزيع التكراري لمفردات عينة الدراسة بحسب اسم البنك



المصدر. إعداد الباحث استنادا إلى بيانات مفردات العينة.

4.3 أداة الدراسة:

تم اختيار الاستبانة أداة لجمع البيانات الأولية، التي صممت بقائمة استقصاء آراء مفردات عينة الدراسة حول فقرات محاور الدراسة وأبعادها لدراسة أثر مستوى توافر متطلبات الأمن السيبراني في تعزيز مستويات حماية سرية نظم المعلومات في البنوك اليمنية.

5.3 تصميم الاستبانة:

في محاولة لضمان الدقة والفاعلية، تم تحضير الاستبانة وفقًا لنموذج الأسئلة المغلقة، وهذا النموذج يتيح للمشاركين في الدراسة اختيار الردود المحددة على مجموعة متنوعة من العبارات، تم تصميمها لتغطية مختلف جوانب الدراسة. وحُدِّدت محاور الدراسة بعد عرضها على الدكتور المشرف على هذه الدراسة، ثم عرضها على (7) محكمين من الخبراء والأكاديميين ملحق رقم (1)، وبعد عمل التعديلات المطلوبة كانت الاستبانة في صورتها النهائية كما في الملحق رقم (3)، وتشمل مكوناتها محورين، بالإضافة إلى الخصائص الديموغرافية للمستجيبين، على النحو الآتي:

الجزء الأول: البيانات الشخصية: وهي المعلومات الأولية لأفراد عينة الدراسة وتشمل (المؤهل العلمي، التخصص، اسم البنك، نوع البنك، المسمى الوظيفي، سنوات الخبرة التخصص، عدد الدورات التدريبية التي حصلت عليها).

الجزء الثاني: البيانات المتعلقة بالدراسة ويتكون من محورين:

- **المحور الأول: متغيرات المستقل (متطلبات الأمن السيبراني)** يتضمن 37 فقرة، وقد تمثل في أربعة أبعاد فرعية وهي: المتطلبات التنظيمية ويحتوي على 10 فقرات من الاستبانة، المتطلبات الفنية تحتوي على 9 فقرات، الامتثال للأطر والمعايير الدولية تحتوي على 10 فقرات، تدابير الأمن المادي تحتوي على 8 فقرات. استنادا لدراسات سابقة منها: (السرحان، 2020) ، (نبيلة،2022) ، (Al-Ramadan & Hasan, 2021).
- **المحور الثاني: المتغير التابع (حماية نظم المعلومات)** ويحتوي على 16 فقرة، وقد اعتمدت فقرات هذا المتغير استناداً إلى دراسات سابقة أمثال:(Alsharabi,2020).

الجدول: 3-3

مكونات أبعاد الاستبانة

المتغيّرات	الأبعاد	عدد الفقرات
(المتغيّر المستقل) : متغيرات الأمن السيبراني	المتطلبات التنظيمية	10
	المتطلبات الفنية	9
	الامتثال للأطر والمعايير الدولية	10
	تدابير الأمن المادي	8
(المتغيّر التابع) : حماية نظم المعلومات		16

الإجمـــالي	53

6.3 دليل قراءات النتائج للإحصاء الوصفي:

استخدم الباحث مقياس ليكرت الخماسي (Likert Scale) دليلاً لقراءة نتائج الدراسة وتفسيرها للإحصاء الوصفي، وهو المقياس المستخدم في الكثير من الدراسات الإدارية وغيرها، ويتكوَّن المقياس من خمس درجات للموافقة تشير أعلاها (5) إلى أعلى موافقة، وأدناها (1) إلى أدنى موافقة، وتتوزع القيم بين 2، 3، 4 بين الموافقة (غير موافق، محايد، موافق) على التوالي (Ahmed, M. Kamarruddeen & Others, 2022). كما هو موضح في الجدول (3-4).

الجدول: 3-4

دليل قراءة النتائج (مقياس ليكرت الخماسي)

النطاق العددي	مستوى درجة الموافقة	مدى الأهمية النسبية
1.0 – 1.8	منخفضة جداً	0-20%
1.81 – 2.6	منخفضة	21-40%
2.61 – 3.4	متوسطة	41-60%
3.41 – 4.2	مرتفعة	61-80%
4.21 – 5.0	مرتفعة جداً	81-100%

7.3 صدق وثبات الاستبانة:

يقصد بصدق الاستبانة مدى صدق عباراتها، وقدرتها على قياس المتغيرات التي صممت لقياسها، وللتحقق من صدق الاستبانة المستخدمة في الدراسة تم قياس الإجراءات الآتية:

1.7.3 الصدق الظاهري (صدق المحتوى):

يعتمد صدق الأدوات القياسية، مثل الاستبانات، على تقييم المحكمين لصلاحية الأداة وموثوقيتها، وفي هذا السياق يقوم الباحث بانتداب مجموعة من المحكمين ذوي الخبرة والتخصص في مجال الدراسة، مثل تكنولوجيا المعلومات والإدارة، بهدف التحقق من وضوح صياغة الفقرات ودقتها، الموجودة في الاستبانة، وفي الدارسة الحالية، تم عرض الاستبانة على 7 من المتخصصين والأكاديميين بهدف مراجعتها وتقديم ملاحظاتهم عليها، وبعد التعديل النهائي والأخذ بملاحظات المحكمين تم توزيع الاستبانة.

2.7.3.الاتساق الداخلي:

لقياس الاتساق الداخلي لفقرات أبعاد محاور الدراسة تم استخدام معامل الارتباط بين الفئات (Intraclass Correlation) وهو مؤشر يعبر عن المفهوم الدقيق لمعامل الثبات لأنه يعكس الفروق في الأداء، ويعتمد على تحليل التباين (الاختلاف) بين فقرات البُعد، ويمكن قياس باستخدام العلاقة التالية:

$$ICC = \frac{MS_{betw} - MS_{with}}{MS_{betw} + (n-1)MS_{with}}$$

الجدول: 3-5

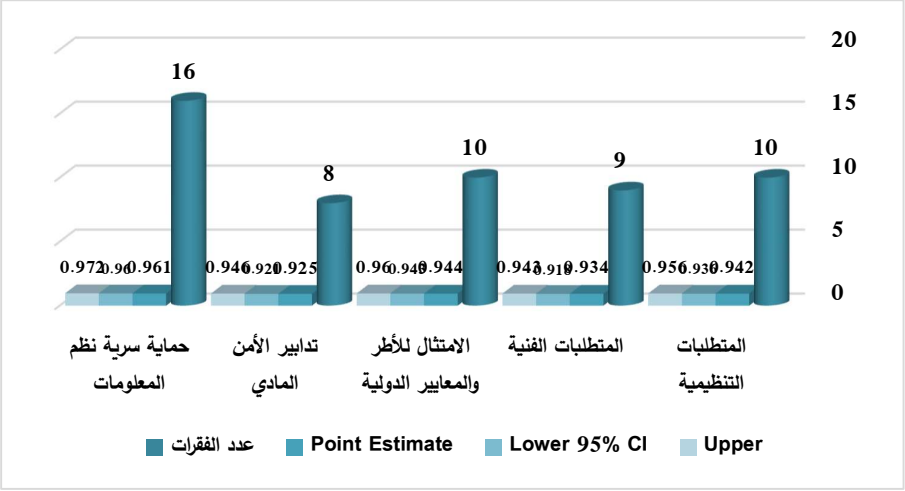
الاتساق الداخلي لفقرات أبعاد الدراسة

أبعاد الدراسة	عدد الفقرات	POINT ESTIMATE	LOWER 95% CI	UPPER 95% CI
المتطلبات التنظيمية	10	0.942	0.936	0.956

المتطلبات الفنية	9	0.934	0.918	0.943
الامتثال للأطر والمعايير الدولية	10	0.944	0.943	0.96
تدابير الأمن المادي	8	0.925	0.921	0.946
حماية سرية نظم المعلومات	16	0.961	0.96	0.972

الشكل:2.3

الاتساق الداخلي لفقرات أبعاد الدراسة



توضح النتائج في الجدول (3–5) والشكل (2.3) أن جميع معاملات الاتساق عالية جداً تقترب من الواحد الصحيح، وهذا يعني أن الفقرات داخل كل بُعد متسقة ومتقاربة جداً، أي لا يوجد اختلاف في الآراء بين الفقرات داخل كل بُعد من أبعاد الدراسة.

8.3 ثبات أداة الدراسة:

قام الباحث بالتحقُّق من ثبات أداة الدراسة باستخدام معادلة Cronbach's Alpha وكذلك McDonald's ω لمعرفة درجة ثبات المقياس المستخدم وصلاحيتها ومؤشرات الثبات للمتغيرات الكامنة المعبرة عن أبعاد الدراسة، كما في الجدول رقم (6.3) والشكل رقم (2.3).

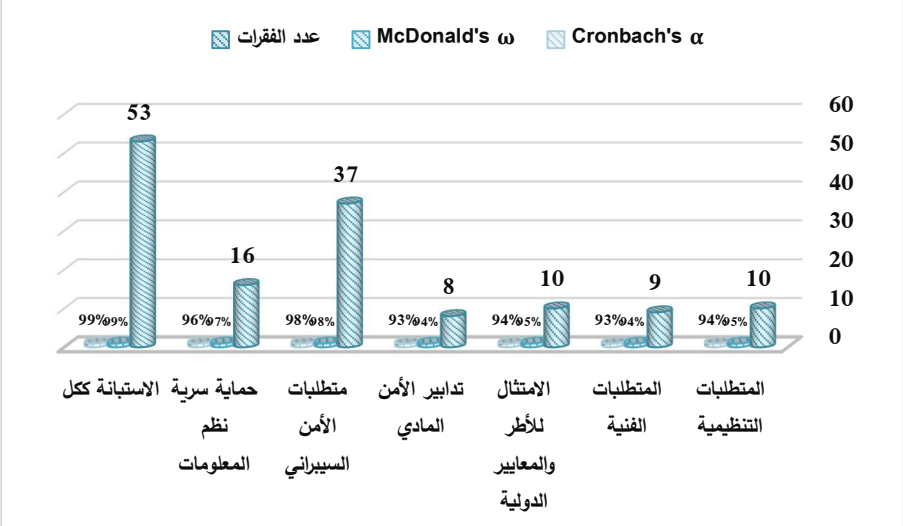
الجدول: 3-6

قيم مؤشرات الفاكرونباخ وماكدونالد لقياس ثبات أداة الدراسة

ESTIMATE	عدد الفقرات	MCDONALD'S Ω	CRONBACH'S A
الحد الأدنى للمؤشر		0.7	0.7
المتطلبات التنظيمية	10	0.947	0.942
المتطلبات الفنية	9	0.939	0.934
الامتثال للأطر والمعايير الدولية	10	0.952	0.944
تدابير الأمن المادي	8	0.935	0.925
متطلبات الأمن السيبراني	37	0.981	0.978
حماية سرية نظم المعلومات	16	0.966	0.961
الاستبانة ككل	53	0.987	0.986

الشكل: 3.3

قيم مؤشرات الفاكرونباخ وماكدونالد لقياس ثبات أداة الدراسة



يبين من الجدول (3-6) والشكل (3.3) أن مؤشرات الثبات للمتغيرات الكامنة المعبرة عن أبعاد الدراسة ومحاورها التي تقريبا في مجملها قد تجاوزت الحدود الدنيا لمدى كل مؤشر، حيث يلاحظ بأن معامل الثبات (McDonald's ω) قد تجاوز الحد الأدنى (0.70) لجميع الابعاد مما يدل على أن مقياس أداة الدراسة يتمتع بمستويات ثبات مقبولة لغرض الدراسة العلمي، وكذلك بالنسبة لمعامل الثبات الفا كرو نباخ (Cronbach's α) فقد تجاوز الحد الأدنى (0.70) (شيخي، مليكة، دحو، وسعيدي، و برزوق، 2020)، مما يدل على أن فقرات المحاور والأبعاد تتمتع بدرجة عالية من الثبات، و يؤكد صحة الاستبانة وصدقها لتحليل البيانات الخاصة بأسئلة الدراسة ، وهناك تفصيل أكثر لاحقاً في تحليل المعادلات البنائية.

9.3 مؤشرات الموثوقية والصلاحية لأداة الدراسة:

ولقياس موثوقية وصلاحية أداة الدراسة تم اختبار معامل التجانس والثقة ومعامل الصدق التميزي كما هو في الجدول رقم (7.3).

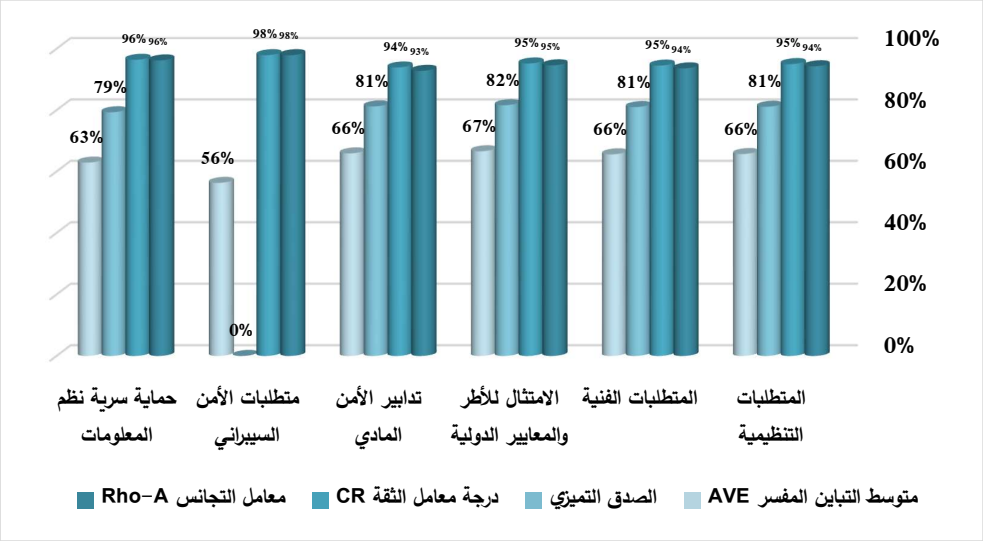
الجدول: 3-7

مؤشرات موثوقية وصلاحية أداة الدراسة

متغيرات الدراسة	معامل التجانس RHO-A	درجة معامل الثقة CR	الصدق التميزي	متوسط التباين المفسر AVE
مدى المؤشر	أكبر من 0.70	أكبر من 0.70	أكبر من 0.70	أكبر من 0.50
المتطلبات التنظيمية	0.943	0.950	0.811	0.657
المتطلبات الفنية	0.936	0.945	0.810	0.656
الامتثال للأطر والمعايير الدولية	0.946	0.952	0.816	0.666
تدابير الأمن المادي	0.928	0.939	0.812	0.659
متطلبات الأمن السيبراني	790.9	790.9	--	630.5
حماية سرية نظم المعلومات	20.96	640.9	0.793	290.6

الشكل: 4.3

مؤشرات موثوقية وصلاحية أداة الدراسة



يبين الجدول (3-7) والشكل (4.3) قيم كل من معامل التجانس ومعامل الثقة ومعامل الصدق التمييزي ومتوسط التباين المفسر والمدى القبول لكل مؤشر حيث يوضح أن جميع قيم المؤشرات المذكورة ضمن مدى القبول المحدد لجميع أبعاد الدراسة ومحاورها، مما يعني أن الأبعاد تفسر معظم التباين لفقراتها وأن جميع العوامل (الأبعاد) قد مثلت المتغيرات المقاسة (الفقرات) المكونة لها بدرجة عالية ، ومن ثم تتميز أداة الدراسة بمستويات عالية من الصدق البنائي ومستويات تجانس لمكوناتها البنائية وإمكانية التمييز فيما بينها من خلال الفقرات التي تمثل كل بعد لأغراض الدراسة العلمي.

10.3. الأساليب الإحصائية المستخدمة:

بعد تصميم الاستبانة واختبارها وتعديلها وتعميمها على العينة المستهدفة، ثم جمعها من المستجيبين، تم استخدام برنامج (IBM SPSS V.27) وبرنامج (SMART.PLS 3 وذلك باستخدام الأساليب الإحصائية التالية:

1- التكرارات والنسب المئوية للمتغيرات الديموغرافية (الخصائص الشخصية) لأفراد عينة الدراسة.

2- المتوسطات الحسابية ومعاملات الاختلاف لفقرات أداة الدراسة والأهمية النسبية.

3- اختبار مربع كاي لمعرفة تطابق آراء أفراد العينة مع ما هو متوقع لها.

4- معاملات التحميل أو التشبع (Factor Loading) لقياس مدى تحميل الفقرات على أبعادها.

5- معامل الثبات ماكدونالد أوميجا (McDonald's ω)، معامل الثبات الفاكرونباخ (Cronbach Alpha).

6- معاملات الموثوقية (معامل التجانس Rho–A، درجة معامل الثقة Composite Reliability، متوسط التباين المفسر AVE) لدراسة مصداقية وموثوقية أداة الدراسة.

7- الصدق التمييزي (Discriminant Validity) لقياس مدى تمييز أبعاد الدراسة من خلال الفقرات الممثلة له.

8- التحليل العاملي التوكيدي (معاملات التحميل – اختبار (KMO) لكفاية حجم العينة).

9- تحليل التباين اللامعلمي (اختبار كروســـكال والس) لمعرفة الاختلاف بين آراء أفراد عينة الدراسة اتجاه محاور الدراسة والتي تعزى إلى اختلاف خصائصهم الديموغرافية.

10-نماذج المعادلة البنائية (SEM) لمعرفة ملاءمة النموذج النظري (ملاءمة أداة الدراسة)، حسب إجابات أفراد عينة الدراسة، حيث من ضمن مخرجات قياس والعلاقة التأثيرية معامل التحديد R^2 الذي يتم الاعتماد علية في تفسير التغيرات في المتغير التابع التي تعزى إلى التغيرات في المتغير المستقل، بالإضافة إلى معامل حجم العلاقة والأثر F^2 والذي يبين مقدار قوة علاقة أثر التغير الذي يحدثه المتغير المستقل في المتغير التابع.

الفصل الرابع:

تحليل البيانات ومناقشة النتائج

الفصل الرابع: تحليل البيانات ومناقشة النتائج

يتناول هذا الفصل عرضاً لتحليل البيانات واختبار الفرضيات حيث يقدم وصفا مفصلاً للمتغيرات الديموغرافية المتعلقة بأفراد عينة الدراسة من المستجيبين، وتحليلا لإجاباتهم على فقرات أداة الدراسة، ووصفا لمتغيرات أنموذج الدراسة وأبعاده الفرعية، كما يعرض نتائج اختبار الفرضيات التي توصلت إليها الدراسة، كذلك مناقشتها والتعليق عليها وعرض الاستنتاجات والتوصيات.

1.4 عرض البيانات الديموغرافية لأفراد عيّنة الدراسة وتحليلها:

يتناول هذا الجزء عرضا لنتائج تحليل البيانات الديموغرافية لأفراد عينة الدراسة، على النحو الآتي:

1.1.4 متغيّر المؤهل العلمي:

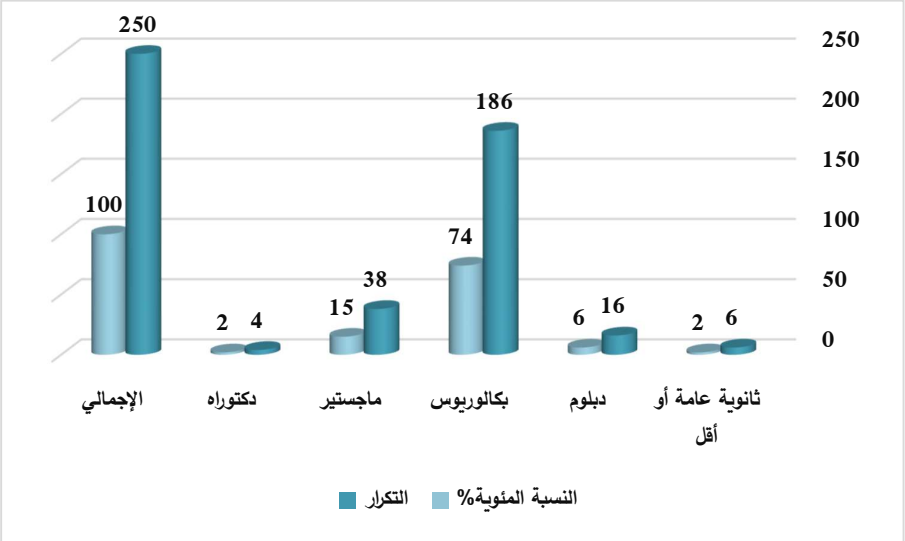
يتناول متغيّر المؤهل العلمي التكرار والنسب المئوية للمؤهلات العلمية الحاصلين عليها أفراد العينة كما هو موضح بالجدول (4-1) والشكل رقم (1.4).

جدول: 4-1

خصائص أفراد العيّنة وفقاً لمتغيّر المؤهل العلمي

المؤهل العلمي	التكرار	النسبة المئوية%
ثانوية عامة أو أقل	6	2
دبلوم	16	6
بكالوريوس	186	74
ماجستير	38	15
دكتوراه	4	2
الإجمالي	**250**	**100**

الشكل: 1.4



يوضح الجدول(4-1) والشكل(1.4) التوزيع التكراري والنسبة المئوية للخصائص الديموغرافية لعينة الدراسة، وقد جاء غالبية المستجيبين من حملة مؤهل البكالوريوس وبنسبة 74% تقريبا فيما جاء حملة درجة الماجستير في الترتيب الثاني وبنسبة 15% تقريبا، يليهم حملة الدبلوم بنسبة 6% تقريبا، والنسبة المتبقية توزعت على الثانوية العامة 2% وحملة الدكتوراه 2% تقريبا.

يستنتج الباحث أن النسبة العالية لحملة البكالوريوس تشير إلى أن قطاع البنوك اليمنية يوظف مستوى تعليمي جيد، مما قد يسهل عملية تدريب وتعزيز مهارات الأمن السيبراني لديهم، وأن وجود موظفين من حملة الماجستير يدل على توفر قاعدة معرفية متقدمة يمكن الاعتماد عليها لفهم وتنفيذ متطلبات الأمن السيبراني المعقدة وتنفيذها.

2.1.4 متغيّر التخصص:

يتناول هذا الجزء خصائص عينة الدراسة حسب متغير التخصص كما هو موضح في الجدول (4-2) والشكل (2.4) أدناه على النحو الآتي:

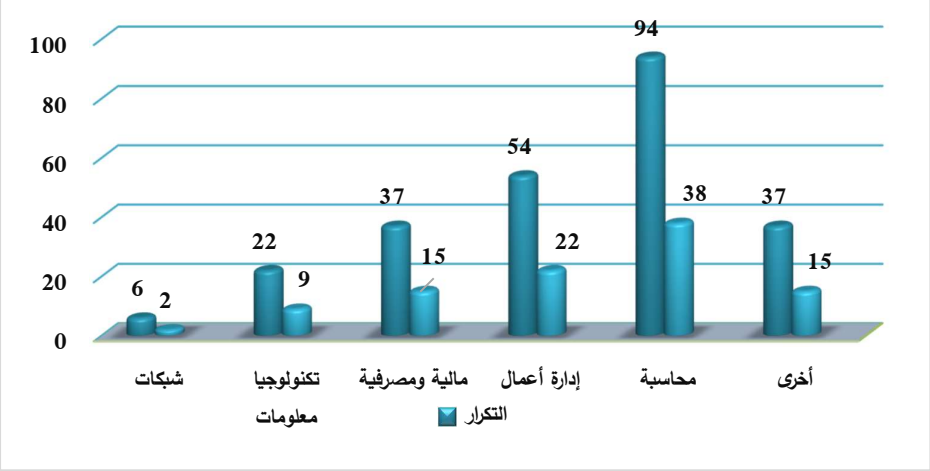
الجدول: 4-2

خصائص عيّنة الدراسة وفقاً لمتغيّر التخصص

التخصص	التكرار	النسبة المئوية%
شبكات	6	2
تكنولوجيا معلومات	22	9
مالية ومصرفية	37	15
إدارة أعمال	54	22
محاسبة	94	38
أخرى	37	15
الإجمالي	**250**	**100%**

الشكل: 2.4

خصائص عينة الدراسة وفقا لمتغير التخصص



يبين الجدول (4-2) والشكل (2.4) أن غالبية أفراد العينة يحملون تخصص المحاسبة بنسبة 38%، وجاء تخصص إدارة الاعمال في الترتيب الثاني بنسبة 22%، بينما تخصص مالية ومصرفية جاء ثالثا بنسبة 15%، وتكنولوجيا معلومات 9% وشبكات 2% وتخصصات أخرى غير مصنفه 15%.

ويعزو الباحث أن نتائج الدراسة تُظهر تركيزًا ملحوظًا في التخصصات المالية والإدارية ضمن القطاع المصرفي، مع تمثيل أكبر للمحاسبة وإدارة الأعمال. يعكس هذا التوزيع الحاجة المتزايدة للمهارات المالية والإدارية، مشيرًا إلى أهمية الإدارة المالية الفعالة والتخطيط الاستراتيجي، ومن جهة أخرى، يلقي التمثيل الأقل لتخصصات تكنولوجيا المعلومات والشبكات الضوء على الحاجة إلى تعزيز المهارات التكنولوجية لمواجهة التحديات السيبرانية ودعم التحول الرقمي. هذه النتائج تشير إلى أهمية التدريب والتطوير المهني في مجالات مثل الأمن السيبراني وتكنولوجيا المعلومات، وتوفر أيضًا فرصة للبحوث المستقبلية حول تأثير التخصصات المختلفة على الابتكار والأمان في القطاع المصرفي.

3.1.4 متغيّر المسمى الوظيفي:

يتناول هذا الجزء خصائص عينة الدراسة حسب متغير المسمى الوظيفي كما هو موضح في الجدول (4–3) والشكل (3.4) أدناه على النحو الآتي:

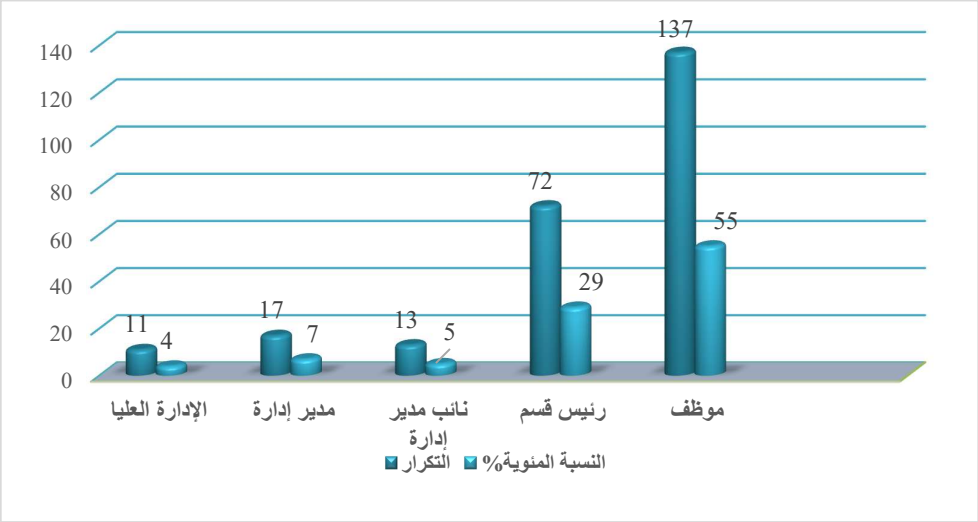
الجدول: 4–3

خصائص عيّنة الدراسة وفقاً لمتغيّر المسمى الوظيفي

المسمى الوظيفي	التكرار	النسبة المئوية%
الإدارة العليا	11	4
مدير إدارة	17	7
نائب مدير إدارة	13	5
رئيس قسم	72	29
موظف	137	55
الإجمالي	**250**	**100%**

الشكل: 3.4

خصائص عينة الدراسة وفقا لمتغير المسمى الوظيفي



يوضح الجدول (4–3) والشكل (3.4) أن غالبية أفراد العينة من الموظفين بما نسبته 55% من اجمالي حجم العينة بينما رؤساء الأقسام مثلوا 29% والنسبة المتبقية توزعت بين نواب المديرين والمديرين والإدارة العليا.

يشير الباحث أن الموظفين في العينة تدل على ضرورة توجيه البرامج التدريبية لمستويات تشغيلية واسعة، لضمان تطبيق معايير الأمن على جميع المستويات الوظيفية.

4.1.4 متغيّر سنوات الخبرة:

يتناول هذا الجزء خصائص عينة الدراسة حسب متغير سنوات الخبرة كما هو موضح في الجدول (4–4) والشكل (4.4) على النحو الآتي:

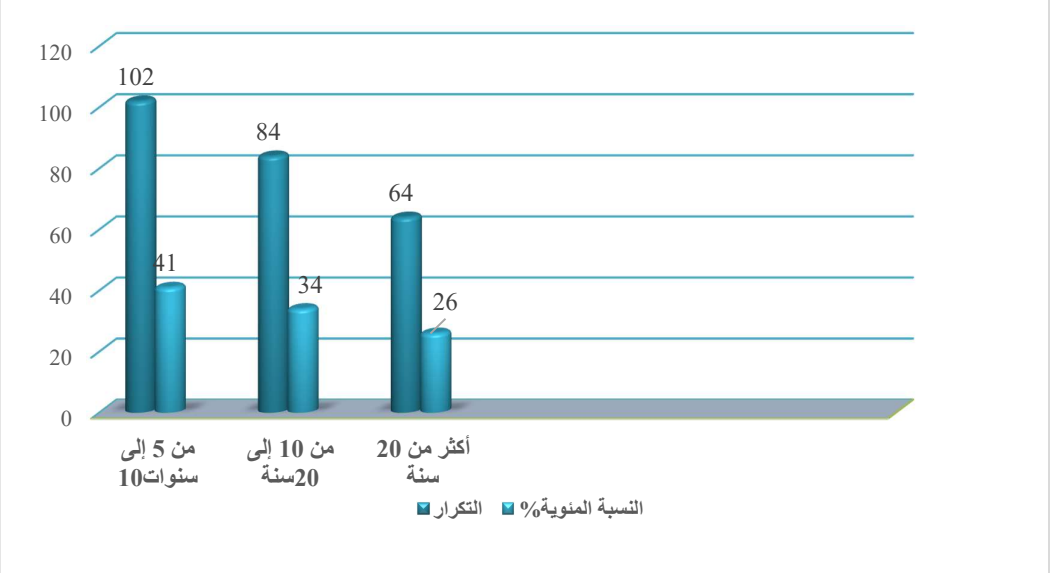
الجدول: 4–4

خصائص عيّنِة الدراسة وفقاً لمتغيّرِ سنوات الخبرة

سنوات الخبرة	التكرار	النسبة المئوية%
من 5 إلى سنوات10	102	41
من 10 إلى 20سنة	84	34
أكثر من 20 سنة	64	26
الإجمالي	**250**	**100%**

الشكل: 4.4

خصائص عينة الدراسة وفقا لمتغير الخبرة



يبين الجدول (4-4) والشكل (4.4) أن النسبة الأعلى من ذوي الخبرات ما بين 5 إلى أقل من 10 أعوام وبنسبة 34% تقريبا، يليهم ذوو الخبرات من 10 سنوات إلى 20 سنه وبنسبة 34% ويليهم ذوو الخبرات الأعلى من 20 عاما وبنسبة 26%.

وتعكس هذه النتائج إدراك البنوك لأهمية توفير الخبرة المتوسطة القادرة على التعامل مع وسائل التكنولوجيا الحديثة وقدرتهم على التعلم والتكيف مع أنظمة الأمن الجديدة والمتطورة.

5.1.4 متغيّر نوع البنك:

يتناول هذا الجزء خصائص عينة الدراسة حسب متغير نوع البنك كما هو موضح في الجدول (4-5) والشكل (5.4) أدناه على النحو الآتي:

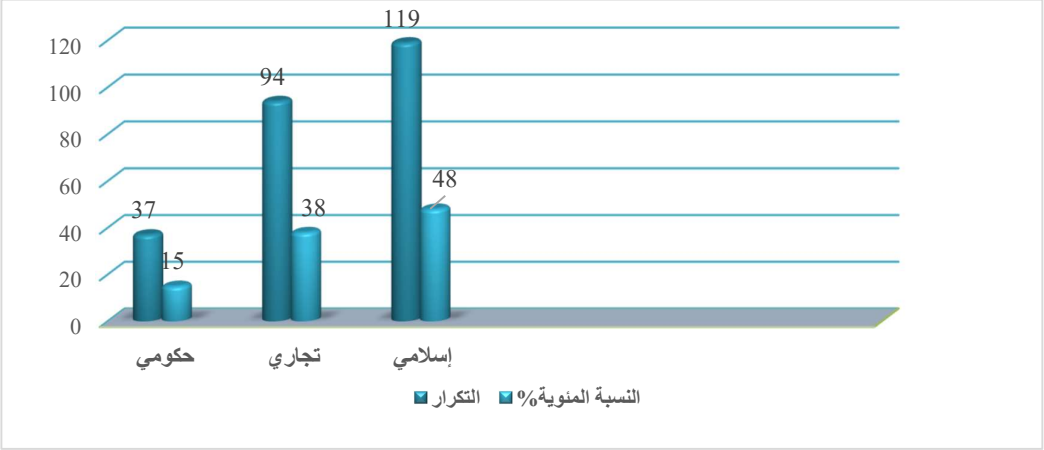
الجدول: 4-5

خصائص عيّنة الدراسة وفقاً لمتغيّر نوع البنك

نوع البنك	التكرار	النسبة المئوية%
حكومي	37	15
تجاري	94	38
إسلامي	119	48
الإجمالي	**250**	**100%**

الشكل: 5.4

خصائص عينة الدراسة وفقا لمتغير نوع البنك



يوضح الجدول (4-5) والشكل (5.4) أن أفراد عينة الدراسة تتوزع بحسب نوع البنك الذي يعملون به إلى بنوك إسلامية بنسبة 48% وتجارية بنسبة 38% وحكومية بنسبة 15% تقريبا.

مما يدل على استحواذ البنوك الإسلامية على ما نسبته 48% من أفراد العينة قيد الدراسة، فيما تأتي البنوك التجارية ثانيا بنسبة 38%.

يؤكد الباحث أن النسب العالية للعاملين في البنوك الإسلامية والتجارية تعطي دلالة على أن هذه البنوك قد تكون أكثر عرضة للمخاطر السيبراني بسبب حجم عملياتها الكبيرة، ويجب عليها تحديث أنظمة الأمن السيبراني لديها.

6.1.4 متغيّر اسم البنك:

يتناول هذا الجزء خصائص عينة الدراسة حسب متغير اسم البنك كما هو موضح في الجدول (4-6) والشكل (6.4) أدناه على النحو الآتي:

الجدول: 4-6

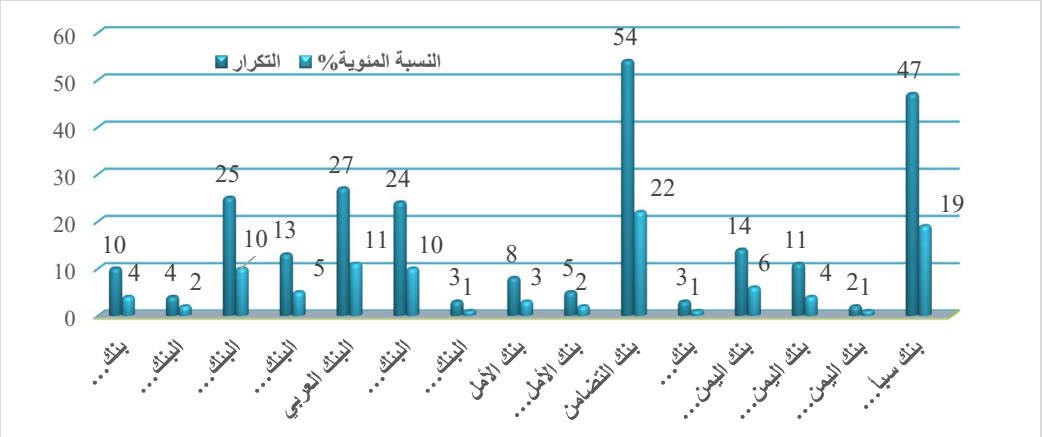
خصائص عيّنة الدراسة وفقاً لمتغيّر اسم البنك

اسم البنك	التكرار	النسبة المئوية%
بنك التسليف (كاك بنك)	10	4
البنك اليمن والكويت	4	2
البنك الأهلي التجاري	25	10
البنك التجاري	13	5
البنك العربي	27	11
البنك المركزي اليمني	24	10
البنك اليمني للإنشاء والتعمير	3	1
بنك الأمل	8	3
بنك الأمل للتمويل الأصغر الإسلامي	5	2
بنك التضامن	54	22

بنك الكريمي الإسلامي	3	1
بنك اليمن البحرين الشامل	14	6
بنك اليمن الأول	11	4
بنك اليمن والخليج	2	1
بنك سبأ الإسلامي	47	19
الإجمالي	**250**	**100%**

الشكل: 6.4

خصائص عينة الدراسة وفقا لمتغير اسم البنك



يوضح الجدول (4-6) والشكل (6.4) أن بنك التضامن يستحوذ على غالبية العينة المبحوثة بما نسبته 22% من إجمالي العينة، يأتي بنك سبأ في الترتيب الثاني بنسبة 19% بينما استحوذ البنك العربي على 11% وجاء ثالثا، فيما توزعت بقية أفراد العينة على بقية البنوك قيد الدراسة بنسب مختلفة.

يعزو تركز أغلب أفراد العينة في بنكي التضامن وسبأ بما يمثل(101) من الموظفين من إجمالي (250) لعدد (15) بنكاً إلى احتفاظ تلك البنوك بعدد أكبر من موظفيها في حين تتجه

أغلب البنوك إلى تقليص وظائفها نتيجة لانعكاس الأوضاع الاقتصادية للبلد على أنشطتها المصرفية، في حين تبقى البنوك الإسلامية أقل تضررا نظرا لطبيعة أنشطتها.

7.1.4 متغيّر عدد الدورات في الأمن السيبراني:

يتناول هذا الجزء خصائص عينة الدراسة حسب متغير عدد الدورات كما هو موضح في الجدول (4-7) والشكل (7.4) أدناه على النحو الآتي:

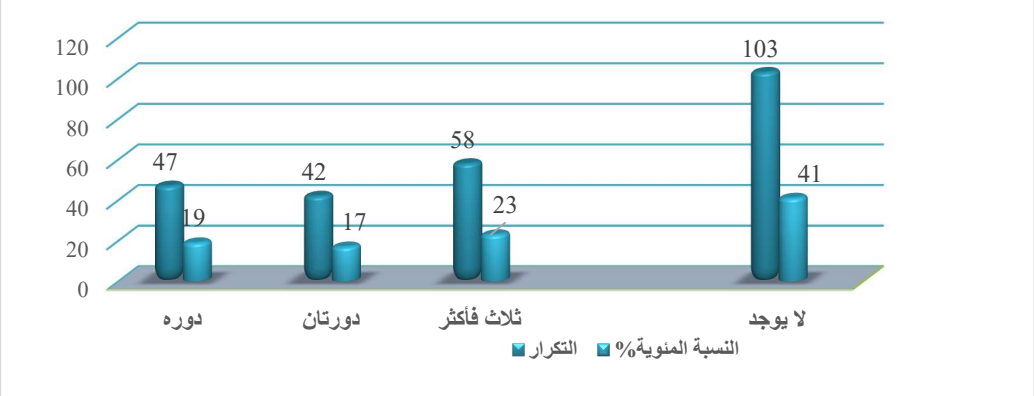
الجدول: 4-7

خصائص عيّنة الدراسة وفقاً لمتغيّر عدد الدورات

عدد الدورات	التكرار	النسبة المئوية%
دوره	47	19
دورتان	42	17
ثلاث فأكثر	58	23
لا يوجد	103	41
الإجمالي	**250**	**100%**

الشكل: 7.4

خصائص عينة الدراسة وفقا لمتغير عدد الدورات



يبين الجدول (4–7) والشكل (7.4) أن ما نسبته 41% من أفراد العينة لم يتلقوا أي دورات تدريبية في مجال الأمن السيبرانية، بينما 23% تلقوا أكثر من دورتين و19% دورة واحدة فقط و17 % دورتين. النسبة المرتفعة للأفراد الذين لم يتلقوا دورات تدريبية تدل على وجود فجوة كبيرة في التدريب والتأهيل، التي يجب سدها لضمان رفع مستوى الوعي والكفاءة في مجال الأمن السيبراني.

ويشير الباحث الى أن النسبة المرتفعة للأفراد لم يتلقوا دورات تدريبية تدل على وجود فجوة كبيرة في التدريب والتأهيل والتي يجب سدها لضمان رفع مستوى الوعي والكفاءة في مجال الأمن السيبراني.

2.4 التحليل الوصفي للنتائج حسب مكونات الاستبانة:

يتناول هذا الجزء التحليل الوصفي لنتائج متغيرات الدراسة والمتمثلة بالمتغير المستقل: متطلبات الأمن السيبراني، والمتغير التابع: حماية نظم المعلومات، وقد استُخدم المتوسط الحسابي المرجح بتكرارات درجات المقياس والأهمية النسبية، والانحرافات المعيارية، لمعرفة درجة موافقة أفراد العينة لمتغيرات الدراسة.

1.2.4 نتائج تحليل أبعاد المتغير المستقل (متطلبات الأمن السيبراني):

يشمل هذا الجزء نتائج تحليل أبعاد المتغيِّر المستقل: متطلبات الأمن السيبراني، وهي (المتطلبات التنظيمية، المتطلبات الفنية، الامتثال للأطر والمعايير الدولية، تدابير الأمن المادي)، وذلك على النحو الآتي:

1.1.2.4 نتائج تحليل فقرات البُعد الأول (المتطلبات التنظيمية):

يتناول هذا الجزء المتوسطات الحسابية، ومعامل الاختلاف، والأهمية النسبية، ومعنوية حسن المطابقة، ودرجات موافقة إجابات أفراد العيِّنة لمستوى توافر المتطلبات التنظيمية للأمن السيبراني في حماية نظم المعلومات في البنوك اليمنية، الجدول (4-8) يوضح ذاك.

الجدول: 4-8

نتائج تحليل فقرات المتطلبات التنظيمية

الرمز	الفقرة	الوسط المرجح	الأهمية النسبية	معامل الاختلاف	معنوية حسن المطابقة	معامل التحميل
x1	يقوم البنك بانتظام بتحديث سياسات الأمن السيبراني الخاصة به وفقًا للوائح التي وضعتها الهيئات والمنظمات الدولية.	4.03	% 81	% 23	0.000	0.811
x2	لدى البنك فريق متخصص مسؤول عن ضمان الامتثال للوائح الأمن السيبراني.	3.98	% 80	% 27	0.000	0.842
x3	يقوم البنك بتدريب الموظفين بشكل منتظم على المتطلبات التنظيمية في مجال الأمن السيبراني.	3.64	%73	% 32	0.000	0.801
x4	يقوم فريق المراجعة الخارجي بإجراء عمليات تدقيق داخلية	3.68	% 74	% 31	0.000	0.781

	لتقييم التزام البنـك بلوائح الأمن السيبراني التنظيمية.					
x5	يتخـذ البنـك خطـة واضـــحـة للاســـتجابـة للحوادث وفقًا لما تتطلبه اللوائح.	3.92	% 78	%27	0.000	0.822
x6	يلتزم البنــك بمتطلبــات إعــداد التقارير الإلزامية لحوادث الأمن السيبراني.	3.75	% 75	% 27	0.000	0.864
x7	حضـور البنك منتديات الصناعة وورش العمــل المتعلقــة بلوائح الأمن السيبراني داخليا وخارجيا.	3.59	% 72	% 30	0.000	0.773
x8	يتخذ البنك إجراءات صـــارمة وحازمـة لمعالجـة عدم الامتثال للمتطلبات التنظيمية.	3.86	% 77	% 30	0.000	0.847
x9	يتعـاون البنـك مع الســلطـات التنظيمية في معالجة قضـــايا الأمن السيبراني.	3.82	%76	% 25	0.000	0.836
x10	يعتمـد البنـك الامتثـال التنظيمي جانبًا مهمًا من استراتيجية الأمن السيبراني الخاصة به.	3.78	% 76	% 28	0.000	0.859
	المتطلبات التنظيمية	**3.81**	**% 76**	**% 23**		

يبين الجدول (4-8) توصـيف الاسـتجابة لأفراد عينة الدراسـة بحسـب مقياس مسـتوى الموافقة بناء على المتوسـط الحسـابي المرجح بتكرارات درجات المقياس وأهميته النسـبية نسـبة لأعلى درجة فيه الذي يبين درجة موافقة عالية لبُعد المتطلبات التنظيمية كأحد أبعاد متطلبات الأمن السيبراني بمتوسط حسابي (3.81)، وأهمية نسبية (76%)، ومعامل اختلاف (23%).

وبناء على ترتيب الفقرات بحسـب الأهمية النسـبية جاءت الفقرة (x2) التي تنص على أنه :"لدى البنك فريق متخصص مسؤول عن ضمان الامتثال للوائح الأمن السيبراني." بأهمية نسبية (80%) ومعامل اختلاف (27%) في المرتبة الأولى وجاءت الفقرة (x7) والتي تنص على:

"حضـور البنك منتديات الصـناعة وورش العمل المتعلقة بلوائح الأمن السـيبراني داخليا وخارجيا". في المرتبة الأخيرة بأهمية نسـبية (72%) ومعامل اختلاف (30%) وتشـير الدلالة الإحصـائية لاختبار مربع كأي لحسن المطابقة إلى معنوية آراء المستجيبين بحسب تكرارات مستويات الموافقة على جميع الفقرات الممثلة للمتطلبات التنظيمية عند مسـتوى دلالة 0.01، كما تشـير معاملات تحميل بُعد المتطلبات التنظيمية على الفقرات التي تقيسـه والممثلة له درجة اتسـاق عالية (أكبر من 0.40) لمستويات استجابة المستجيبين بحسب مقياس أداة الدراسة على جميع فقرات البُعد.

من خلال تحليل البيانات المتعلقة بالمتطلبات التنظيمية للبنوك قيد الدراسة، يمكن الإشارة إلى أن الفقرة المرجعية (2x) تُفيد بأن البنوك المستهدفة في الدراسة تدين بالالتزام الدوري بتجديد سياسات الأمن السيبراني بما يتوافق مع المعايير والمتطلبات الصادرة عن الهيئات والمنظمات الدولية. وقد تم تحديد قيمة التقدير المرجح للفقرة المذكورة بـ 4.03، مما يُؤكد على الالتزام المستمر للبنوك بالمعايير التنظيمية العالمية. وفي السياق ذاته، تظهر الفقرة المرجعية 7x قيمة تقدير مرجح تقدر بـ 3.59، مما يشير إلى وجود فجوة في توجيه البنوك المبحوثة نحو المشاركة الفعّالة في منتديات الصناعة وورش العمل المرتبطة بالأمن السيبراني. بالإضافة إلى ذلك، تم تحديد نقص في الفقرة المرجعية 3x حيث أُسندت لها قيمة تقدير مرجح قدرها 3.64، مما يدل على الحاجة الماسة لتطوير جهود تدريب الموظفين بما يتوافق مع المتطلبات التنظيمية.

وفي هذا السياق، تظهر النتائج أن البنوك تأخذ مسألة الأمن السيبراني على محمل الجد، لكن هناك حاجة لزيادة الجهود في بعض المجالات الخاصة بالتدريب والمشاركة في منتديات الصناعة لتحقيق مستوى أعلى من الامتثال والاستجابة للتهديدات السيبرانية.

2.1.2.4 نتائج تحليل فقرات البُعد الثاني (المتطلبات الفنية):

يتناول هذا الجزء المتوسطات المرجحة، والأهمية النسبية، ومعاملات الاختلاف، ومعنوية حسن المطابقة لإجابات أفراد العيِّنة لمستوى توافر المتطلبات الفنية للأمن السيبراني في حماية نظم المعلومات في البنوك اليمنية، الجدول (4-9) يوضح ذلك.

الجدول: 4-9

نتائج تحليل فقرات بعد المتطلبات الفنية

الرمز	الفقرة	الوسط المرجح	الأهمية النسبية	معامل الاختلاف	معنوية حسن المطابقة	معامل التحميل
c1	يستخدم البنك أحدث برامج الحماية وبرامج مكافحة الفيروسات والبرامج الضارة على جميع الأنظمة.	4.32	% 86	% 20	0.000	0.810
c2	يعتمد البنك على تقنيات تشفير قوية مثل SSL/TLS (Secure Sockets Layer/Transport Layer Security)	4.04	% 81	% 23%	0.000	0.818
c3	يمتلك البنك الجيل التالي من جدران الحماية لحماية أنظمة المعلومات الخاصة به من التهديدات الخارجية.	3.97	% 79	% 26	0.000	0.865
c4	يعتمد البنك على تقنيات متقدمة للكشف عن التسلل والوقاية منه، مثل أنظمة الكشف عن التسلل ((IDS	3.99	% 80	% 24	0.000	0.837
c5	يُجري البنك تحديثات أمنية وتصحيحات منتظمة لمكونات البرامج والأجهزة.	4.10	% 82	% 22	0.000	0.832

c6	يقوم البنـك بوضـــع إجراءات للوصـــول الأمن إلى أنظمـة المعلومات الخاصة به.	4.05	% 81	% 25	0.000	0.835
c7	يقوم البنـك بـانتظـام بـإجراء تقييمـات الضـــعف واختبـار الاختراق على أنظمة المعلومات الخاصة به.	3.91	% 78	% 26	0.000	0.864
c8	يمتلك البنك تدابير آمنة وسريعة للنســخ الاحتياطي بشــكل آلي للبيانات والتصميمات الهامة في أي لحظة.	4.13	% 83	% 25	0.000	0.797
c9	يســـتخدم البنـك الشـــبكـات الافتراضـــيـة مثـل VLANs (Virtual Local Area Networks)	3.94	% 79	% 23	0.000	0.697
	المتطلبات الفنية	**4.05**	**% 81**	**% 19**		

يبين الجدول (4–9) توصـيف الاسـتجابة لأفراد عينة الدراسـة بحسـب مقياس مسـتوى الموافقة بناء على المتوسـط الحسـابي المرجح بتكرارات درجات المقياس وأهميته النسـبية نسـبة لأعلى درجة فيه والذي يبين درجة موافقة عالية لبُعد المتطلبات الفنية كأحد أبعاد متطلبات الأمن السيبراني بمتوسط حسابي (4.05) وأهمية نسبية (81%) ومعامل اختلاف (19%).

وبناء على ترتيب الفقرات بحســب الأهمية النســبية جاءت الفقرة (c1) التي تنص على: "يســتخدم البنك أحدث برامج الحماية وبرامج مكافحة الفيروســات والبرامج الضــارة على جميع الأنظمة.." بأهمية نســبية (86%) ومعامل اختلاف (27%) في المرتبة الأولى، وجاءت الفقرة (c7) والتي تنص على: " يقوم البنك بوضـــع إجراءات للوصـــول الأمن إلى أنظمة المعلومات الخاصة به.." في المرتبة الأخيرة بأهمية نسبية (78%) ومعامل اختلاف (26%) وتشير الدلالة الإحصـائية لاختبار مربع كأي لحسـن المطابقة إلى معنوية آراء المسـتجيبين بحسـب تكرارات

مستويات الموافقة على جميع الفقرات الممثلة للمتطلبات الفنية عند مستوى دلالة (0.01)، كما تشير معاملات تحميل بُعد المتطلبات الفنية على الفقرات التي تقيسه والممثلة له درجة اتساق عالية (أكبر من 0.40) لمستويات استجابة المستجيبين بحسب مقياس أداة الدراسة على جميع فقرات البُعد.

ويتضح من الفقرة المرجعية (c8) أن هناك التزاما من جانب البنوك بوجود تدابير آمنة وموثوقة للنسخ الاحتياطي التلقائي للبيانات والتصميمات الرئيسية، وهذا يتم تأكيده من خلال قيمة التقدير المرجح المحددة بـ (4.13)، وهذا يعبر عن التزام البنوك الثابت بضمان استمرارية الأعمال وصون المعلومات الأساسية، ومن ناحية أخرى، تشير الفقرة المرجعية (c9) التي حصلت على قيمة تقدير مرجح قدرها (3.94) إلى أن استخدام الشبكات الافتراضية مثل VLANs قد يحتاج إلى تعزيز وتطوير لضمان تحقيق أمان شبكي أعلى.

من جانب آخر، تم التعرف إلى نقص في الفقرة المرجعية (c7)، التي أُسندت لها قيمة تقدير مرجح بـ (3.91)، ما يوضح وجود ضرورة لزيادة جهود البنوك في إجراء تقييمات الضعف واختبارات الاختراق وتقييم الفجوات الأمنية يمكن ملاحظة الاختلاف بين الفقرتين المرجعيتين (c8) (4.13)و (c9) (3.94)، وهذا الاختلاف يُبرز التميز النسبي في تقنيات النسخ الاحتياطي التلقائي عند المقارنة مع تقنيات الشبكات الافتراضية، مما يشير إلى ضرورة تقييم وتطوير استراتيجيات الأمان المتعلقة بتقنية الشبكات في البنوك اليمنية وتطويرها.

3.1.2.4 نتائج تحليل فقرات البُعد الثالث (الامتثال للأطر والمعايير الدولية):

يتناول هذا الجزء المتوسطات المرجحة، والأهمية النسبية، ومعاملات الاختلاف، ومعنوية حسن المطابقة لإجابات أفراد العيّنة لمستوى لامتثال للأطر والمعايير الدولية للأمن السيبراني في حماية نظم المعلومات في البنوك اليمنية، الجدول (4-10) يوضح ذلك.

الجدول: 4-10

نتائج تحليل فقرات بعد الامتثال للأطر والمعايير الدولية

الرمز	الفقرة	الوسط المرجح	الأهمية النسبية	معامل الاختلاف	معنوية حسن المطابقة	معامل التحميل
v1	يطبق البنك معايير الأمن السيبراني الدولية كمعيار ISF وصناعة بطاقات الدفع ومعيار أمان البيانات PCI/DSNot	3.84	% 77	% 25	0.000	0.790
v2	يعمل البنك على مواءمة ممارسات الأمن السيبراني مع المعايير المعترف بها دوليًا.	3.89	% 78	% 24	0.000	0.871
v3	يقوم البنك بمراجعة وتحديث سياسات الأمن السيبراني الخاصة به بانتظام لتلبية المعايير الدولية.	3.86	% 77	% 27	0.000	0.873
v4	يخصص البنك موارد لضمان الامتثال لمعايير الأمن السيبراني الدولية.	3.84	% 77	% 26	0.000	0.879
v5	يستخدم البنك الأطر والمعايير الدولية لعمليات تقييم المخاطر وإدارتها.	3.94	% 79	% 22	0.000	0.869
v6	يتلقى موظفو البنك تدريبًا على أطر ومعايير الأمن السيبراني الدولية.	3.67	% 73	% 30	0.000	0.771
v7	يشارك البنك في منتديات ومؤتمرات الأمن السيبراني الدولية للبقاء على اطلاع بأفضل الممارسات.	3.56	% 71	% 33	0.000	0.792

v8	يقوم البنك بقياس ممارسات الأمن السيبراني الخاصة به مقابل نظرائه في الصناعة والمعايير الدولية.	3.62	% 72	% 32	0.000	0.822
v9	يستخدم البنك شهادات معترف بها دوليًا للتحقق من قدرات الأمن السيبراني الخاصة به.	3.72	% 74	% 29	0.000	0.842
v10	يسعى البنك إلى تطوير استراتيجياته الخاصة لضمان أمن المؤسسة بما لا يتعارض مع المعايير الدولية.	3.85	% 77	% 29	0.000	0.862
	الامتثال للأطر والمعايير الدولية	**3.78**	**76%**	**22%**		

يبين الجدول (4–10) توصيف الاستجابة لأفراد عينة الدراسة بحسب مقياس مستوى الموافقة بناء على المتوسط الحسابي المرجح بتكرارات درجات المقياس وأهميته النسبية نسبة لأعلى درجة فيه، الذي يبين درجة موافقة عالية لبُعد الامتثال للأطر والمعايير الدولية كأحد أبعاد متطلبات الأمن السيبراني بمتوسط حسابي (3.78) وأهمية نسبية (76%) ومعامل اختلاف (22%).

وبناء على ترتيب الفقرات بحسب الأهمية النسبية جاءت الفقرة (v5) والتي تنص على: "يستخدم البنك الأطر والمعايير الدولية لعمليات تقييم المخاطر وإدارتها..." بأهمية نسبية (79%) ومعامل اختلاف (22%) في المرتبة الأولى، وجاءت الفقرة (v7) التي تنص على: "يشارك البنك في منتديات ومؤتمرات الأمن السيبراني الدولية للبقاء على اطلاع بأفضل الممارسات..." في المرتبة الأخيرة بأهمية نسبية (71%) ومعامل اختلاف (33%) وتشير الدلالة الاحصائية لاختبار مربع كاي لحسن المطابقة إلى معنوية آراء المستجيبين بحسب تكرارات مستويات الموافقة على جميع الفقرات الممثلة للامتثال للأطر والمعايير الدولية عند مستوى دلالة 0.01، كما تشير معاملات تحميل بُعد الامتثال للأطر والمعايير الدولية على الفقرات التي تقيسه والممثلة له درجة

اتساق عالية (أكبر من 0.40) لمستويات استجابة المستجيبين بحسب مقياس أداة الدراسة على جميع فقرات البُعد.

تظهر النتائج كما في الفقرة المرجعية (v1) أن هناك التزاماً واضحاً من جانب البنوك بتطبيق المعايير الدولية للأمن السيبراني مثل معيار (ISF) المعروف أيضًا بمعيار "المنتدى الدولي للأمن المعلوماتي (Information Security Forum's Standard of Good Practice for " Information Security وصناعة بطاقات الدفع ومعيار أمان البيانات(PCI/DSS) هذا يُؤكد على التزام البنوك المبحوثة بالحفاظ على معلوماته وتطبيق أفضل الممارسات، وهو ما يتجلى من خلال قيمة التقدير المرجح المحددة بـ (3.84). ومن ناحية أخرى، تظل الفقرة المرجعية (v7)، التي حصلت على قيمة تقدير مرجح قدرها (3.56)، تُشير إلى أن هناك فرصة لتعزيز مشاركة البنوك اليمنية في المنتديات والمؤتمرات الدولية المتعلقة بالأمن السيبراني.

وتظهر النتائج وجود ضعف معين في الفقرة المرجعي(v6)، حيث أُسندت لها قيمة تقدير مرجح بـ (3.67). وتدل على الحاجة الملحة لتقوية برامج تدريب الموظفين على أطر الأمن السيبراني ومعاييره الدولية لضمان رفع مستوى وعيهم ومهاراتهم، وعلى صعيد تقييم الفجوات الموجودة، تبرز الفرق بين الفقرتين المرجعيتين (3.84) (v1) و(v7) (3.56) هذا الاختلاف يعكس التميز في تطبيق المعايير الدولية للأمن السيبراني بالمقارنة مع مشاركة البنوك اليمنية في المنتديات الدولية، ما يشير إلى أهمية إعادة التقييم وتعزيز جهود البنك في هذا الاتجاه.

4.1.2.4 نتائج تحليل فقرات البُعد الرابع (تدابير الأمن المادي):

يتناول هذا الجزء المتوسطات المرجحة، والأهمية النسبية، ومعاملات الاختلاف، ومعنوية حسن المطابقة لإجابات أفراد العينة لمستوى توافر تدابير الأمن المادي للأمن السيبراني في حماية

نظم المعلومات في البنوك اليمنية، الجدول (4-11) يوضح ذلك.

الجدول: 4-11

نتائج تحليل فقرات بعد تدابير الأمن المادي

الرمز	الفقرة	الوسط المرجح	الأهمية النسبية	معامل الاختلاف	معنوية حسن المطابقة	معامل التحميل
a1	يقوم البنك بتطبيق أنظمة التحكم في الوصول لتقييد الدخول غير المصرح به إلى الأنظمة الأكثر حساسية.	4.17	% 83	% 22	0.000	0.803
a2	ينشئ البنك غرف خوادم مؤمنة تحتوي على ضوابط بيئية لحماية أنظمته.	4.06	%81	% 23	0.000	0.783
a3	لدى البنك نظام متقدم لإدارة ومتابعة الزوار الخارجيين	3.85	% 77	% 28	0.000	0.851
a4	يقوم البنك بإجراء عمليات تدقيق أمنية منتظمة لتقييم فعالية تدابير الأمن المادي الخاصة به.	3.90	% 78	% 26	0.000	0.867
a5	يتلقى موظفو البنك دورات تدريبية دورية متكررة حول أهمية تعزيز الأمن المادي والحفاظ عليه.	3.68	% 74	% 31	0.000	0.722
a6	لدى البنك سياسة واضحة للتعامل مع المستندات المادية الحساسة والتخلص منها.	3.86	% 77	% 28	0.000	0.870
a7	يمتلك البنك خطة طوارئ لحوادث الأمن المادي مثل السرقة أو التخريب.	3.98	% 80	% 27	0.000	0.859

a8	تضـــع إدارة البنـك تـدابير الأمن المادي جزءًا لا يتجزأ من استراتيجية الأمن السيبراني الخاصة بها.	3.86	% 77	% 26	0.000	0.869
	تدابير الأمن المادي	**3.92**	**% 78**	**%21**		

يبين الجدول (4–11) توصيف الاستجابة لأفراد عينة الدراسة بحسب مقياس مستوى الموافقة بناء على المتوسط الحسابي المرجح بتكرارات درجات المقياس وأهميته النسبية نسبة لأعلى درجة فيه والذي يبين درجة موافقة عالية لبُعد تدابير الأمن المادي كأحد أبعاد متطلبات الأمن السيبراني بمتوسط حسابي (3.92) وأهمية نسبية (78%) ومعامل اختلاف (21%).

وبناء على ترتيب الفقرات بحسب الاهمية النسبية جاءت الفقرة (a1) التي تنص على: "يقوم البنك بتطبيق أنظمة التحكم في الوصول لتقييد الدخول غير المصرح به إلى الأنظمة الأكثر حساسية...." بأهمية نسبية (83%) ومعامل اختلاف (22%) في المرتبة الأولى، وجاءت الفقرة (a5) والتي تنص على: "يتلقى موظفو البنك دورات تدريبية دورية متكررة حول أهمية تعزيز الأمن المادي والحفاظ عليه...." في المرتبة الأخيرة بأهمية نسبية (74 %) ومعامل اختلاف (31%)، وتشير الدلالة الاحصائية لاختبار مربع كأي لحسن المطابقة إلى معنوية آراء المستجيبين بحسب تكرارات مستويات الموافقة على جميع الفقرات الممثلة لتدابير الأمن المادي عند مستوى دلالة 0.01، كما تشير معاملات تحميل بُعد تدابير الأمن المادي على الفقرات التي تقيسه والممثلة له درجة اتساق عالية (أكبر من 0.40) لمستويات استجابة المستجيبين بحسب مقياس أداة الدراسة على جميع فقرات البُعد.

وعليه يتضح من الفقرة المرجعية (a1) أن هذه البنوك تضع في مقدمة أولوياتها تطبيق أنظمة التحكم في الوصول للحد من أي دخول غير مصرح به إلى الأنظمة الحساسة. وهذا يُعزز من الثقة في ممارسات البنوك الأمنية المادية، وهو ما يتجلى من خلال قيمة التقدير المرجح المحددة بـ (4.17). من جانب آخر، تُظهر الفقرة المرجعي(a7)، التي حصلت على قيمة تقدير مرجح قدرها (3.68)، أن هناك حاجة ملحة لزيادة جهود التوعية والتدريب الموجهة للموظفين حول أهمية تعزيز الأمن المادي والحفاظ عليه.

وفي السياق ذاته، نلاحظ أن الفقرة المرجعية (a6) تُسلط الضوء على الحاجة لتطوير نظام متقدم لإدارة ومتابعة الزوار الخارجيين، حيث حصلت على تقدير مرجح بلغ (3.85). هذه النتيجة تُشير إلى أن هناك مجالًا لتحسين وتقوية الإجراءات المتعلقة بإدارة الزوار، على صعيد تقييم الفجوات، يظهر اختلاف واضح بين الفقرتين المرجعيتين (4.17) (a1) و (3.68) (a7)هذه الفجوة تعكس التميز في تطبيق أنظمة التحكم في الوصول مقابل الحاجة الملحة لزيادة التوعية والتدريب الموجه لموظفي البنوك اليمنية في مجال الأمان المادي.

2.2.4 نتائج تحليل فقرات المتغيّر التابع (حماية نظم المعلومات):

يوضح هذا الجزء نتائج تحليل بعد المتغيّر التابع: حماية نظم المعلومات، من حيث المتوسطات المرجحة، والأهمية النسبية، ومعاملات الاختلاف، ومعنوية حسن المطابقة لإجابات أفراد العيّنة لمستوى حماية سرية نظم المعلومات في البنوك اليمنية، الجدول (4-12) يوضح ذلك على النحو الآتي:

الجدول: 4-12

نتائج تحليل فقرات المتغير التابع: حماية سرية نظم المعلومات

الرمز	الفقرة	الوسط المرجح	الأهمية النسبية	معامل الاختلاف	معنوية حسن المطابقة	معامل التحميل
y1	يقوم البنك بتنفيذ تدابير لعمليات التحقق والتدقيق والمراجعة الدورية للبيانات، وتحديثها عند الحاجة.	4.10	% 82	% 20	0.000	0.802
y2	يمتلك البنك سياسة أمنية لاكتشاف الأخطاء التي قد تظهر في البيانات ويتخذ إجراءات فورية لتصحيحها.	4.06	% 81	% 21	0.000	0.865
y3	يطبق البنك ضوابط فعالة للتأكد من أن البيانات المسجلة في النظام دقيقة وحديثة وكاملة.	4.02	% 80	% 24	0.000	0.820
y4	يتخذ البنك تدابير أمنية لضمان استمرارية توافر أنظمة المعلومات الخاصة به	4.06	% 81	% 23	0.000	0.862
y5	يجري البنك المراقبة الدورية للأنظمة استباقياً بحثًا عن المشكلات المحتملة للحفاظ على التوافرية.	3.87	% 77	% 27	0.000	0.834
y6	لدى البنك خطة تعافي من الكوارث في حالة حدوثها واستعادة توافر النظام في حالة وقوع حادث.	3.94	% 79	% 25	0.000	0.807
y7	يمتلك البنك نظام إدارة الطاقة الاحتياطية والتمويل الكافي لدعم استمرارية وتوافريه أنظمة المعلومات.	3.97	% 79	%24	0.000	0.816
y8	يخصص البنك موارد مالية وتقنية وبشرية لتطوير وتحسين بنيته الاساسية لتكنولوجيا المعلومات.	3.90	% 78	% 28	0.000	0.852
y9	يفرض البنك شروطا صارمة على المستخدمين لإنشاء كلمات مرور قوية وفريدة	4.06	% 81	% 25	0.000	0.828
y10	يستخدم البنك المصادقة متعددة العوامل (Multi-Factor Authentication)	3.85	% 77	% 29	0.000	0.756

y11	يقوم البنك بمراجعة وتحديث آليات المصادقة الخاصة به بانتظام لضمان فعاليتها.	3.92	% 78	% 26	0.000	0.849
y12	يقوم البنك بفرض تغيير كلمات المرور بشكل دوري لجميع المستخدمين.	4.18	% 84	% 23	0.000	0.749
y13	يقوم البنك بإجراء عمليات اختبار اختراق لبيئات وسيناريوهات محددة للتأكد من قوة آليات المصادقة لديه.	3.88	% 78	%27	0.000	0.808
y14	يتخذ البنك نظام تحكم في الوصول قائم على الأدوار كنظام (Role-Based Access Control)	3.86	% 77	% 25	0.000	0.800
y15	يتخذ البنك إجراءات لإلغاء صلاحيات الوصول الخاصة بالموظفين	4.14	% 83	% 24	0.000	0.797
y16	يحدد البنك سياسات واضحة ومزمنة لتخويل وإلغاء تخويل المستخدمين للوصول إلى أنظمة المعلومات والبيانات.	4.17	% 83	% 22	0.000	0.818
	حماية سرية نظم المعلومات	**4.00**	**% 80**	**% 19**		

يبين الجدول (4-12) توصيف الاستجابة لأفراد عينة الدراسة بحسب مقياس مستوى الموافقة بناء على المتوسط الحسابي المرجح بتكرارات درجات المقياس وأهميته النسبية نسبة لأعلى درجة في، الذي يبين درجة موافقة عالية لمحور حماية سرية نظم المعلومات بمتوسط حسابي (4.00) وأهمية نسبية (80%) ومعامل اختلاف (19%).

وبناء على ترتيب الفقرات بحسب الأهمية النسبية جاءت الفقرة (y12)، التي تنص على: "يقوم البنك بفرض تغيير كلمات المرور بشكل دوري لجميع المستخدمين....." بأهمية نسبية (84%) ومعامل اختلاف (23%) في المرتبة الأولى، وجاءت الفقرات (y5,y10,y14)، التي تنص على: "يجري البنك المراقبة الدورية للأنظمة استباقياً بحثًا عن المشكلات المحتملة للحفاظ

على التوافرية، يستخدم البنك المصادقة متعددة العوامل (Multi-Factor Authentication))، ويتخذ البنك نظام تحكم في الوصول قائم على الأدوار كنظام (Role-Based Access Control)" في المرتبة الأخيرة بأهمية نسبية (77%) لكل ومعامل اختلاف (27%,29%,25%) على التوالي.

وتشير الدلالة الإحصائية لاختبار مربع كاي لحسن المطابقة إلى معنوية آراء المستجيبين بحسب تكرارات مستويات الموافقة على جميع الفقرات الممثلة لحماية سرية نظم المعلومات عند مستوى دلالة 0.01، كما تشير معاملات تحميل محور حماية سرية نظم المعلومات على الفقرات التي تقيسه والممثلة له درجة اتساق عالية (أكبر من 0.40) لمستويات استجابة المستجيبين بحسب مقياس أداة الدراسة على جميع فقرات البُعد.

وبناء على ما سبق، يتضح من الفقرة المرجعية (y12) أن هذه البنوك تقوم بتطبيق تغيير كلمات المرور بشكل دوري لجميع المستخدمين، ما يُسهم في تعزيز الأمان الرقمي للأنظمة. هذا الالتزام يُظهر الحرص الدائم للبنوك اليمنية على أمان المعلومات، وهو ما يُؤكد من خلال قيمة التقدير المرجح المحددة بـ (4.18). من جهة أخرى، تشير الفقرة المرجعية(y5)، التي حصلت على تقدير مرجح قدره (3.87)، إلا أن هناك حاجة لزيادة الجهود في المراقبة الاستباقية للأنظمة للحفاظ على توافريتها.

كما تظهِر النتائج ضعفاً في الفقرة المرجعية (y10) حول استخدام البنوك اليمنية المستهدفة في الدراسة للمصادقة متعددة العوامل، حيث أُسندت لها قيمة تقدير مرجح بلغت (3.85) وهذا يُشير إلى ضرورة تطوير وتعزيز استخدام ممارسات المصادقة متعددة العوامل لضمان أعلى مستويات الأمان. وعلى صعيد تقييم الفجوات، تبرز فجوة بين الفقرتين المرجعيتين(4.18) (y1) ،

(3.85) (y10)تعكس هذه الفجوة التركيز الكبير على تحسين تغيير كلمات المرور بشكل دوري، مقابل الحاجة الملحة لتطوير استخدام المصادقة متعددة العوامل.

3.4 اختبار فرضيات الدراسة:

يتناول هذا الجزء اختبار الفرضيات ومعالجتها إحصائياً باستخدام النموذج البنائي الرئيسي لتوصيف العلاقات السببية بين ابعاد المتغير المستقل (متطلبات الأمن السيبراني) والمتغير التابع (حماية سرية أنظمة المعلومات).

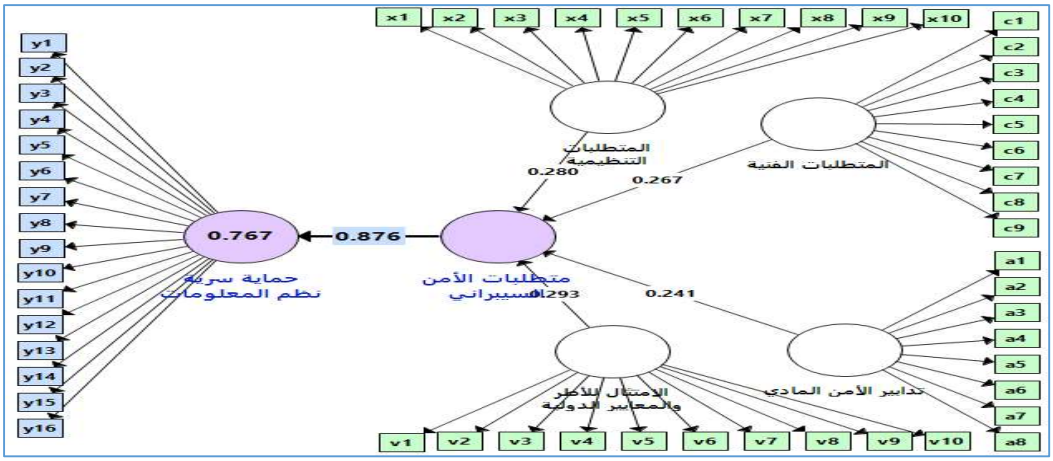
1.3.4 اختبار الفرضية الرئيسة الأولى والفرضيات الفرعية المنبثقة منها:

اختبار الفرضية الرئيسة الأولى:

وتنص على أنه " لا يوجد أثر لمستويات توافر متطلبات الأمن السيبراني على مستويات حماية سرية أنظمة المعلومات في البنوك اليمنية".

الشكل: 8.4

النموذج البنائي الرئيسي لتوصيف العلاقات السببية بين ابعاد المتغير المستقل (متطلبات الأمن السيبراني) والمتغير التابع (حماية سرية أنظمة المعلومات)



الجدول: 4-13

مؤشرات مطابقة نموذج تأثير				
المؤشر	Q^2	GOF	SRMR	rms Theta
مدى المؤشر	أكبر من الصفر	0 - 1	0 - 1	0 - 1
قيمة المؤشر	0.469	0.695	0.070	0.139
النتيجة	مقبولة	مقبولة	مقبولة	مقبولة

مؤشرات العلاقة التأثيرية: متطلبات الأمن السيبراني -> حماية سرية أنظمة المعلومات						
المؤشرات	معامل المسار	الخطأ المعياري	قيمة اختبار T	المعنوية Sig	معامل التفسير R^2	معامل حجم الأثر F^2
قيمة المؤشر	0.876	0.016	59.089	0.000	0.767	3.284
النتيجة	توجد علاقة تأثير دالة احصائياً عند مستوى دلالة 0.05					

تدل مؤشرات المطابقة الموضحة في الجدول (4-13) والشكل (4.8) لتحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الرئيسية الأولى أنها حققت مستويات القبول المطلوبة، حيث كانت قيم جميع المؤشرات ضمن المدى المقبول، أي أن هناك مستوى تطابق مقبولاً للنموذج المفترض مع البيانات الميدانية، كما نلاحظ أن معامل المسار بين محور (متطلبات الأمن السيبراني) متغيراً مستقلاً ومحور (حماية سرية أنظمة المعلومات) متغيراً تابعاً إيجابي وعالٍ من حيث القوة (0.876)، بينما حجم الأثر الذي يخلفه المتغير المستقل على المتغير التابع يُعد **عاليا بدرجة كبيره إلى حد ما** (3.284) وتشير قيمة معامل التحديد إلى أن التغير في المتغير المستقل بحسب وحدة القياس المعتمدة لمقياس أداة الدراسة يحدد ما نسبته (77%) تقريبا من التغير في المتغير التابع بحسب وحدة القياس نفسها، كما أن علاقة الأثر بين المتغيرين المستقل والتابع ذات دلالة إحصائية عند مستوى (0.05).

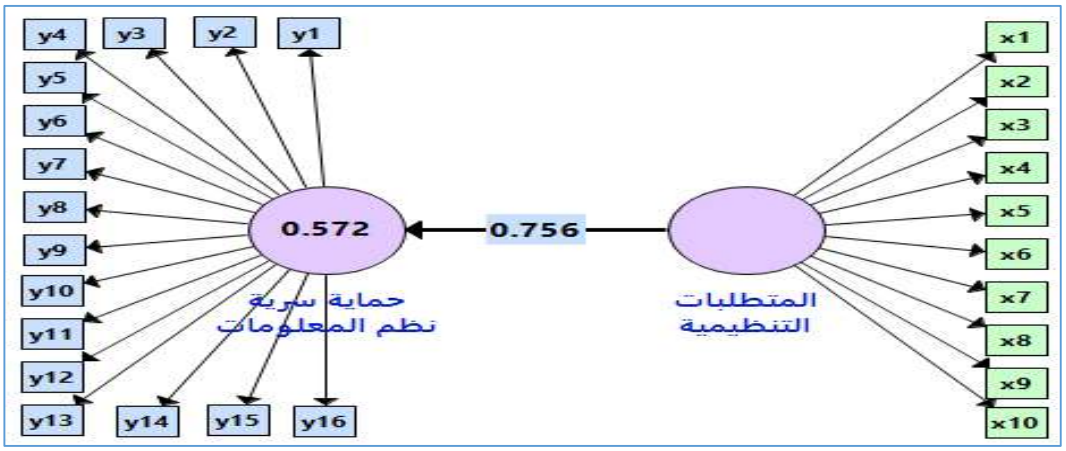
وهذا يعني رفض الفرضية الصفرية الرئيسية الأولى للدراسة التي تنص على أنه: "لا يوجد أثر لمستويات توافر متطلبات الأمن السيبراني في مستويات حماية أنظمة المعلومات في البنوك اليمنية بحسب اراء العاملين فيها" وقبول الفرضية البديلة التي تنص على: "يوجد أثر لمستويات توافر متطلبات الأمن السيبراني في مستويات حماية نظم المعلومات في البنوك اليمنية".

اختبار الفرضية الفرعية الأولى المنبثقة من الفرضية الرئيسية الأولى:

وتنص على أنه: "لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني التنظيمية في مستوى حماية سرية أنظمة المعلومات في البنوك اليمنية".

الشكل: 9.4

النموذج البنائي الرئيسي لتوصيف العلاقات السببية بين بعد (المتطلبات التنظيمية) كمتغير مستقل والمتغير التابع (حماية سرية أنظمة المعلومات)



الجدول: 4-14

تحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الأولى

مؤشرات مطابقة نموذج تأثير				
المؤشر	Q^2	GOF	SRMR	rms Theta

مدى المؤشر	أكبر من الصفر	0 - 1	0 - 1	0 - 1
قيمة المؤشر	0.354	0.613	0.051	0.123
النتيجة	مقبولة	مقبولة	مقبولة	مقبولة

مؤشرات العلاقة التأثيرية: المتطلبات التنظيمية -> حماية سرية أنظمة المعلومات

المؤشرات	معامل المسار	الخطأ المعياري	قيمة اختبار T	المعنوية Sig	معامل التفسير R^2	معامل حجم الأثر F^2
قيمة المؤشر	0.756	0.032	23.890	0.000	0.572	1.336
النتيجة	توجد علاقة تأثير دالة احصائياً عند مستوى دلالة 0.05					

تدل مؤشرات المطابقة الموضحة في الجدول (4-14) والشكل (9.4) لتحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الأولى إنها حققت مستويات القبول المطلوبة، حيث كانت قيم جميع المؤشرات ضمن المدى المقبول، أي أن هناك مستوى تطابق مقبول للنموذج المفترض مع البيانات الميدانية، كما نلاحظ إن معامل المسار بين بعد (المتطلبات التنظيمية) متغيراً مستقلاً ومحور (حماية سرية أنظمة المعلومات) متغيراً تابعاً **إيجابي ومتوسط** من حيث القوة (0.756) ، بينما حجم الأثر الذي يخلفه المتغير المستقل على المتغير التابع يُعد **عاليا بدرجة كبيره** إلى حد ما (1.336). وتشير قيمة معامل التحديد إلى أن التغير في المتغير المستقل بحسب وحدة القياس المعتمدة لمقياس أداة الدراسة يحدد ما نسبته (57%) تقريبا من التغير في المتغير التابع بحسب وحدة القياس نفسها، كما أن علاقة الأثر بين المتغيرين المستقل والتابع ذات دلالة إحصائية عند مستوى(0.05).

وهذا يعني رفض الفرضية الفرعية الأولى التي تنص على أنه "لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني التنظيمية في مستوى حماية سرية أنظمة المعلومات في البنوك اليمنية بحسب اراء العاملين فيها" وقبول الفرضية الفرعية الأولى البديلة التي تنص على أنه: "يوجد أثر

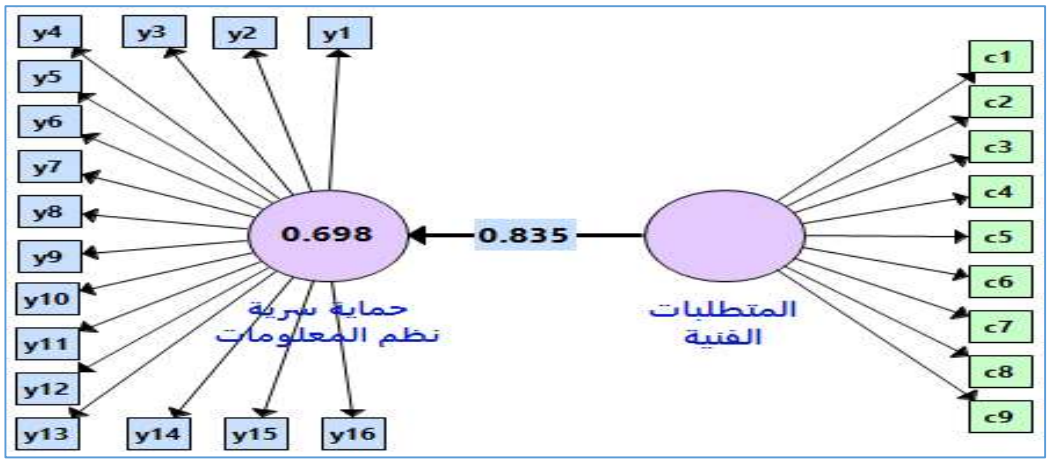
لمستويات توافر المتطلبات التنظيمية للأمن السيبراني في مستويات حماية نظم المعلومات في البنوك اليمنية".

اختبار الفرضية الفرعية الثاني المنبثقة من الفرضية الرئيسية الأولى:

وتنص على: "لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني الفنية في مستوى حماية سرية أنظمة المعلومات في البنوك اليمنية".

الشكل: 10.4

النموذج البنائي الرئيسي لتوصيف العلاقات السببية بين بعد (المتطلبات الفنية) كمتغير مستقل والمتغير التابع (حماية سرية أنظمة المعلومات)



الجدول: 4 – 15

تحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الثانية

مؤشرات مطابقة نموذج تأثير				
المؤشر	Q^2	GOF	SRMR	rms Theta
مدى المؤشر	أكبر من الصفر	1 - 0	1 - 0	1 - 0
قيمة المؤشر	0.427	0.677	0.048	0.125
النتيجة	مقبولة	مقبولة	مقبولة	مقبولة

مؤشرات العلاقة التأثيرية: المتطلبات الفنية -> حماية سرية أنظمة المعلومات						
المؤشرات	معامل المسار	الخطأ المعياري	قيمة اختبار T	المعنوية Sig	معامل التفسير R^2	معامل حجم الأثر F^2
قيمة المؤشر	0.835	0.018	47.672	0.000	0.698	2.308
النتيجة	توجد علاقة تأثير دالة احصائياً عند مستوى دلالة 0.05					

تدل مؤشرات المطابقة الموضحة في الجدول (4-15) والشكل (10.4) لتحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الثانية أنها حققت مستويات القبول المطلوبة، حيث كانت قيم جميع المؤشرات ضمن المدى المقبول. أي أن هناك مستوى تطابق مقبول للنموذج المفترض مع البيانات الميدانية، كما نلاحظ أن معامل المسار بين بعد (المتطلبات الفنية) متغيراً مستقلاً ومحور (حماية سرية أنظمة المعلومات) متغيراً تابعاً **إيجابي وعالي من حيث القوة** (0.835)، بينما حجم الأثر الذي يخلفه المتغير المستقل على المتغير التابع يُعد **عاليا بدرجة كبيره** إلى حد ما (2.308)، وتشير قيمة معامل التحديد إلى أن التغير في المتغير المستقل بحسب وحدة القياس المعتمدة لمقياس أداة الدراسة يحدد ما نسبته (70%) تقريبا من التغير في المتغير التابع بحسب وحدة القياس نفسها، كما إن علاقة الأثر بين المتغيرين المستقل والتابع ذات دلالة إحصائية عند مستوى (0.05).

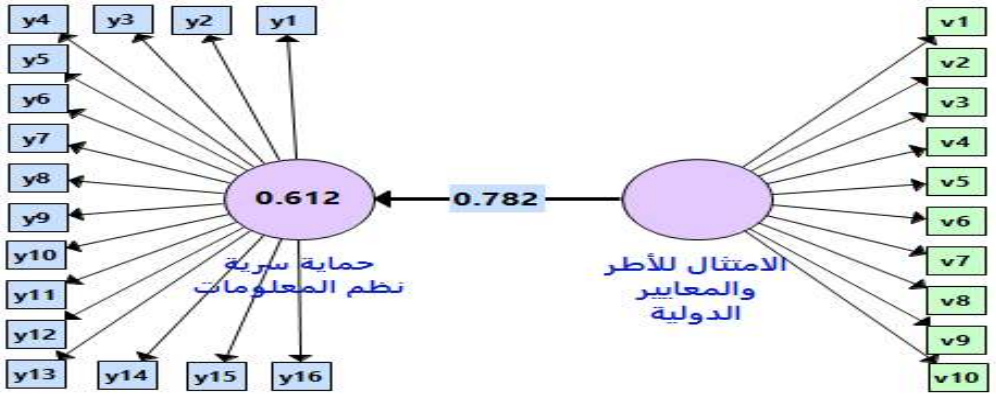
وهذا يعني رفض الفرضية الفرعية الثانية التي تنص على أنه:" لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني الفنية في مستوى حماية سرية أنظمة المعلومات في البنوك اليمنية بحسب اراء العاملين فيها"، وقبول الفرضية الفرعية الثانية البديلة التي تنص على "يوجد أثر لمستويات توافر المتطلبات الفنية للأمن السيبراني في مستويات حماية نظم المعلومات في البنوك اليمنية".

اختبار الفرضية الفرعية الثالثة المنبثقة من الفرضية الرئيسية الأولى:

وتنص على أنه "لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني (الامتثال للأطر والمعايير الدولية) في مستوى حماية سرية أنظمة المعلومات في البنوك اليمني".

الشكل: 11.4

النموذج البنائي الرئيسي لتوصيف العلاقات السببية بين بعد (الامتثال للأطر والمعايير الدولية) كمتغير مستقل والمتغير التابع (حماية سرية أنظمة المعلومات)



الجدول: 4-16

تحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الثالثة

مؤشرات مطابقة نموذج تأثير				
المؤشر	Q^2	GOF	SRMR	rms Theta
مدى المؤشر	أكبر من الصفر	0 - 1	0 - 1	0 - 1
قيمة المؤشر	0.372	0.683	0.048	0.125
النتيجة	مقبولة	مقبولة	مقبولة	مقبولة

مؤشرات العلاقة التأثيرية: الامتثال للأطر والمعايير الدولية -> حماية سرية أنظمة المعلومات					
المؤشرات	معامل المسار	الخطأ المعياري	قيمة اختبار T	المعنوية Sig	معامل التفسير R^2	معامل حجم الأثر F^2
قيمة المؤشر	0.782	0.033	23.689	0.000	0.612	1.574
النتيجة	توجد علاقة تأثير دالة احصائياً عند مستوى دلالة 0.05					

تدل مؤشرات المطابقة الموضحة في الجدول (4-16) لتحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الثالثة أنها حققت مستويات القبول المطلوبة، حيث كانت قيم جميع المؤشرات ضمن المدى المقبول. أي إن هناك مستوى تطابق مقبول للنموذج المفترض مع البيانات الميدانية، كما نلاحظ أن معامل المسار بين بعد (الامتثال للأطر والمعايير الدولية) متغيراً مستقلاً ومحور (حماية سرية أنظمة المعلومات) متغيراً **تابعاً إيجابي ومتوسط** من حيث القوة (0.782). بينما حجم الأثر الذي يخلفه المتغير المستقل على المتغير التابع يعتبر **عاليا بدرجة كبيره إلى حد ما** (1.574)، وتشير قيمة معامل التحديد إلى أن التغير في المتغير المستقل بحسب وحدة القياس المعتمدة لمقياس أداة الدراسة يحدد ما نسبته (61%) تقريبا من التغير في المتغير التابع بحسب وحدة القياس نفسها، كما أن علاقة الأثر بين المتغيرين المستقل والتابع ذات دلالة إحصائية عند مستوى دلالة (0.05).

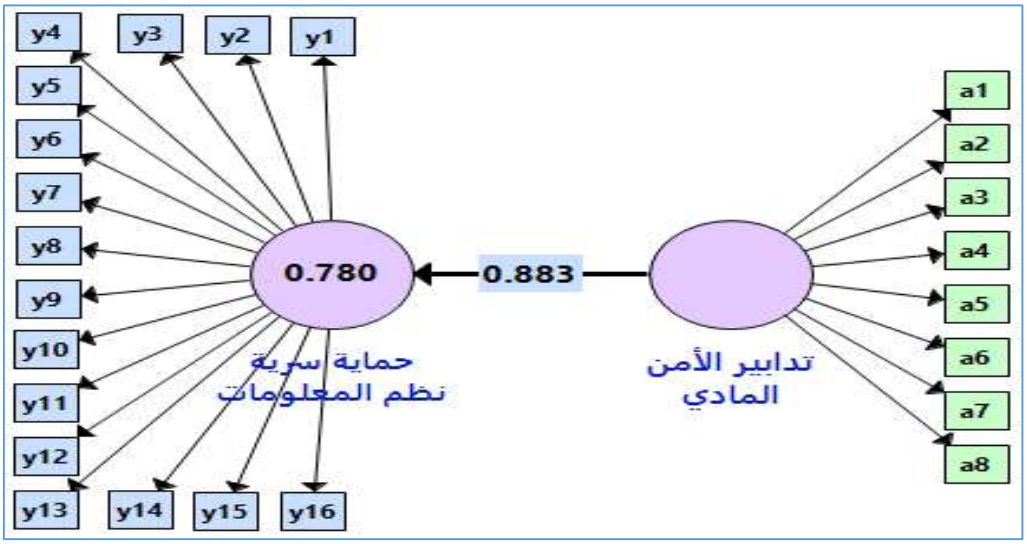
وهذا يعني رفض الفرضية الفرعية الثالثة التي تنص على أنه:" لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني (الامتثال للأطر والمعايير الدولية) في مستوى حماية سرية أنظمة المعلومات في البنوك اليمني بحسب أراء العاملين فيها" وتقبل الفرضية الفرعية الثالثة البديلة التي تنص على "يوجد أثر لمستويات توافر المتطلبات (الامتثال للأطر والمعايير الدولية) للأمن السيبراني على مستويات حماية نظم المعلومات في البنوك اليمنية".

اختبار الفرضية الفرعية الرابعة المنبثقة من الفرضية الرئيسية الأولى:

وتنص على أنه: "لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني (تدابير الأمن المادي) في مستوى حماية سرية أنظمة المعلومات في البنوك اليمنية".

الشكل: 12.4

النموذج البنائي الرئيسي لتوصيف العلاقات السببية بين بعد (تدابير الأمن المادي) كمتغير مستقل والمتغير التابع (حماية سرية أنظمة المعلومات)



الجدول: 4-17

نتائج تحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الرابعة

مؤشرات مطابقة نموذج تأثير				
المؤشر	Q^2	GOF	SRMR	rms Theta
مدى المؤشر	أكبر من الصفر	1 - 0	1 - 0	1 - 0
قيمة المؤشر	0.478	0.717	0.052	0.134
النتيجة	مقبولة	مقبولة	مقبولة	مقبولة

مؤشرات العلاقة التأثيرية: تدابير الأمن المادي -> حماية سرية أنظمة المعلومات					
المؤشرات	معامل المسار	الخطأ المعياري	قيمة اختبار T	المعنوية Sig	معامل التفسير R^2	معامل حجم الأثر F^2
قيمة المؤشر	0.883	0.017	52.662	0.000	0.780	3.545
النتيجة	توجد علاقة تأثير دالة احصائياً عند مستوى دلالة 0.05					

تدل مؤشرات المطابقة الموضحة في الجدول (4-17) لتحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الفرعية الرابعة أنها حققت مستويات القبول المطلوبة، حيث كانت قيم جميع المؤشرات ضمن المدى المقبول. أي أن هناك مستوى تطابق مقبول للنموذج المفترض مع البيانات الميدانية، كما نلاحظ أن معامل المسار بين بعد (تدابير الأمن المادي) متغيراً مستقلاً ومحور (حماية سرية أنظمة المعلومات) متغيراً تابعاً إيجابي وعالي من حيث القوة (0.883). بينما حجم الأثر الذي يخلفه المتغير المستقل على المتغير التابع يُعد عاليا بدرجة كبيرة إلى حد ما (3.545)، وتشير قيمة معامل التحديد إلى أن التغير في المتغير المستقل بحسب وحدة القياس المعتمدة لمقياس أداة الدراسة يحدد ما نسبته 78 % تقريبا من التغير في المتغير التابع بحسب نفس وحدة القياس. كما إن علاقة الأثر بين المتغيرين المستقل والتابع ذات دلالة إحصائية عند مستوى دلالة 0.05.

وهذا يعني رفض الفرضية الفرعية الرابعة التي تنص على أنه: "لا يوجد أثر لمستوى توافر متطلبات الأمن السيبراني (تدابير الأمن المادي) في مستوى حماية سرية أنظمة المعلومات في البنوك اليمنية بحسب اراء العاملين فيها"، وتقبل الفرضية الفرعية الرابعة البديلة التي تنص على "يوجد أثر لمستويات توافر المتطلبات المادية للأمن السيبراني في مستويات حماية نظم المعلومات في البنوك اليمنية".

2.3.4 اختبار الفرضية الرئيسية الثانية:

وتنص على أنه:" لا يوجد فروق جوهرية بين متوسطات استجابات أفراد العينة حول مستويات توافر متطلبات الأمن السيبراني وأثرها في حماية نظم المعلومات تعزى إلى متغيراتهم الديموغرافية".

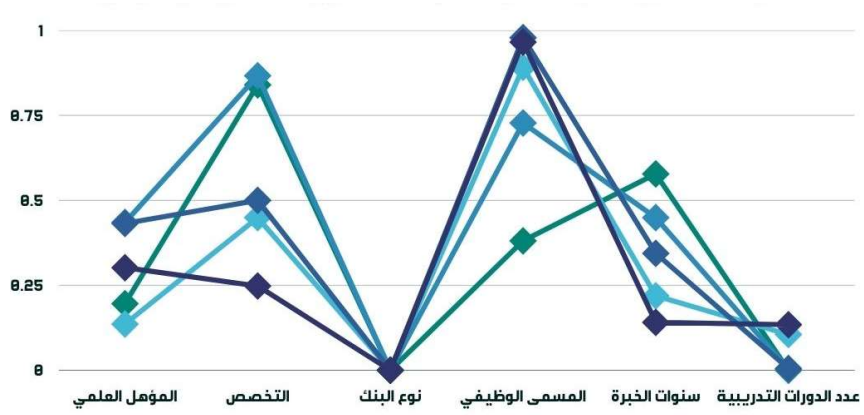
الجدول: 4-18

تحليل التباين اللامعلمي لاستجابات أفراد العينة اتجاه محاور الدراسة بحسب المتغيرات الديموغرافية

Cc	المتطلبات التنظيمية	المتطلبات الفنية	الامتثال للأطر والمعايير الدولية	تدابير الأمن المادي	حماية سرية نظم المعلومات
المؤهل العلمي	1960.	360.1	0.435	320.4	3020.
التخصص	400.8	90.44	670.8	000.5	0.248
نوع البنك	0.000	0.000	0.000	0.000	0.000
المسمى الوظيفي	810.3	920.8	7280.	790.9	660.9
سنوات الخبرة	780.5	190.2	490.4	440.3	410.1
عدد الدورات التدريبية	0.000	50.10	0.003	50.00	340.1

الشكل: 14.4

تحليل التباين اللامعلمي لاستجابات أفراد العينية تجاه محاور الدراسة بحسب المتغيرات الديموغرافية



الجدول (4–18) والشكل (14.4) يبين نتائج تحليل التباين اللامعلمي للفروق بين مستويات الاستجابة حول محتوى أبعاد محوري الدراسة متطلبات الأمن السيبراني وحماية سرية نظم المعلومات بحسب الاختلاف في الخصائص الديموغرافية للمبحوثين والمتمثلة في (المؤهل–

التخصص–نوع البنك المسمى الوظيفي–سنوات الخبرة –عدد الدورات) ومن خلال قيم الدلالة الإحصائية للاختبار نلاحظ ما يلي:

1– قبول الفرضية الصفرية القائلة بتساوي وسيط الرتب لمتوسط استجابة المبحوثين حول محتوى أبعاد محوري الدراسة على اختلاف مؤهلاتهم العلمية وتخصصاتهم أو مسميات وظائفهم أو سنوات خبرتهم.

2- رفض الفرضية الصفرية القائلة بتساوي وسيط الرتب لمتوسط استجابة المبحوثين حول أبعاد محوري الدراسة على اختلاف نوع البنك الذين يعملون به.

3- رفض الفرضية الصفرية القائلة بتساوي وسيط الرتب لمتوسط استجابة المبحوثين حول أبعاد متطلبات الأمن السيبراني (التنظيمية – الامتثال للأطر والمعايير الدولية – تدابير الأمن المادي) على اختلاف عدد الدورات التدريبية التي تلقوها في مجال الأمن السيبراني.

ولمعرفة مصدر معنوية الفروق بالنسبة لنوع البنك وذلك بمقارنة متوسطات مستويات الاستجابة لكل بنكين على حده كما يلي:

الجدول: 4–19

متوسطات الاستجابة اتجاه أبعاد الدراسة بحسب نوع البنك

نوع البنك:	المتطلبات التنظيمية	المتطلبات الفنية	الامتثال للأطر والمعايير الدولية	تدابير الأمن المادي	حماية سرية نظم المعلومات
حكومي	3.2838	3.7538	3.2784	3.5372	3.7280
تجاري	3.7160	3.8747	3.6628	3.7779	3.7819
إسلامي	4.0378	4.2810	4.0235	4.1481	4.2537

الجدول:4–20

أبعاد المتغير المستقل	نوع البنك		
	حكومي (A)	تجاري (B)	إسلامي (C)
المتطلبات التنظيمية		A (0.022)	A (0.000) B (0.015)
المتطلبات الفنية			A (0.001) B (0.000)
الامتثال للأطر والمعايير الدولية		A (0.045)	A (0.000) B (0.004)
تدابير الأمن المادي			A (0.000) B (0.003)
حماية سرية نظم المعلومات			A (0.001) B (0.000)

من خلال المقارنات المتعددة الموضحة في الجدولين (4-19) (4-20) والشكل (15.4) يلاحظ أن مصادر الاختلاف في استجابات المبحوثين حول محتوى ابعاد محوري الدراسة بحسب الاختلاف في نوع البنك الذي ينتمون إليه يعود إلى البنوك الإسلامية، حيث مستويات الموافقة الأعلى على محتوى جميع ابعاد محوري الدراسة مقارنه بمستويات الموافقة للعاملين في البنوك الحكومية والتجارية. كما اختلفت البنوك التجارية والحكومية كذلك في مستويات الموافقة على محتوى بعدي (المتطلبات التنظيمية – الامتثال للأطر والمعايير الدولية) عند مستوى دلالة إحصائية .0.05

ولمعرفة مصدر معنوية الفروق بالنسبة لعدد الدورات التدريبية وذلك بمقارنة متوسطات مستويات الاستجابة لكل فئتين على حده كما يلي:

الجدول: 4-21

أبعاد المتغير المستقل (متطلبات الأمن السيبراني)	عدد الدورات التدريبية التي حصلت عليها في مجال الأمن السيبراني:			
	دورة (A)	دورتين (B)	ثلاث فأكثر (C)	لا شيء (D)
المتطلبات التنظيمية		D (0.005)	D (0.002)	
المتطلبات الفنية الامتثال للأطر والمعايير الدولية		D (0.024)	D (0.007)	
تدابير الأمن المادي			D (0.009)	
حماية سرية نظم المعلومات				

من خلال المقارنات المتعددة الموضحة في الجدول (4-21) والشكل (16.4) يلاحظ أن مصادر الاختلاف في استجابات المبحوثين حول محتوى ابعاد محوري الدراسة بحسب الاختلاف في عدد الدورات التي تلقوها يعود الى من تلقوا دورتين فأكثر حيث مستويات الموافقة الأعلى على محتوى ابعاد (المتطلبات التنظيمية – الامتثال للأطر والمعايير الدولية) عند مستوى دلالة إحصائية 0.05 وبعد (تدابير الأمن المادي) لمن تلقوا 3 دورات فأكثر.

4.4. خلاصة النتائج:

أولا: تحليل أبعاد الفقرات:

الجدول : 4-22

جدول تحليل أبعاد الفقرات

بُعد الدراسة	الفقرة الأكثر أهمية	الوسط المرجح	الأهمية النسبية	الفقرة الأقل أهمية	الوسط المرجح	الأهمية النسبية
المتطلبات التنظيمية	x2: فريق الامتثال	3.98	80%	x7: المشاركة في منتديات	3.59	72%
المتطلبات الفنية	c1: برامج الحماية	4.32	86%	c7: تقييمات الضعف	3.91	78%
الامتثال للمعايير	v5: تقييم المخاطر	3.94	79%	v7: المشاركة في المؤتمرات	3.56	71%
تدابير الأمن المادي	a1: أنظمة التحكم في الوصول	4.17	83%	a5: التدريب على الأمن المادي	3.68	74%
حماية نظم المعلومات	y12: تغيير كلمات المرور	4.18	84%	y10: المصادقة متعددة العوامل	3.85	77%

نتائج الدراسة:

المتطلبات التنظيمية

- **الأكثر أهمية :(x2)** النتائج تشير إلى أن البنوك تولي أهمية كبيرة لوجود فريق متخصص يضمن الامتثال للوائح الأمن السيبراني. هذا يعكس وعياً عالياً بأهمية الأمن السيبراني والحاجة لمتابعة مستمرة ومهنية.
- **الأقل أهمية :(x7)** مع ذلك، هناك نقص في المشاركة الفعالة بمنتديات الصناعة. هذا يدل على فرصة لتحسين التواصل وتبادل الخبرات والمعرفة مع أقرانهم في الصناعة.

المتطلبات الفنية

- **الأكثر أهمية :(c1)** استخدام أحدث برامج الحماية يشير إلى التزام البنوك بحماية بنيتها التحتية الرقمية من الأخطار المتزايدة.
- **الأقل أهمية :(c7)** التركيز أقل على إجراء تقييمات الضعف يوضح مجالاً للتحسين في فهم وإدارة المخاطر الأمنية.

الامتثال للمعايير الدولية

- **الأكثر أهمية :(v5)** تركيز البنوك على استخدام الأطر الدولية لتقييم المخاطر يدل على التزامها بأعلى المعايير وأفضل الممارسات العالمية.
- **الأقل أهمية :(v7)** مجدداً، نلاحظ تقصير في المشاركة الدولية، مما يحد من فرص التعلم وتبادل الخبرات.

تدابير الأمن المادي

- **الأكثر أهمية :(a1)** تطبيق أنظمة التحكم في الوصول يشير إلى وعي بأهمية حماية البيانات والأنظمة من الدخول غير المصرح به.
- **الأقل أهمية :(a5)** قلة التدريب المنتظم للموظفين على الأمن المادي يعتبر نقطة ضعف، إذ يجب تعزيز الوعي الأمني لدى الموظفين لضمان مستوى أعلى من الحماية.

حماية نظم المعلومات

- **الأكثر أهمية :(y12)** تغيير كلمات المرور بشكل دوري يظهر التزام البنوك بممارسات الأمان الأساسية، وهو خطوة مهمة نحو حماية البيانات.
- **الأقل أهمية :(y10)** استخدام المصادقة متعددة العوامل لم يحظ بنفس الاهتمام، مما يشير إلى حاجة لتحسين آليات المصادقة لزيادة الأمان.

ويستنتج الباحث أن هناك تركيز قوي على بعض المجالات، مثل المتطلبات التنظيمية والفنية، ولكن هناك فجوات واضحة في مجالات أخرى، مثل الامتثال للمعايير الدولية والتدريب المستمر

للموظفين. هذا يشير إلى أن البنوك اليمنية تتخذ خطوات جادة نحو تعزيز الأمن السيبراني، ولكنها تحتاج إلى توسيع نطاق جهودها لتشمل مجالات أوسع.

من وجهة نظر الباحث، ضرورة تبني البنوك استراتيجية شاملة تغطي جميع جوانب الأمن السيبراني. يجب أن تشمل هذه الاستراتيجية تحسين الامتثال للمعايير الدولية وزيادة مشاركة الموظفين في برامج التدريب والتوعية. من خلال توسيع نطاق الجهود وتعزيز التزامها بممارسات الأمن السيبراني وضرورة الاستمرار في تطوير وتحسين هذه الممارسات.

ثانياً: نتائج الفرضية الأولى وفروعها:

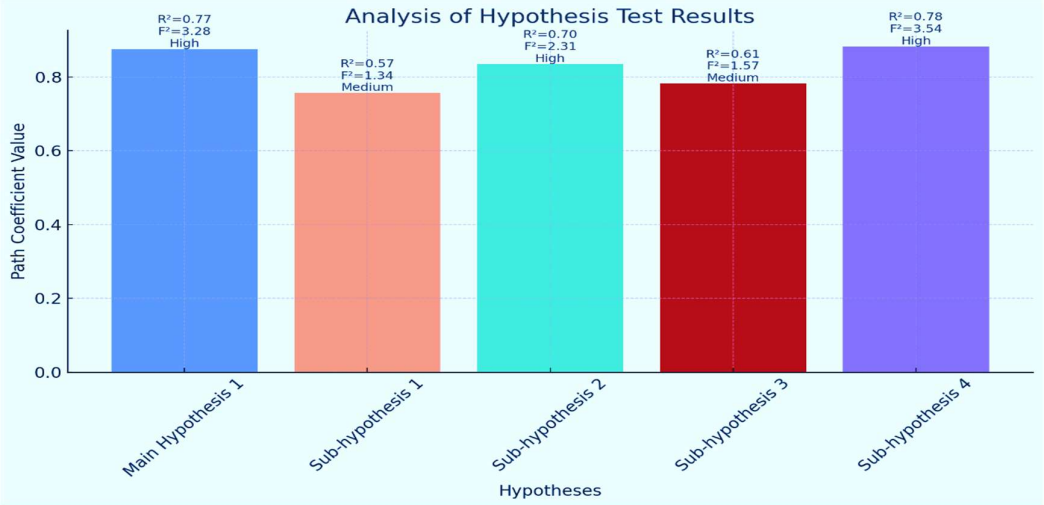
الجدول: 4-23

نتائج تحليل النموذج البنائي للمتغيرات الكامنة المعتمد على الفرضية الرئيسية وفروعها

الفرضية	R^2	F	تصنيف القوة
الفرضية الرئيسية 1	0.77	3.28	عالي
الفرضية الفرعية 1	0.57	1.34	متوسط
الفرضية الفرعية 2	0.70	2.31	عالي
الفرضية الفرعية 3	0.61	1.57	متوسط
الفرضية الفرعية 4	0.78	3.54	عالي

الشكل: 15.4

نتائج الفرضية الرئيسية الأولى والفرضيات الفرعية المنبثقة عنها



يبين الجدول رقم (4–18) والشكل رقم (15.4) الآتي:

الفرضية الرئيسية الاولى: لها قيمة معامل مسار عالية (R^2 = 0.77) وقيمة F مرتفعة = F) (3.28، ما يدل على قوة العلاقة والتأثير الكبير لهذه الفرضية.

الفرضية الفرعية الأولى: تُظهر قيمة متوسطة لمعامل المسار (R^2 = 0.57) وقيمة F متوسطة (F = 1.34)، ما يشير إلى أن هذه الفرضية لها تأثير معتدل.

الفرضية الفرعية الثانية: لديها قيمة معامل مسار عالية (R^2 = 0.70) وقيمة F عالية F) (2.31 =، ما يعني أن تأثيرها قوي.

الفرضية الفرعية الثالثة: تُظهر قيمة متوسطة لمعامل المسار (R^2 = 0.61) وقيمة F متوسطة (F = 1.57)، ما يعني أن لها تأثير معتدل أيضًا.

الفرضية الفرعية الرابعة: تمتلك أعلى قيمة معامل مسار (R^2 = 0.78) وأعلى قيمة F (F 3.54 =بين الفرضيات الأخرى، ما يشير إلى أن لها التأثير الأكبر وأقوى العلاقات.

ثانياً: نتائج الفرضية الرئيسية الثانية:

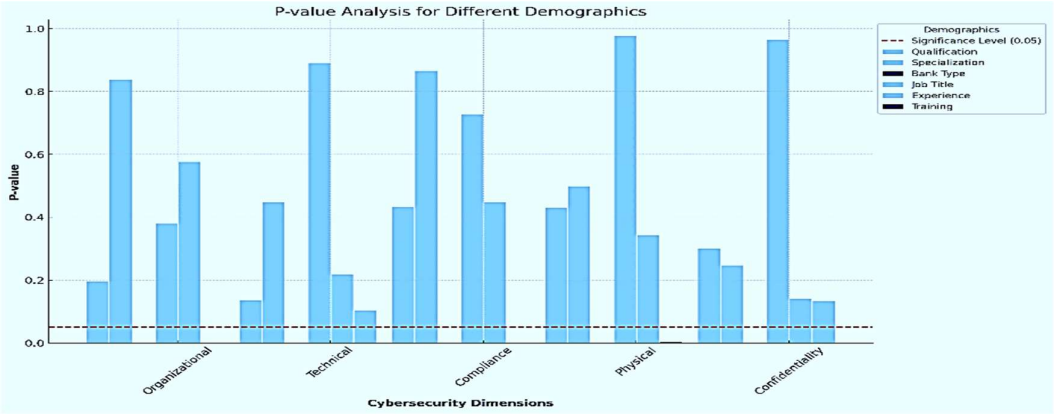
الجدول: 4-24

نتائج تحليل الفرضية الرئيسية الثاني:

	المتطلبات التنظيمية	المتطلبات الفنية	الامتثال للأطر والمعايير	المتطلبات المادية	حماية نظم المعلومات
المؤهل العلمي	0.196	0.136	0.435	0.432	0.302
التخصص	0.84	0.449	0.867	0.5	0.248
نوع البنك	0	0	0	0	0
المسمى الوظيفي	0.381	0.892	0.728	0.979	0.966
سنوات الخبرة	0.578	0.219	0.449	0.344	0.141
عدد الدورات التدريبية	0	0.105	0.003	0.005	0.134

الشكل: 16.4

نتائج تحليل الفرضية الرئيسية الثاني:



تُظهر النتائج المجمعة لتحليل الفرضية الرئيسية الثانية أن هناك تأثيرات متفاوتة للمتغيرات الديموغرافية على متطلبات الأمن السيبراني وحماية سرية أنظمة المعلومات، حيث تُشير القيم المنخفضة لـ p-value (دون مستوى الدلالة 0.05) إلى وجود فروق جوهرية بين متوسطات

الاستجابات في بعض المتغيرات الديموغرافية، وخاصةً "نوع البنك" و"عدد الدورات التدريبية"، مما يعني أن هذه المتغيرات لها تأثير ملحوظ على كيفية إدراك توافر متطلبات الأمن السيبراني وفعالية حماية سرية المعلومات.

يتبين أن الموظفين في البنوك الإسلامية لديهم استجابات أكثر إيجابية تجاه جميع أبعاد الأمن السيبراني مقارنة بالبنوك الحكومية والتجارية، مما قد يعكس مستوى أعلى من الوعي أو التنفيذ لمتطلبات الأمن السيبراني في هذه البنوك، كما يشير التحليل إلى أن الأفراد الذين حضروا دورتين تدريبيتين فأكثر يظهرون فهماً أكبر للمتطلبات التنظيمية والامتثال للأطر والمعايير الدولية، الأمر الذي يدل على أهمية التدريب في تعزيز فهم الأمن السيبراني.

5.4. الاستنتاجات:

بناء على تحليل البيانات والنتائج، توصل الباحث إلى مجموعة من الاستنتاجات أبرزها الآتي:

1- يقر العاملين في البنوك اليمنية بتوافر مستويات متوسطه من متطلبات الامن السيبراني في بنوكهم بحسب آرائهم

2- يرى العاملون في البنوك اليمنية بأن المتطلبات الفنية هي الأعلى توافر من جميع المتطلبات الأخرى وبالأخص أحدث برامج الحماية وبرامج مكافحة الفيروسات والبرامج الضارة على جميع الأنظمة.

3- كما يقر العاملين من خلال مستويات استجاباتهم بوجود مستويات عالية من الحماية لسرية نظم المعلومات في البنوك التي يعملون بها وخصوصا بما بفرضه البنك من تغيير كلمات المرور بشكل دوري لجميع المستخدمين.

4- هناك علاقة قوية وأثر عالي لمستويات توافر متطلبات الامن السيبراني في البنوك اليمنية على تعزيز مستويات الحماية لسرية نظم المعلومات في تلك البنوك بحسب اراء العاملين فيها

5- تعتبر مستويات التوافر لتدابير الامن المادي الأعلى تأثيرا بين جميع المتطلبات على مستويات الحماية لسرية نظم المعلومات في البنوك اليمنية بحسب اراء العاملين فيها

6- لا يوجد اختلاف جوهري بين اراء العاملين في البنوك اليمنية حول مستويا توافر متطلبات الامن السيبراني ومستويات الحماية لسرية نظم المعلومات في بنوكهم باختلاف مؤهلاتهم العلمية، أو تخصصاتهم، او مسميات وظائفهم ،او سنوات خبرتهم .

7- هناك اختلاف جوهري في اراء العاملين في البنوك اليمنية حول مستويا توافر متطلبات الامن السيبراني ومستويات الحماية لسرية نظم المعلومات في بنوكهم باختلاف نوع البنك الذي ينتمون اليه حيث تمثل البنوك الإسلامية مصدر الاختلاف في هذه الحالة بمستويات توافر اعلى من بقية البنوك لمتطلبات الامن السيبراني ومستويات الحماية لسرية نظم المعلومات فيها

8- هناك اختلاف جوهري في اراء العاملين في البنوك اليمنية حول مستويات توافر متطلبات الامن السيبراني خاصه (المتطلبات التنظيمية- الامتثال للأطر والمعايير الدولية) باختلاف عدد الدورات التي تلقوها وتمثل مصدر الاختلاف في اراء من تلقوا أكثر من دورتين عن الذين لم يتلقوا أي دوره او تلقوا دوره واحده

6.4. توصيات الدراسة:

في ضوء نتائج الدراسة يمكن تقديم التوصيات الآتية:

1. **تحسين وتعزيز المتطلبات التنظيمية والامتثال للمعايير الدولية:** نظرًا لأن هناك تباين في الآراء حول مستويات توافر المتطلبات التنظيمية والامتثال للمعايير الدولية باختلاف عدد الدورات التدريبية، يُنصح بتعزيز برامج التدريب والتطوير المهني للعاملين في البنوك لضمان فهم أعمق وامتثال أفضل لهذه المتطلبات.

2. **تعزيز الأمن المادي:** بما أن الأمن المادي يُعتبر من أهم العوامل المؤثرة على حماية سرية نظم المعلومات، يجب على البنوك تخصيص المزيد من الموارد والجهود لتحسين الإجراءات الأمنية المادية، مثل تعزيز الأمن في مراكز البيانات والفروع.
3. **تحديث وتطوير برامج الحماية ومكافحة الفيروسات:** يجب على البنوك استمرار التحديث والتطوير المستمر لبرامج الحماية ومكافحة الفيروسات لضمان أعلى مستويات الحماية من التهديدات السيبرانية.
4. **إدارة كلمات المرور وسياسات الأمن السيبراني:** يُوصى بتبني سياسات متقدمة لإدارة كلمات المرور، مثل تغيير كلمات المرور بشكل دوري واستخدام كلمات مرور قوية وفريدة، لتعزيز الحماية ضد الوصول غير المصرح به.
5. **تقديم تدريبات متخصصة حول الأمن السيبراني:** يُنصح بتقديم دورات تدريبية متخصصة في مجال الأمن السيبراني للعاملين، خاصةً للذين لم يتلقوا تدريبات كافية، لزيادة الوعي وتعزيز المهارات الأمنية.
6. **تعزيز التعاون والتنسيق بين أنواع البنوك المختلفة:** بما أن هناك اختلافات في مستويات الأمان السيبراني بين البنوك الإسلامية وغيرها، يجب تشجيع التعاون وتبادل الخبرات بين مختلف أنواع البنوك لتحسين معايير الأمان السيبراني على نطاق أوسع.
7. **تطوير خطط الاستجابة للحوادث السيبرانية:** يُنصح بتطوير وتحديث خطط الاستجابة للحوادث السيبرانية بشكل مستمر للتعامل مع أي تهديدات أمنية بفعالية وسرعة.
8. **إجراء تقييمات دورية للأمن السيبراني:** يُنصح بإجراء تقييمات دورية للبنية التحتية السيبرانية للكشف عن أية ثغرات أمنية والتعامل معها بشكل فوري.

7.4 مقترحات بالدراسات المستقبلية:

1. تأثير الذكاء الاصطناعي على أمان البنوك.
2. الممارسات الأمنية السيبرانية في البنوك التجارية والإسلامية: تحليل الاختلاف والتشابه.
3. العلاقة بين الهياكل التنظيمية، الثقافة المؤسسية، واستجابات البنوك للتحديات الأمنية: دراسة تحليلية.
4. تأثير العوامل الثقافية والهيكلية على استراتيجيات الأمان السيبراني: دراسة مقارنة بين البنوك.
5. تقييم تأثير التهديدات السيبرانية المستجدة والتكنولوجيا المالية على استعداد البنوك واستجاباتها: دراسة متعددة الأبعاد.

المراجع

المراجع

أولاً: المراجع العربية:

إبراهيم طارق، مجذوب. (2023). دور البنك المركزي في تطوير أدوات التكنولوجيا التنظيمية Regtech استخدامها في الرقابة المصرفية. Academic Journal of Research and Scientific Publishing. https://doi.org/10.52132/ajrsp/v4.45.1

البابلي، عمار ياسر. (2020). آليات التأمين والوقاية من الهجمات السيبرانية بالتطبيق على معايير الجودة الخاصة بالمواصفات القياسية لنظام إدارة أمن المعلومات ISO 27001 للحماية من مخاطر الإرهاب الإلكتروني. مجلة الأمن والقانون, 28(251-356) , ع2. أكاديمية شرطة دبي. https://doi.org/10.54000/0576-028-002-006

الخطيب، محمد. (يوليو, 2021). تحديات الأمن السيبراني وكيفية احباط الهجمات السيبرانية. مجلة المصارف, صفحة 40. تم الاسترداد من file:///D:/%D9%85%D8%AC%D9%8A%D8%A8%20%D8%A7%D9%84%D8%AD%D9%83%D9%8A%D9%85%D9%8A/1629055746.pdf

الدحياني، ن. س. ع. م.، والصنوي، أ. ع. ح. م. (2021). متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء. مجلة الجامعة الوطنية, 2021(18), 93-126 . https://search.emarefa.net/detail/BIM-1465600

السمحان، منى عبد الله. (يوليو, 2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود.

السمور، أنس محمد سند والخزعلي، عاطف سالم خالد. (2020). تقييم الأمن السيبراني الوطني في منع الأزمات والكوارث في البنوك الأردنية.

الصويلح، س م. (2023). دور أنظمة الذكاء الاصطناعي في مكافحة الشائعات الالكترونية. المجلة العربية للدراسات الأمنية, 39(1) , 80-97. https://doi.org/10.26735/QFPP7610 .

العزام، نوره. (2020). دور الذكاء الاصطناعي في رفع كفاءة النظم الادارية لإدارة الموارد البشرية في جامعة تبوك. جامعة الامام محمد بن سعود الاسلامية، تبوك.

الزبيدي، محمد علي والحميري، نبيل حسام. (فبراير, 2021). أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات – دراسة ميدانية على شركات الاتصالات العاملة في اليمن. مجلة الدراسات الاجتماعية، صفحة 125 . https://doi.org/10.20428/JSS.27.1.5

بن ساسي، خضرة دحو، وحسيني إسحاق. (2023). علاقة التكنولوجيا المالية الرقمية بالشمول المالي. مجلة الدراسات القانونية والاقتصادية, 5(3) , 991-1010. تم الاسترداد من https://www.asjp.cerist.dz/en/downArticle/649/5/3/227328

جمعية البنوك اليمنية . https://yemen-yba.com/category/tech. (2022). .صنعاء.

سما العلم. (2022). الأمن السيبراني في اليمن ما هو الأمن السيبراني. تم الاسترداد من https://samaaleelm.blogspot.com/2021/10/blog-post_13.html

شيخي، م، مليكة، خ، دحو، ع، وسعيدي، ع، وبرزوق، ع. (2020). تأثير التمكين النفسي على الأداء الوظيفي للعاملين بوجود الرضا الوظيفي كمتغير وسيط: دراسة حالة القطاع المصرفي بسعيدة. مجلة التنظيم والعمل, 8(3) , 42-60. تم الاسترداد من https://search.emarefa.net/detail/BIM-1039043

صالح، فرح يحي عيسى والمجالي، رضوان محمود سليمان. (2022). أثر تهديدات الأمن السيبراني على الأمن القومي: الولايات المتحدة الأمريكية حالة دراسة (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة، الأردن. تم الاسترداد من http://search.mandumah.com/Record/1362215

صندوق النقد العربي. (2019). موجز سياسات الأمن السيبراني في القطاع المصرفي . https://www.amf.org.ae/arد. محمد اسماعيل.

عبد السلام، ياسر . (2022). دور الضبط الإداري الإلكتروني في الرقابة السيبرانية وتهيئة البيئة السيبرانية الأمنة. مجلة القانون والتكنولوجيا, 2(1) , 139-176. https://doi.org/10.54873/jolets.v2i1.22 .

عطياني، م س، الخرابشة، س ع، نور، م والبستنجي، خ ع. (2022). الخدمات المصرفية الإلكترونية وأثرها في تحقيق الميزة التنافسية للبنوك الإسلامية الأردنية. المجلة الأردنية للعلوم التطبيقية – سلسلة العلوم الإنسانية, 31(2) , 99-114. https://doi.org/10.35192/jjoas-h.v31i2.306 .

لرقط، سمية. (ديسمبر, 2021). أثر تكنولوجيا المعلومات على الأمن المعلوماتي. مجلة ابحاث اقتصادية واجتماعية, 3, 431-448.

فارغ المسلمي. (2019 فبراير). *إعادة تفعيل القطاع المصرفي في اليمن: خطوة ضرورية لاستئناف الدورة المالية الرسمية وتحقيق أسس الاستقرار الاقتصادي.* مركز صنعاء للدراسات الاستراتيجية. تم الاسترداد من https://sanaacenter.org/files/Revitalizing_Yemens_Banking_Sector_ar.pdf

مؤمن، ش م. (2019). التعدين المالي للبيانات لدعم الممارسات الرقابية بهدف رفع كفاءة النظم المحاسبية الرقمية. *الفكر المحاسبي*. 96-152. *(ATASU)*, 23(3) , تم الاسترداد من https://sciences.univeyes.net/journals/atasu_journal/article_495

ثانيا: المراجع الأجنبية:

Abad-Segura, E., González-Zamar, M., López-Meneses, E., & Vázquez-Cano, E. (2020). Financial technology review of trends, approaches, and management. *Mathematics*, 8(6), 951-973. https://doi.org/10.3390/math8060951

Abohatem, A., Al-Khulaidi, A., & Ba-Alwi, F. (2023). Suggestion Cybersecurity Framework (CSF) for Reducing Cyber-Attacks on Information Systems. *Journal of Sana'a University for Applied Sciences and Technology*, 1(3), 234-252. https://doi.org/10.59628/jast.v1i3.248

Adak, A., Pradhan, B., & Shukla, N. (2022). Sentiment Analysis of Customer Reviews of Food Delivery Services Using Deep Learning and Explainable Artificial Intelligence: Systematic Review. *Foods*, 11. https://doi.org/10.3390/foods11101500

Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. *Sensors (Basel, Switzerland)*, 23. https://doi.org/10.3390/s23010218

Alawadhi, M., & Awad, W. (2023). Multi-Factor Authentication Modeling using Petri Nets: Review. In *Proceedings of the 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, (pp. 1-5). https://doi.org/10.1109/ITIKD56332.2023.10099567

Alexei, A. (2021). Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Sciences*. https://doi.org/10.52326/JSS.UTM.2021.4(1).11

Al-Khulaidi, A. A., Nasser, A. A., Alanesi, N. K., Hazaa, M. A., Aljober, M., & Alkhulaidi, N. A. (2022). Information security gap analysis: An applied study on the Yemeni banking sector's technology and innovation practices. *The Seybold Report Journal*, (11), 17. https://doi.org/10.5281/zenodo.7307869

Amiruddin, A., Afiansyah, H., & Nugroho, H. (2021). Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. In *2021 International Conference on Informatics, Multimedia, Cyber and Information System*

(ICIMCIS) (pp. 19-24). Jakarta: IEEE. https://doi.org/10.1109/ICIMCIS53775.2021.9699337

Anand, K., Duley, C., & Gai, P. (2022). Cybersecurity and Financial Stability. *Deutsche Bundesbank Discussion*, 8. Retrieved from https://ssrn.com/abstract=4073158 or http://dx.doi.org/10.2139/ssrn.4073158

Ansari, M. (2022). A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs. *International Journal of Smart Sensor and Adhoc Network*. https://doi.org/10.47893/ijssan.2022.1212

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., ... Bonacina, S. (2022). Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. *Journal of Medical Internet Research*, 25.

Ariza-López, I., Ariza-López, F., Reinoso-Gordo, J., Gómez-Blanco, A., Rodríguez-Moreno, C., & León-Robles, C. (2015). Quality Elements for BIM Applied to Heritage Monuments. *Semantic Scholar*. Retrieved from https://blogs.ugr.es/smlab/wp-content/uploads/sites/26/2018/02/Ariza-etal-2015a.pdf

Arner, D., Barberis, J., & Buckley, R. (2015). The evolution of fintech: a new post-crisis paradigm? *SSRN Electron.* Retrieved from https://doi.org/10.2139/ssrn.2676553

Asutosh, V., Kumar, A., Sattar, A., & Ranjan, M. (2023). Fortifying the Cloud: Unveiling the Next-Generation Security Model of AWS. *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*. https://doi.org/10.37082/ijirmps.v11.i3.230230

Atnafie, S., Anteneh, D., Yimenu, D., & Kifle, Z. (2021). Assessment of exposure risks to COVID-19 among frontline health care workers in Amhara Region, Ethiopia: A cross-sectional survey. *PLoS ONE*, 16. https://doi.org/10.1371/journal.pone.0251000

Ben Naseir, M. A., Dogan, H., & Apeh, E. (2020). National Cybersecurity Capacity Building Framework for counties in a Transitional Phase (Using Spring Land as a case study). In *Proceedings of the 22nd International Conference on Enterprise Information Systems*, 2, 1-307. Bournemouth University. https://doi.org/10.5220/0009576708410849

Berdyugin, A., & Revenkov, P. (2019). Approaches to measuring the risk of cyberattacks in remote banking services of Russia. *Bit Numerical Mathematics*, (26), 83-92. https://doi.org/10.26583/bit.2019.4.06

Bleier, T., Langer, D., Skopik, F., & Smith, P. (2013). Smart grid cybersecurity standards: today and tomorrow. *AIT Austrian Institute of Technology*. http://www.flosko.at/ait/2013_sgforum.pdf

Bourgeois, D. T., Smith, J. L., Wang, S., ... Joseph. (2019). Information Systems for Business and Beyond. *Open Textbooks*, 1. Retrieved from https://digitalcommons.biola.edu/open-textbooks/1

Buchanan, W. (2014, October 31). In cybersecurity, the weakest link is ... you. *Journal of Computer Science*, 12(4). Retrieved from https://theconversation.com/in-cybersecurity-the-weakest-link-is-you-33524

Calzolari, G. (2021). Artificial Intelligence and the financial sector at crossroads. *PE 662.912*. https://doi.org/247172166

Canavan, J. (2012). Fundamentals of Network Security. https://doi.org/13413977

Chen, Y., & Chou, J. (2014). ID-Based Certificateless Electronic Cash on Smart Card: Protection against Identity Theft and Financial Card Fraud. https://doi.org/281815

Choi, W., Kim, M., & Na, D. (2023). Recent issues and regulatory requirements of data integrity in the pharmaceutical industry. *Yakhak Hoeji*. https://doi.org/10.17480/psk.2023.67.4.215

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2005). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*. https://doi.org/10.1108/TQM-09-2020-0202

David, R. S. (2021, FAB). Organizational science and cybersecurity: abundant opportunities for research at the interface. USA*, 37, 1-29.*

Davis, K., Yost, E., Brauneis, J., Krumme, A., Geldhof, A., Tuck, A., ... Ephross, S. (2023). Landscape review of global real-world data sources for studying medication use in pregnancy and lactation that support regulatory decision making. *Pharmacoepidemiology and Drug Safety*. https://doi.org/10.1002/pds.5711

de Azambuja, A., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*. https://doi.org/10.3390/electronics12081920

Dhatchina, M., & Dhatchina, M. (2020). Cyber Attacks in banking industry. *cyber-attacks in banks; Bournemouth Project: cyber-crime in banking*. Faculty of Science and Technology. U.S. Retrieved from https://www.researchgate.net/publication/347440777_CYBER_ATTACKS_IN_THE_BANKING_INDUSTRY

Ding, Y., Wu, Z., Tan, Z., & Jiang, X. (2021). Research and application of security baseline in business information system. Procedia Computer Science, 630-635.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*. https://doi.org/10.4236/JIS.2013.42011

Dodge, C., Fisk, N., Burruss, G., Moule, R., & Jaynes, C. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*. https://doi.org/10.1111/1745-9133.12641

Dongol, R., & Chatterjee, J. (2019). Robust security framework for mitigating cyber threats in banking payment system: A study of Nepal. *Journal of Computer Science*, 35(1), 45-60. https://doi.org/10.26683/208155709

Ecubay, F., & Kilimvi, A. (2023). Implications of informal money transfer systems on Kenya's financial sector. *American Journal of Finance*, 15, 20. https://doi.org/10.47672/ajf.1520

Efijemue, O., Ejimofor, I., & Owolabi, O. (2023). Insider Threat Prevention in the US Banking System. *International Journal on Soft Computing*. https://doi.org/10.5121/ijsc.2023.14302

Force, J. T. (2020). Security and Privacy Controls for Information Systems and Organizations. *nvlpubs*. https://doi.org/10.6028/NIST.SP.800-53R5

Friedman, J. H. (2006). Recent Advances in Predictive (Machine) Learning. *Journal of Classification*, 23, 2, 175-197.

García Araque, J. O. (2017). Auditoría al Sistema de Gestión de Seguridad información en el proceso de desarrollo de software de acuerdo a la Norma ISO/IEC 27001:2013 en la empresa IT Stefanini Colombia. *Universidad Nacional Abierta y a Distancia UNAD*. https://repository.unad.edu.co/handle/10596/11944

Gavėnaitė-Sirvydienė, J., & Miečinskienė, A. (2023). The Assessment of Cyber Security's Significance in the Financial Sector of Lithuania. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1243

George, A., & George, A. (2021). A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall. *IJARCCE: International Journal of Advanced Research in Computer and Communication Engineering*, 5, 31-37. https://doi.org/10.5281/zenodo.7027397

Górka, M. (2023). Design of an Innovative Model of Cooperation Between Schools and the Public for the Cybersecurity of Children and Adolescents. *Multidisciplinary Journal of School Education*. https://doi.org/10.1145/3274694.3274710

Grandon Gill, T., & DBA. (2018). A NOTE ON THE CYBERSECURITY PROBLEM SPACE IN. Muma Case Review. A publication of the Muma College of Business, University of South Florida. Retrieved from http://pubs.mumacasereview.org/2018/MCR-03-08-Note-CybersecurityProblemSpace-Fulford-p1-9.pdf

Grasmick, T., & Reichwald, H. (2015). Cyber Compliance: The Board's Next Enforcement Action Worry. *ABA Banking Journal*, 107, 62.

Gurgun, A., Bayhan, H., Polat, G., & Turkoglu, H. (2018). Schedule Risk Assessment in Green Building Projects in M. Abdul-Malak, H. Khoury, A. Singh, & S. Yazdani (Eds.), *Responsible Design and Delivery of the Constructed Project*. ISEC Press. https://doi.org/10.14455/isec.res.2018.50

Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). Defending against cybersecurity threats to the payments and banking system. *arXiv preprint arXiv*, 2212.12307.

Hedlund, B. (2013, July 9). What is a distributed firewall? *VMware Blogs*. Retrieved from https://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html/

Hema, T. (2022). Integrated Automotive Software Quality Management System in compliance with Automotive SPICE, ISO 26262, ISO 21448 and ISO 21434 Standards. *International Journal of Scientific and Research Publications*, 12(1). https://doi.org/10.29322/ijsrp.12.01.2022.p12123

Herrera, D., Pereira, W., Volochen, L., & Zárate Moreno, A. (2023). Open Finance in Latin America and the Caribbean: Great Opportunities, Large Challenges. http://dx.doi.org/10.18235/0004937

Hsu, T. (2021). Machine learning applied to stock index performance enhancement. *J Bank Financ Technol*. https://doi.org/10.1007/s42786-021-00025-6.

Humied, I. A. (2023). Cybersecurity As an Emerging Challenge to Yemen Security. *Journal of Cyber Security in Computer System*, 1(3), 1-4. https://doi.org/10.13140/RG.2.2.12582.29764

Ige, O. (2021). Trends of cybercrime from 2001 to 2021: cybersecurity action plan for Papua New Guinea. *Global Society*. https://doi.org/10.1007/s44282-023-00007-7

Ikram, I., & Madkour, M. (2020). A Hybrid Intrusion Detection System for 802.11 Networks with Effective Feature Selection. *JKAU: Computer and Information Technology*, 9(1), 45-62. https://doi.org/10.4197/Comp.9-1.4

Inayat, U., Zia, M., Mahmood, S., Berghout, T., & Benbouzid, M. (2022). Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects. *Electronics*, 11, 3854. https://doi.org/10.3390/electronics11233854

Initiative, J. (2021). Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39). *National Institute of Standards and Technology*. https://csrc.nist.gov/publications/detail/sp/800-39/final

Islam, H., Madavarapu, J., Sarker, N., & Rahman, A. (2022). The Effects of Cyber Threats and Technical Problems on Customer's Attitude Towards E-Banking Services. *Oblik i finansi*. https://doi.org/10.33146/2307-9878-2022-2%2896%29-58-67

Jenifa, M., & Ambika, K. (2020). Enabling Secure Data Sharing Scheme in Cloud Storage Group by Verify Using Third Party Authentication. *International Journal of Research in Engineering, Science and Management*, 3(7). Retrieved from https://journal.ijresm.com/index.php/ijresm

Johnson, T. (2005). Computer Security Incident Handling Guide. https://doi.org/10.1201/9781420028379.AXC

Junaido, B. M., & Mua'zu, A. S. (2015). Cyber-Attacks: The legal response. *International Journal of International Law*, 1, 2.

K, B., N, B., & Prithvikiran. (2023). Malware Classification using Deep Learning Methods. *2023 3rd International Conference on Smart Data Intelligence (ICSMDI)*, 278-281. https://doi.org/10.1109/ICSMDI57622.2023.00058

Kafi, M., & Akter, N. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *American Journal of Trade and Policy*. https://doi.org/10.18034/ajtp.v10i1.659

Kale, N., Metre, K., Chitte, P., Mahankale, N., Gore, S., & Gore, S. (2023). Cloud Computing for Effective Cyber Security Attack Detection in Smart Cities. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9s), 777-785. https://doi.org/10.17762/ijritcc.v11i9s.7968

Karakaya, M., & SevinA. (2022). Survey of Cyber-Threats for the Security of Institutions. In *5th International Symposium on Innovative Approaches in Smart Technologies (ISAS2022)*, (pp. 93-99). SETSCI. https://doi.org/10.36287/setsci.5.1.018

Kaspersky. (2021, June 5). Retrieved from Kaspersky: http://www.Kaspersky.com

Kaspersky. (2021, January 28). Retrieved from Kaspersky: http://www.Kaspersky.com

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 15. https://doi.org/10.3390/su15075828

Kolesnichenko, A. N. (2023, University Journal). The possibilities of using virtual reality technology in teaching a foreign language. 12(2), pp. 266-270. doi:https://doi.org/10.55355/snv2023122311

Koláříková, D. (2019). About the current lexical productivity of the word-forming element "cyber". *31*(1), pp. 37-51. doi: doi: 10.5507/ro.2019.003

Laib, S. (2021). The Importance of Cyber Security in the Financial Sector in the Age of Digital Transformation. *Al-Asil Journal of Economic and Administrative Research*, 5, 1, 448-464. ISSN 2571-9866

Lankton, N., Price, J., & Karim, M. (2021). Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters. *Journal of Information Systems*, 35(1), 101–119. https://doi.org/10.2308/isys-18-071

Lee, I., & Shin, Y. (2018). Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges. *Business Horizons*, 61(1), 35-46. https://doi.org/10.1016/j.bushor.2017.09.003

Leonard, O., & Eugenia, O. (2020). Effect of Environmental Disclosures on Dividend Payout of Firms in Nigeria. *IIARD International Journal of Banking and Finance Research*, 6(3). Retrieved from http://m.sc

Lewis, N., Connelly, Y., Henkin, G., Leibovich, M., & Akavia, A. (2022). Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records. *Healthcare Informatics Research*, 28, 132-142. https://doi.org/10.4258/hir.2022.28.2.132

Li, L. (2023). Data Security Technology in Electronic Commerce System Development. In *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)*, (pp. 1-6). https://doi.org/10.1109/ICAISC58445.2023.10200851

Liang, J., & Kim, Y. (2022). Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall. In *Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. https://doi.org/10.1109/CCWC54503.2022.9720435

Logan, P., & Clarkson, A. (2020). Enhancing Information Security: A Qualitative Risk Analysis Method for Overcoming the Insider Threat. In M. Khosrow-Pour (Ed.), *Managing Modern Organizations Through Information Technology, Proceedings of the 2005 Information Resources Management Association International Conference*. Idea Group Publishing. http://www.idea-group.com

Long, Y., & Liu, Y. (2018). Text Coverless Information Hiding Based on Word2vec. In *Lecture Notes in Computer Science, 11066*. (Z. Sun, & E. Pan, Eds.) https://doi.org/10.1007/978-3-030-00015-8_40

Manisha, M., Jadhav, M., & Nalawade, K. (2016, December). Online Banking and Cyber Attacks: The Current Scenario. 5, pp. 743-749. Retrieved from https://www.researchgate.net/publication/290325373_Online_Banking_and_Cyber_Attacks_The_Current_Scenario

Mishra, A., Alzoubi, Y., Gill, A., & Anwar, M. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, 22, 538. https://doi.org/10.3390/s22020538

Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, 13(10). https://doi.org/10.3390/app13105875

Mungo, J. (2023). Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. *Journal of Cyber Security Technology*. https://doi.org/10.1080/23742917.2023.2244210

Nguyen, T., Koblandin, K., Suleymanova, S., & Volokh, V. (2021). Effects of 'Digital' Country's Information Security on Political Stability. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1112

Nowikowska, M. (2021). Personal Data Protection in the Context of the Act on the National Cybersecurity System. *Cybersecurity in Poland*. https://doi.org/10.1007/978-3-030-78551-2_11

Nykänen, R., & Kärkkäinen, T. (2014). Aligning Two Specifications for Controlling Information Security. *IJCWT*, 4(2). https://doi.org/10.4018/IJCWT.2014040104

Olusolade, A., Fadare, & Mat Aji, Z. (2020). Modelling the Phishing Avoidance Behaviour Among Internet Banking Users in Nigeria: The Initial Investigation. *Journal of Computer Engineering and Technology*, 4(1), 1-17. Retrieved from https://ssrn.com/abstract=3528954

Oprea, A., Li, Z., Norris, R., & Bowers, K. (2018). MADE: Security Analytics for Enterprise Threat Detection. *Proceedings of the 34th Annual Computer Security Applications Conference*. https://doi.org/10.1145/3274694.3274710

Paganini, S., Meier, E., Terhorst, Y., Wurst, R., Hohberg, V., Schultchen, D., ... Messner, E. (2023). Stress Management Apps: Systematic Search and Multidimensional Assessment of Quality and Characteristics. *JMIR Mhealth Uhealth*, 11. https://doi.org/10.2196/42415

Pambudi, R., & Ramli, K. (2023). Information security risk management design of supervision management information system at XYZ Ministry using NIST SP 800-30. *Jurnal Teknik Informatika (JUTIF)*, 4(3), 591-599. https://doi.org/10.52436/1.jutif.2023.4.3.978

Pandey, P. (2021). Overview of Cyber Security. *International Journal of Advanced Research in Science, Communication and Technology* (IJARSCT), 7(3). https://doi.org/10.22214/ijraset.2021.38022

Paoletti, M., Haut, J., Tao, X., Plaza, J., & Plaza, A. (2020). A New GPU Implementation of Support Vector Machines for Fast Hyperspectral Image Classification. *Remote Sensing*, 12, 1257. https://doi.org/10.3390/rs12081257

Purwanto, H., Yandri, D., & Yoga, M. (2022). Perkembangan dan dampak financial technology (fintech) terhadap perilaku manajemen keuangan di masyarakat. *Jurnal Ilmiah Manajemen, Organisasi dan Bisnis.*, 11(1). https://doi.org/10.56486/kompleksitas.vol11no1.220

Putra, A., & Soewito, B. (2023). Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector. *International Journal of Advanced Computer Science and Applications*, 4(14), 625-633. https://doi.org/10.14569/ijacsa.2023.0140468

Putri, M., & Hakim, A. (2021). Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005: 2018 dan NIST SP 800-30 Revisi 1. *Info Kripto*, 15, 134-141.

Rathod, R. H. (2013). Roll of Distributed Firewalls in Local Network for Data Security. https://doi.org/ID: 39173224

Ren, R., Ma, M., & Liu, W. (2023). Design of Network Information Security Optimal Defense System Based on SM2 Algorithm and Blockchain Technology. In *Proceedings of the 2023 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS)*. https://doi.org/10.1109/AIARS59518.2023.00052

Rjoub, H., Adebayo, T., & Kırıkkaleli, D. (2023). Blockchain technology-based FinTech banking sector involvement using adaptive neuro-fuzzy-based K-nearest neighbors algorithm. Financial Innovation. https://doi.org/10.1186/s40854-023-00469-3

RSBP for Central Asia. (2020). COVID-19: cybersecurity challenges for financial institutions. Retrieved from https://s1.rsbp-ca.org/en/library/msme-finance/ksep-lib-cybersecurity-during-covid-19.html

Samour, A., & Al-Khazali, A. (2022). Assessment of National Cyber Security in Preventing Crisis and Disaster in Jordanian Bank. Unpublished master's thesis. Hashemite University, Zarqa, Jordan. Retrieved from http://hcraes.hamudnam.moc/droceR/9768131

Santos, E., Galang, G., & Amon, M. (2023). Maritime Education and Training (MET) Cybersecurity and ISO/IEC 27001:2022 from Maritime Academy of Asia and the Pacific (MAAP) Perspectives and Traditions. *Pedagogika-Pedagogy*, 95(6s). https://doi.org/10.53656/ped2023-6s.08

Sawant, V., Vishwas, S., Giri, R., Shingote, A., & Joglekar, P. (2023). Face Recognition Based Password Encryption and Decryption System. *2023 4th International Conference for Emerging Technology (INCET)*, 1, 5. https://doi.org/10.1109/INCET57972.2023.10170090

Schoeffel, P. (2016). Taming the Beast: A Scientific Definition of FinTech. *Journal of Innovation Management*. https://doi.org/10.2139/ssrn.3097312

Sell, M., & Dupuis, M. (2023). Designing an Industrial Cybersecurity Program for an Operational Technology Group. In *Proceedings of the 24th Annual Conference on Information Technology Education* (pp. 125-130). Association for Computing Machinery. https://doi.org/10.1145/3585059.3611438

Semin, V., Grigoreva, S., & Ilyina, E. (2016). A process model of risk management in the system of management of strategic sustainability of cargo motor transport enterprises. In *IEEE Conference on Quality*. https://doi.org/10.1109/ITMQIS.2016.7751951

Shakir, A., & Vihari, N. (2022). Perception and Awareness Analysis of Financial Technology (Fintech) Services Amongst the Expatriates in the United Arab Emirates. *Journal of Information System and Technology Management*, 27(7), 63-75. https://doi.org/10.35631/jistm.727005

Shejin, T., & Sudheer, K. (2023). A review on major cyber threats and recommended countermeasures. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 3(11). https://www.ijraset.com

Siddiqui, Z., & Rivera, C. A. (2022). FinTech and FinTech ecosystem: A review of literature. Risk Governance and Control: Financial Markets & Institutions, 12(1), 63–73. https://doi.org/10.22495/rgcv12i1p5

Silvers, J. (2007). Risk Management for Meetings and Events. Routledge. https://doi.org/10.4324/9780080560731

Singh, V., & Govindarasu, M. (2020). A Novel Architecture for Attack-Resilient Wide-Area Protection and Control System in Smart Grid. In *Proceedings of the 2020 Resilience Week* (RWS). https://doi.org/10.1109/RWS50334.2020.9241291

Snopkov, V. N., Nasser, A. A., & Nasser, A. V. (2020). Neural network modeling and mathematical algorithms in the differential diagnosis of diabetic retinopathy. *Bulletin of the Southwestern State University*, 2, 1, 50-57. Retrieved from https://www.researchgate.net/publication/311675554_NEURAL_NETWORK_MODELING_AND_MATHEMATICAL_ALGORITHMS_IN_DIFFERENTIAL_DIAGNOSIS_OF_DIABETIC_RETINOPATHY

Strahilevitz, L., & Liu, L. (2022). Cash substitution and deferred consumption as data breach harms. *Public Law and Legal Theory Working Papers*. University of Chicago Law School. Retrieved from https://chicagounbound.uchicago.edu/public_law_and_legal_theory

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*. https://doi.org/10.3390/electronics11142181

Talabi, A. A., Longe, O., Muhammad, A., & Olusanya, K. (2021). Cybersecurity Risk Management in Identity Systems using Biometric-based Multimodal Authentication. In *Proceedings of the 28th iSTEAMS Intertertiary Multidisciplinary Conference*. American International University West Africa, The Gambia, 60-88. Retrieved from https://www.isteams.net/_files/ugd/185b0a_b4473ae8be3a43f7b05f23ccaa186332.pdf

Tekleselase, W. (2019). Emerging Cyber Security Threats in Organization. *International Journal of Scientific Research in Network Security and Communication*, 7(6), 7-10. Retrieved from https://www.indianjournals.com/ijor.aspx?target=paid_journals_list

Tolossa, D. (2023). Importance of cybersecurity awareness training for employees in business. *Vidya - A Journal of Gujarat*, 2(2). https://doi.org/10.47413/vidya.v2i2.206

Tuteja, A., & Shanker, R. (2022). Optimization of Snort for Extrusion and Intrusion Detection and Prevention. *International Journal of Engineering Research and Applications (IJERA)*, 2(3), 1768-1774. ISSN: 2248-9622

Udroiu, A., Dumitrache, M., & Sandu, I. (2022). Improving the cybersecurity of medical systems by applying the NIST framework. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. https://doi.org/10.1109/ecai54874.2022.9847498

Usman, A., Ayoib, C., & Abdulmalik, S. (2023). The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review. *International Journal of Professional Business Review*, 8(8), 1-11. Retrieved from https://www.semanticscholar.org/paper/f9e29b6a85555bfa38c68482c6b02296ef693220

Zhyvylo, E., & Shevchenko, D. (2022). Risk Assessment of Cyber Security and Control of Privacy in Public Administration Information Systems. *Collection of Scientific Works of the Military Institute of Kyiv National Taras Shevchenko University*. https://doi.org/10.17721/2519-481x/2022/75-07

الملاحق

ملحق 1: الاستبانة بصورتها الأولية:

تحكيم استبانة

الأستاذ الدكتور /.....المحترم

تحية طيبة... وبعد:

يقوم الباحث بدراسة عنوانها: "**متطلبات الأمن السيبراني وأثرها في حماية نظم المعلومات في البنوك اليمنية**"، كجزء من متطلبات الحصول على درجة الماجستير التنفيذي في إدارة الأعمال

ولتحقيق اهداف الدراسة تم تصميم استبانة تشمل متغيري الدراسة: **المتغير المستقل: متطلبات الأمن السيبراني متمثلة** بالأبعاد الاتية :(التنظيمية ، الفنية ، المادية ، الامتثال)، **والمتغير التابع: حماية نظم المعلومات.**

ولما عرف عنكم من خبرة علمية وتميز في مجال البحثي العلمي، فأن الباحث يتوجه اليكم بطلب تحكيم هذه الاستبانة في مدى صلاحية فقراتها، ومدى انتماء الفقرات للأبعاد الواردة تحتها.

علما ان الدراسة اعتمدت مقياس ليكرت الخماسي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة.)

شاكرين ومقدرين جميل تعاونكم ومشاركتكم في تحكيم هذه الاستبانة

الباحث/ **المشرف/**

داوود عبده أحمد سعيد الشريحي **د/ مجيب الحكيمي**

أسم المحكم	التخصص	الدرجة العلمية	جهة العمل	رقم الهاتف	التوقيع

اولا: الخصائص الديموغرافية لعينة الدراسة.

1- **النوع:**

☐ ذكر ☐ انثى

2- **العمر:**

☐ اقل من 30سنة ☐ من 30 الي اقل من 40 سنة ☐ من 40 الي اقل من 50 سنة

☐ من 50 سنة فأكثر

3- **سنوات الخبرة:**

☐ اقل من 5 سنوات ☐ من 5 الي اقل من 10 سنوات ☐ من 20 الي اقل من 30 سنة ☐ 30 سنة فأكثر

4- **المؤهل العلمي:**

☐ ثانوية عامة او اقل ☐ دبلوم عالي ☐ بكالوريوس

☐ ماجستير ☐ دكتوراه

5- **الشهادة الجامعية في تخصص:**

☐ إدارة أعمال ☐ محاسبة ☐ تمويل ومصارف

☐ تكنولوجيا المعلومات ☐ أخرى

ثانيا : المعلومات المهنية والعلمية

1. **اسم البنك** : .....

2. **عدد الدورات في مجال الأمن السيبراني**

☐ لا شيء ☐ دورة واحدة فأكثر

3. **المنصب داخل البنك:**

☐ مدير عام ☐ مدير إدارة ☐ مدير فرع

☐ موظفو تكنولوجيا المعلومات ☐ غير موظفي تكنولوجيا المعلومات ☐ آخري

الجزء الثاني: فقرات الاستبانة

اولاً: المتغير المستقل: متطلبات الأمن السيبراني

م	العبـــــــــارة	صلاحية الفقرة	ملاحظات وتعديل
	المتطلبات التنظيمية (10 أسئلة):		
1.	يقوم البنك بانتظام بتحديث سياسات الأمن السيبراني الخاصة به وفقًا للوائح التي وضعتها الهيئات والمنظمات الصناعية.		

2.	لدى البنك فريق متخصص مسؤول عن ضمان الامتثال للوائح الأمن السيبراني.
3.	يقوم البنك بتدريب الموظفين بشكل منتظمً على المتطلبات التنظيمية في مجال الأمن السيبراني.
4.	يقوم البنك بإجراء عمليات تدقيق داخلية لتقييم التزام البنك بلوائح الأمن السيبراني التنظيمية.
5.	يتخذ البنك خطة واضحة للاستجابة للحوادث ، وفقًا لما تتطلبه اللوائح.
6.	يلتزم البنك بمتطلبات إعداد التقارير الإلزامية لحوادث الأمن السيبراني.
7.	يشارك البنك بنشاط في منتديات الصناعة وورش العمل المتعلقة بلوائح الأمن السيبراني.
8.	يوضع البنك إجراءات لمعالجة عدم الامتثال للمتطلبات التنظيمية.
9.	يتعاون البنك مع السلطات التنظيمية في معالجة قضايا الأمن السيبراني.
10.	يعتبر البنك الامتثال التنظيمي جانبًا مهمًا من استراتيجية الأمن السيبراني الخاصة به.
المتطلبات الفنية (10 أسئلة):	
11.	يستخدم البنك أحدث برامج مكافحة الفيروسات ومكافحة البرامج الضارة على جميع الأنظمة.
12.	يستخدم البنك تقنيات تشفير قوية لتخزين البيانات ونقلها مثل SSL/TLS (Secure Sockets Layer/Transport Layer Security).
13.	يمتلك البنك جدران الحماية (المضيفةHost-based firewalls – الشبكية Network-based firewalls – الويب Web Application Firewalls– الحماية الآمنةSecure Firewalls) لحماية أنظمة المعلومات الخاصة به من التهديدات الخارجية.
14.	يقوم البنك بتطبيق طرق الكشف عن التسلل والوقاية لمراقبة التهديدات المحتملة والاستجابة لها.
15.	يُجري البنك تحديثات أمنية وتصحيحات منتظمة لمكونات البرامج والأجهزة.
16.	يقوم البنك بوضع إجراءات للوصول الآمن إلى أنظمة المعلومات الخاصة به.
17.	يقوم البنك بانتظام بإجراء تقييمات الضعف واختبار الاختراق على أنظمة المعلومات الخاصة به.
18.	يمتلك البنك تدابير آمنة للنسخ الاحتياطي والاسترداد للبيانات والتصميمات الهامة.

19.	يستخدم البنك تقسيم الشبكة واسطة تقنيات مثل VLANs (Virtual Local Area Networks)والتي تتيح تجزئة الشبكة إلى مجموعات مختلفة، كل منها يمكن الوصول إليها فقط من قبل المستخدمين المصرح لهم بذلك للحد من التأثير المحتمل للاختراق الأمني.
20.	يمتلك البنك التكوين الآمن ومتوافقة مع معايير الأمان المعتمدة والإدارة لجميع أجهزة وأنظمة الشبكة الخاصة به كالمعايير الدولية ISO – 27001) ,NIS)
الامتثال للأطر والمعايير الدولية (10 أسئلة):	
21.	يطبق البنك معايير الأمن السيبراني الدولية، مثل ISO 27001 أو NIST.
22.	يعمل البنك على مواءمة ممارسات الأمن السيبراني مع المعايير المعترف بها دوليًا.
23.	يقوم البنك بمراجعة وتحديث سياسات الأمن السيبراني الخاصة به بانتظام لتلبية المعايير الدولية.
24.	يخصص البنك موارد لضمان الامتثال لمعايير الأمن السيبراني الدولية.
25.	يستخدم البنك الأطر والمعايير الدولية لعمليات تقييم المخاطر وإدارتها.
26.	يتلقى موظفو البنك تدريبًا على أطر ومعايير الأمن السيبراني الدولية.
27.	يشارك البنك في منتديات أو مؤتمرات الأمن السيبراني الدولية للبقاء على اطلاع بأفضل الممارسات.
28.	يقوم البنك بقياس ممارسات الأمن السيبراني الخاصة به مقابل نظرائه في الصناعة والمعايير الدولية.
29.	يستخدم البنك شهادات معترف بها دوليًا للتحقق من قدرات الأمن السيبراني الخاصة به.
30.	يسعى البنك باستمرار لتحسين وضع الأمن السيبراني من خلال التعلم من أفضل الممارسات العالمية.
تدابير الأمن المادي (10 أسئلة):	
31.	يقوم البنك بتطبيق أنظمة التحكم في الوصول لتقييد الدخول غير المصرح به إلى المناطق الحساسة.
32.	يستخدم البنك أنظمة المراقبة مثل كاميرات CCTV لمراقبة مرافقه.
33.	ينشئ البنك غرف خوادم آمنة مع ضوابط بيئية لحماية أنظمته.
34.	لدى البنك نظام إدارة الزوار لتتبع ومراقبة الزوار الخارجيين.
35.	لدى البنك إجراءات أمنية للحماية من السرقة المادية للأجهزة أو البيانات.
36.	يقوم البنك بإجراء عمليات تدقيق أمنية منتظمة لتقييم فعالية تدابير الأمن المادي الخاصة به.

37.	يتلقى موظفو البنك تدريبًا على أهمية الحفاظ على الأمن المادي.
38.	لدى البنك سياسة واضحة للتعامل مع المستندات المادية الحساسة والتخلص منها.
39.	يمتلك البنك خطة طوارئ لحوادث الأمن المادي مثل السرقة أو التخريب.
40.	تضع إدارة البنك تدابير الأمن المادي جزءًا لا يتجزأ من استراتيجية الأمن السيبراني الخاصة بها.
المتغير التابع: حماية سرية نظم المعلومات	
النزاهة (3 أسئلة):	
41.	يقوم البنك بتنفيذ تدابير لعمليات التحقق والتدقيق والمراجعة الدورية للبيانات، وتحديثها عند الحاجة لضمان الدقة والاتساق.
42.	يقوم البنك بالتحقق المنتظم من صحة البيانات والتحقق من النزاهة على أنظمة المعلومات الخاصة به.
43.	يمتلك البنك سياسة محددة لاكتشاف الأخطاء التي قد تظهر في البيانات، ويتخذ إجراءات فورية لتصحيحها.
44.	يقوم البنك بإجراء عمليات تدقيق دورية شاملة لضمان دقة ونزاهة البيانات في أنظمة المعلومات.
45.	يطبق البنك ضوابط فعالة للتأكد من أن البيانات المسجلة في النظام دقيقة وحديثة وكاملة.
التوفر (3 أسئلة):	
46.	يتخذ البنك تدابير لضمان استمرارية توافر لأنظمة المعلومات الخاصة به من خلال توفير الصيانة الدورية والتحديثات واستخدام الحلول لضمان استمرار خدماته بشكل مستمر
47.	يراقب البنك أنظمته بشكل استباقي بحثًا عن المشكلات المحتملة التي تؤثر على التوافر.
48.	لدى البنك خطة للتعافي من الكوارث لاستعادة توفر النظام في حالة وقوع حادث.
49.	يمتلك البنك نظام إدارة الطاقة الاحتياطية والتمويل الكافي لدعم استمرارية أنظمة المعلومات.
50.	يستثمر البنك باستمرار في بنيته الأساسية لتكنولوجيا المعلومات لتعزيز قدرة أنظمته على التحمل والتوفر.
المصادقة (3 أسئلة):	
51.	يفرض البنك شروطا صارمة على المستخدمين لإنشاء كلمات مرور قوية وفريدة للوصول إلى أنظمة المعلومات الخاصة به للحفاظ على أمان الأنظمة وحمايتها من الاختراقات

52.	يستخدم البنك المصادقة متعددة العوامل (Multi-Factor Authentication) للوصول إلى الأنظمة والبيانات الحساسة.
53.	يقوم البنك بمراجعة وتحديث آليات المصادقة الخاصة به بانتظام لضمان فعاليتها.
54.	تتطلب سياسات البنك تغيير كلمات المرور بشكل دوري لجميع المستخدمين.
55.	يقوم البنك بإجراء عمليات اختبار اختراق لبيئات وسيناريوهات محددة للتأكد من قوة آليات المصادقة لديه.
التفويض (3 أسئلة):	
56.	يتخذ البنك نظام تحكم في الوصول قائم على الأدوار كنظام (Role-Based Access Control) لإدارة أذونات المستخدم حسب مستوى وظيفتهم ومسؤولياتهم
57.	يقوم البنك بمراجعة وتحديث صلاحيات الوصول للمستخدمين بانتظام لضمان توافقها مع وظائف الوظيفة.
58.	يتخذ البنك إجراءات لإلغاء صلاحيات الوصول الخاصة بالموظفين الذين يغادرون الشركة أو يتغيرون في أدوارهم.
59.	يحدد البنك سياسات واضحة لتخويل وإلغاء تخويل المستخدمين للوصول إلى أنظمة المعلومات والبيانات.
60.	يقوم البنك بإجراء مراجعات دورية لجميع حسابات المستخدمين وصلاحيات الوصول لديهم لضمان اتساقها مع أدوارهم الوظيفية الحالية.

ملحق 2: أسماء محكمي الاستبيان

الاسم	الدرجة العلمية	التخصص	مكان العمل
د. عبد الرقيب السماوي	أستاذ دكتور	إدارة أعمال	جامعة تعز
د. محمد نعمان محمد عقلان	أستاذ مشارك	إدارة أعمال	جامعة تعز
د. بسام سلطان السبئ	أستاذ مساعد	المحاسبة والمراجعة	الجهاز المركزي
د. رضوان محمد النخلاني	أستاذ مشارك	حماية الأنترنت	جامعة إب كلية الهندسة
د. صبري سعيد محمد الشيباني	أستاذ مساعد	شبكات وحاسبات جامعة	جامعة الجند
د. خالد شمسان اسماعيل	أستاذ مساعد	إدارة مالية	المعهد الوطني للعلوم الادارية
د. نشوان المجمر	أستاذ مشارك	تقنية معلومات	جامعة الجزيرة

ملحق 3: الاستبانة بصورتها النهائية

الجزء الأول: البيانات الديموغرافية

1. **الاسم: .... اختياري**

1- **المؤهل العلمي:**

☐ ثانوية عامة او اقل ☐ دبلوم عالي

☐ بكالوريوس ☐ ماجستير ☐ دكتورا ه

2- **التخصص:**

☐ **شبكات** ☐ **تكنولوجيا معلومات**

☐ **مالية ومصرفية** ☐ **إدارة اعمال** ☐ **محاسبة**

☐ **غيرذلك**

2. **البنك الذي تعمل فيه: .....**

3. **نوع البنك:**

☐ حكومي ☐ تجاري

☐ إسلامي

4. **المسمى الوظيفي:**

☐ الإدارة العليا ☐ مدير ادارة

☐ نائب مدير فرع ☐ رئيس قسم ☐ موظف

3- **سنوات الخبرة:**

☐ اقل من 5 سنوات ☐ من 5 الي اقل من 10 سنوات ☐ من 20 الي 30 سنة

☐ 30 سنة فأكثر

5. **عدد الدورات في مجال الأمن السيبران ي**

☐ دورة ☐ دورتين ☐ ثلاث فأكثر ☐ لا شي

الجزء الثاني: فقرات الاستبانة

م	العبـــــــــــــــارة	درجة الموافقة				
		موافق بشدة	موافق	موافق الى حد ما	غير موافق	موافق غير بشدة
	المتغير المستقل: متطلبات الأمن السيبراني **المتطلبات التنظيمية 10 أسئلة**					
1.	يقوم البنك بانتظام بتحديث سياسات الأمن السيبراني الخاصة به وفقًا للوائح التي وضعتها الهيئات والمنظمات الدولية.					
2.	لدى البنك فريق م تخصص مسؤول عن ضمان الامتثال للوائح الأمن السيبراني.					
3.	يقوم البنك بتدريب الموظفين بشكل منتظمً على المتطلبات التنظيمية في مجال الأمن السيبراني.					
4.	يقوم فريق المراجعة الخارجي بإجراء عمليات تدقيق داخلية لتقييم التزام البنك بلوائح الأمن السيبراني التنظيمية.					
5.	يتخذ البنك خطة واضحة للاستجابة للحوادث، وفقًا لما تتطلبه اللوائح.					
6.	يلتزم البنك بمتطلبات إعداد التقارير الإلزامية لحوادث الأمن السيبراني.					
7.	حضور البنك منتديات الصناعة وورش العمل المتعلقة بلوائح الأمن السيبراني داخليا وخارجيا.					
8.	يتخذ البنك إجراءات صارمة وحازمة لمعالجة عدم الامتثال للمتطلبات التنظيمية.					
9.	يتعاون البنك مع السلطات التنظيمية في معالجة قضايا ا لأمن السيبراني.					
10	يعتمد البنك الامتثال التنظيمي جانبًا مهمًا من استراتيجية الأمن السيبراني الخاصة به.					
	البعد الثاني: المتطلبات الفنية 10 أسئلة	موافق بشدة	موافق	موافق الى حد ما	غير موافق	موافق غير بشدة
11.	يستخدم البنك أحدث برامج الحماية وبرامج مكافحة الفيروسات والبرامج الضارة على جميع الأنظمة.					
12.	يعتمد البنك على تقنيات تشفير قوية مثلSSL/TLS Secure Sockets Layer/Transport Layer Security)(لتشفير الاتصالات بين العميل والخادم.					

13. يمتلك البنك الجيل التالي من جدران الحماية لحماية أنظمة المعلومات الخاصة به من التهديدات الخارجية.
14. يعتمد البنك على تقنيات متقدمة للكشف عن التسلل والوقاية منه، مثل أنظمة الكشف عن التسلل **(IDS)** وأنظمة منع التسلل**(IPS)** ، لمراقبة التهديدات المحتملة والتعامل معها بفعالية.
15. يُجري البنك تحديثات أمني ة وتصحيحات منتظمة لمكونات البرامج والأجهزة.
16. يقوم البنك بوضع إجراءات للوصول الأمن إلى أنظمة المعلومات الخاصة ب هـ.
17. يقوم البنك بانتظام بإجراء تقييمات الضعف واختبار الاختراق على أنظمة المعلومات الخاصة به.
18. يمتلك البنك تدابير آمنة وسريعة للنسخ الاحتياطي بشكل آلي للبيانات وإمكانية البيانات والتصميمات الهامة في أي لحظة.
19. يستخدم البنك الشبكات الافتراضية مثل **VLANs (Virtual Local Area Networks)** والتي تتيح تجزئة الشبكة الى مجموعة من الشبكات ذات صلاحيات مختلفة كل منها يمكن الوصول إليها فقط من قبل المستخدمين المصرح لهم بذلك للحد من التأثير المحتمل للاختراق الأمني.

الامتثال للأطر والمعايير الدولية 10 أسئلة	موافق بشدة	موافق	حد ما	موافق الى	غير موافق	موافق غير بشدة
20. يطبق البنك معايير الأمن السيبراني الدولية كمعيار ISFاوصناعة بطاقات الدفع ومعيار أمان البيانات PCI/DSSNotللتخزين. مثل ISO 27001أو NIST.						
21. يعمل البنك على مواءمة ممارسات الأمن السيبراني مع المعايير المعترف بها دوليًا.						
22. يقوم البنك بمراجعة وتحديث سياسات الأمن السيبراني الخاصة به بانتظام تلبية المعايير الدولية.						
23. يخصص البنك موارد لضمان الامتثال لمعايير الأمن السيبراني الدولية.						
24. يستخدم البنك الأطر والمعايير الدولية لعمليات تقييم المخاطر وإدارتها.						
25. يتلقى موظفو البنك تدريبًا على أطر ومعايير الأمن السيبراني الدولية.						
26. يشارك البنك في منتديات أو مؤتمرات الأمن السيبراني الدولية للبقاء على اطلاع بأفضل الممارسات.						
27. يقوم البنك بقياس ممارسات الأمن السيبراني الخاصة به مقابل نظرائه في الصناعة والمعايير الدولية.						

يستخدم البنك شهادات معترف بها دوليًا للتحقق من قدرات الأمن السيبراني
28. لخاصة به.

يسعى البنك إلى تطوير استراتيجياته الخاصة لضمان أمن المؤسسة بما لا
29. يتعارض مع المعايير الدولي ة.

تدابير الأمن المادي 10 أسئلة	موافق بشدة	موافق	موافق الى حد ما	غير موافق	موافق غير بشدة
يقوم البنك بتطبيق أنظمة التحكم في الوصول لتقييد الدخول غير المصرح به 30. إلى الأنظمة الأكثر حساسية.					
ينش ئ البنك غرف خوادم مؤمنة تحتوي على ضوابط بيئية لحماية أنظمته، 31. كما يعتمد على أنظمة مر اقبة مثل كاميرات **CCTV**لتأمين مرافقه بشكل فعّال.					
32. لدى للبنك نظام إدارة زوار متقدم يسهم في رصد وتأمين العناصر الخارجية، ويحمي الموارد المادية والمعلوماتية من مخاطر السرقة.					
33. يقوم البنك بإجراء عمليات تدقيق أمنية منتظمة لتقييم فعالية تدابير الأمن المادي الخاصة به.					
34. يتلقى موظفو البنك دورات تدريبية دوري ة متكررة حول أهمية تعزيز الأمن المادي والحفاظ عليه.					
35. لدى البنك سياسة واضحة للتعامل مع المستندات المادية الحساسة والتخلص منها.					
36. يمتلك البنك خطة طوارئ لحوادث الأمن المادي مثل السرقة أو التخريب.					
37. تضع إدارة البنك تدابير الأمن المادي جزءًا لا يتجزأ من استراتيجية الأمن السيبراني الخاصة بها.					

2- المتغير التابع: حماية سرية نظم المعلومات	موافق بشدة	موافق	موافق الى حد ما	غير موافق	موافق غير بشدة
38 يقوم البنك بتنفيذ تدابير لعمليات التحقق والتدقيق والمراجعة الدورية للبيانات، وتحديثها عند الحاجة.					
39. يمتلك البنك سياسة أمنية لاكتشاف الأخطاء التي قد تظهر في البيانات ويتخذ إجراءات فورية لتصحيحها.					
40. يطبق البنك ضوابط فعالة للتأكد من أن البيانات المسجلة في النظام دقيقة وحديثة وكاملة.					

41. يتخذ البنك تدابير أمنية لضمان استمرارية توافر أ نظمة المعلومات الخاصة بهمن خلال توفير الصيانة الدورية والتحديثات واستخدام الحل الأمثل لضمان تو افر خدماته بشكل مستمر
42. يجر ي البنك المراقبة الدورية للأنظمة استباقياً بحثًا عن المشكلات المحتملة للحفاظ على التوافرية.
43. لدى البنك خطة تعافي من الكوارث في حالة حدوثها واستعادة تو افر النظام في حالة وقوع حادث.
44. يمتلك البنك نظام إدارة الطاقة الاحتياطية والتمويل الكافي لدعم استمرارية وتوافريه أنظمة المعلومات.
45. يخص البنك موارد مالية وتقنية وبشرية لتطوير وتحسين بنيته الأساسية لتكنولوجيا المعلومات.
46. يفرض البنك شروطا صارمة على المستخدمين لإنشاء كلمات مرور قوية وفريدة للوصول إلى أنظمة المعلومات الخاصة به للحفاظ على أمان الأنظمة وحمايتها من الاختر اقات
47. يستخدم البنك المصادقة متعددة (العوامل) للوصول إلى الأنظمة والبيانات الحساسة.
48. يقوم البنك بمراجعة وتحديث آليات المصادقة الخاصة به بانتظام لضمان فعاليتها.
49. يقوم البنك بفرض تغيير كلمات المرور بشكل دوري لجميع المستخدمين.
50. يقوم البنك بإجراء عمليات اختبار اختراق لبيئات وسيناريوهات محددة للتأكد من قوة آليات المصادقة لديه.
51. يتخذ البنك نظام تحكم في الوصول قائم على الأدوار كنظام (Role-Based Access Control) لإدارة أذونات المستخدم حسب مستوى وظيفتهم ومسؤولياته م
52. يتخذ البنك إجراءات لإلغاء صلاحيات الوصول الخاصة بالموظفين الذين يغادرون البنك أو يتغيرون في أدوارهم.
53. يحدد البنك سياسات واضحة لت خويل وإلغاء تخويل المستخدمين للوصول إلى أنظمة المعلومات والبيانات.

ملحق 4 : الاختصارات

1. AVE: متوسط الاختلاف المستخرج (Average Variance Extracted).
2. BSI: المعهد البريطاني للمعايير (British Standards Institution).
3. CI: البنية التحتية الحرجة (Critical Infrastructure).
4. CR: الثقة المركبة (Composite Reliability).
5. CS: الأمان السيبراني (Cyber Security).
6. CSF: الإطار الأمني السيبراني (Cybersecurity Framework).
7. DLP: منع فقدان البيانات (Data Loss Prevention).
8. DSS: قد يشير إلى معيار الأمان لبطاقات الدفع (Payment Card Industry Data Security Standard).
9. F2: حجم التأثير (Effect Size).
10. GDPR: اللائحة العامة لحماية البيانات (General Data Protection Regulation).
11. GOF: معيار الجودة (Goodness of Fit).
12. HIDS: نظام الكشف عن الاختراقات المضيف (Host Intrusion Detection System).
13. HSBC: البنك الهونغ كونغ وشنغهاي المحدود (Hongkong and Shanghai Banking Corporation Limited).
14. IAM: إدارة الهويات والوصول (Identity and Access Management).
15. IDPS: نظام الوقاية/الكشف عن الاختراقات (Intrusion Detection and Prevention System).
16. IEC: اللجنة الكهروتقنية الدولية (International Electrotechnical Commission).
17. IS: نظم المعلومات (Information Systems).
18. ISMS: نظام إدارة أمان المعلومات (Information Security Management System).
19. ISO: المنظمة الدولية للمعايير (International Organization for Standardization).

20. IT: تقنية المعلومات (Information Technology).
21. KMO: مقياس كايزر-ماير-أولكين (Kaiser-Meyer-Olkin Measure).
22. NIDS: نظام الكشف عن الاختراقات الشبكي (Network Intrusion Detection System).
23. NIST: المعهد الوطني للمعايير والتقنية (National Institute of Standards and Technology).
24. PCI: معايير أمان الصناعة لبطاقات الدفع (Payment Card Industry Security Standards).
25. PLS: الأقل مربعات جزئية (Partial Least Squares).
26. R2: معامل التحديد (Coefficient of Determination).
27. SEM: النمذجة بالمعادلة الهيكلية (Structural Equation Modeling).
28. SIEM: إدارة المعلومات الأمنية وإدارة الأحداث (Security Information and Event Management).
29. SOGP: قد يشير إلى ممارسات العمليات الأمنية (Security Operations Good Practices).
30. SOC: مركز عمليات الأمان (Security Operations Center).
31. SPSS: الحزمة الإحصائية للعلوم الاجتماعية (Statistical Package for the Social Sciences).
32. SRMR: الجذر المتوسط المربع المعياري للبقايا (Standardized Root Mean Square Residual).
33. SSL: طبقة المقابس الآمنة (Secure Sockets Layer).

Abstract

"The Impact of Cybersecurity Requirements on the Protection of Information Systems in Yemeni Banks"

This study aimed to identify the impact of the availability of cybersecurity requirements (regulatory, technical, compliance with international frameworks and standards, physical) on protecting information systems in the Yemeni banking sector. The study population included (15) Yemeni banks during the period from July to September 2023. Data were collected using a questionnaire distributed to a random sample of 250 employees in bank branches (governmental, Islamic, and commercial) in the governorates of Taiz and Aden. The study employed a descriptive methodology, supplemented by various statistical analyses to process the data.

The results of the study demonstrated a significant positive relationship between cybersecurity requirements and the protection of information systems in the examined banks. There were also substantial differences in responses based on demographic variables such as the nature of the bank, educational level, and job position. The study recommends the necessity of enhancing training and compliance with international standards, improving physical security, updating protection programs, and managing passwords. It also highlights the importance of offering specialized training, encouraging collaboration among banks, developing plans for responding to cyber incidents, and conducting regular security assessments.

Keywords: Cybersecurity requirements, Information systems protection , Yemeni banks

Taiz University
Vice-Rectorate of Graduate Studies and Scientific Research
Graduate Studies Center
Executive Department of Business
Administration Master's Program

Master's thesis entitled.

Cybersecurity requirements and their impact on protecting information systems in Yemeni banks.

This thesis was submitted to complete the requirements for obtaining an executive master's degree in administrative sciences.

Executive Business Administration Major

Student Preparation:

Dawood Abdo Ahmed Saeed Al - Shuraihi

Supervision:

Associate Professor of Information Technology

Dr. Mujeeb Abdulhakim Al-Hakimi

Academic Year (1445 AH / 2024 AD)