

—دولة ليبيا

وزارة التعليم العالي والبحث العلمي



إدارة الدراسات العليا والتدريب بالجامعة

كلية الاقتصاد / قسم المحاسبة

دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر

الأمن السيبراني

دراسة ميدانية على شركات الاتصالات الليبية

قدمت الرسالة استكمالاً لمتطلبات الحصول على درجة الإجازة العالية (الماجستير) في

المحاسبة

إعداد الطالب:

محمد أحمد عبد الحفيظ النايض

بكالوريوس محاسبة : كلية الاقتصاد – جامعة غريان

رقم القيد: 5213028024

إشراف الدكتور:

خليفة إبراهيم ميلاد

أستاذ المحاسبة المشارك جامعة الزاوية

للعام الجامعي 2026م

الآية القرآنية

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿يَرْفَعُ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ﴾

سورة المجادلة/ جزء من الآية "11"

الإهداء

إلى والديَّ الكريمين،
، جزاهما الله عني خير الجزاء.،،
شكرًا لصبركم ودعمكم وتشجيعكم المستمرّ، جعل الله أيامكم سعادة
ورضًا.

،

أسأل الله أن يحفظكم ويبارك فيكم ويجعلكم من الصالحين النافعين.
إلى إخوتي الأعزاء،
جزاكم الله عني خيرًا على ما قدّمتم من محبةٍ ومساندةٍ ودعاء،
فأنتم السند بعد الله في كلّ خطوة.
إلى أصدقائي الأوفياء،
من شاركوني الطّريق بالكلمة الطّيبة والموقف الصّادق،
دمتم زادًا للروح وبلسمًا في أوقات العناء.
إلى كلّ هؤلاء،
أهدي ثمرة جهدي المتواضع، عرفانًا بالجميل ووفاءً للمحبّة.

الشكر والتقدير

أولاً وقبل كل شيء ، أحمّد الله وأشكره على ما منّ به عليّ من توفيقٍ وتسديدٍ لإنجاز هذا العمل المتواضع ، وأسأله سبحانه أن يجعله خالصاً لوجهه الكريم .
وبعد...

يسعدني أن أتقدّم بخالص الشّكر وعظيم الامتنان إلى أستاذي الفاضل الدكتور: خليفة إبراهيم ميلاد، على إشرافه الكريم، وتوجيهاته السّديدة، ومتابعته المستمرة التي كان لها الأثر البالغ في إخراج هذا العمل إلى صورته النّهائية، فجزاه الله عني خير الجزاء ، وبارك له في علمه وعمره.

كما أتوجّه بخالص الشكر والتقدير إلى الأساتذة الأجلاء الذين تقضّوا بتحكيم أداة الدّراسة (الاستبانة)، وما قدّموه من ملاحظات ببناء أسهمت في إثراء هذا البحث وصقله علمياً .
ولا يفوتني أن أعبر عن جزيل شكري وتقديري للأساتذة الأفاضل أعضاء لجنة المناقشة الموقّرين، على تفضّلهم بقراءة هذه الرسالة وتقييمها، وعلى ما أبدوه من ملاحظات قيّمة أسهمت في تطوير مضمونها.

كما أتقدّم بالشكر والعرفان لكلّ من قدّم لي يد العون والمساندة، من زملاء وأصدقاء، سواء بكلمة طيبة أو دعوة صادقة، في سبيل إنجاز هذا العمل وإتمامه.

جزاكم الله عني جميعاً خير الجزاء

الباحث

محمد أحمد عبد الحفيظ النايض

مستخلص الدراسة

هدفت الدراسة إلى التعرف على دور الاتجاهات الحديثة للمراجعة الداخلية قي الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية، من خلال التركيز على ثلاث أبعاد رئيسية هي: إدارة المخاطر، الدور الحوكمي، إضافة قيمة للمراجعة. وتتبع أهمية الدراسة من تصاعد التهديدات السيبرانية في بيئة الأعمال الرقمية، وما تفرضه من تحديات على المؤسسات التي تعتمد على الأنظمة الإلكترونية في إدارة بياناتها وعملياتها، لاسيما شركات الاتصالات التي تتعامل مع معلومات حساسة وحيوية.

اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم جمع البيانات الأولية باستخدام استبانة وزعت على عينة من العاملين في شركات الاتصالات الليبية محل الدراسة. كما استندت الدراسة في بنائها النظري إلى عدد من الدراسات العربية والأجنبية ذات الصلة بموضوع المراجعة الداخلية والأمن السيبراني.

وتوصلت الدراسة إلى وجود دور ذو دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني، كما أظهرت النتائج وجود دور معنوي لكل من إدارة المخاطر، والدور الحوكمي، إضافة قيمة للمراجعة في تعزيز قدرة شركات الاتصالات على مواجهة التهديدات السيبرانية والحد من اثارها. وبينت النتائج أيضا أن تطوير المراجعة الداخلية وتفعيل أدوارها الحديثة من شأنه أن يسهم في تحسين بيئة الرقابة الداخلية، ورفع مستوى الشفافية، ودعم اتخاذ القرارات، وتعزيز حماية المعلومات والأصول الرقمية.

وأوصت الدراسة بضرورة دعم إدارات المراجعة الداخلية في شركات الاتصالات الليبية، وتوفير برامج تدريبية متخصصة في الأمن السيبراني، وتعزيز التكامل بين المراجعة الداخلية وإدارة تقنية المعلومات، إلى جانب تطوير الأطر الرقابية والحكومية بما يواكب التطورات التقنية والمخاطر الرقمية المتجددة.

الكلمات المفتاحية: المراجعة الداخلية، الاتجاهات الحديثة، الأمن السيبراني، شركات الاتصالات الليبية .

Abstract:

This study aimed to identify the role of modern internal audit trends in reducing cybersecurity risks in Libyan telecommunications companies in Tripoli, focusing on three main dimensions: risk management, corporate governance, and value-added auditing. The importance of the study stems from the increasing cyber threats in the digital business environment and the challenges they pose to institutions that rely on electronic systems in managing their data and operations, especially telecommunications companies that handle sensitive and vital information.

The study adopted the descriptive analytical approach. Primary data were collected through a questionnaire distributed to a sample of employees working in the selected Libyan telecommunications companies. The theoretical framework of the study was also based on a number of relevant Arabic and foreign studies in the fields of internal auditing and cybersecurity.

The study found that modern internal audit trends have a statistically significant role in reducing cybersecurity risks. The results also showed a significant role for each of risk management, corporate governance, and value-added auditing in enhancing the ability of telecommunications companies to confront cyber threats and reduce their effects. In addition, the findings indicated that developing internal auditing and activating its modern roles can contribute to improving the internal control environment, increasing transparency, supporting decision-making, and strengthening the protection of information and digital assets.

The study recommended supporting internal audit departments in Libyan telecommunications companies, providing specialized training programs in cybersecurity, enhancing integration between internal audit and information technology departments, and developing regulatory and governance frameworks in line with technological developments and emerging digital risks.

Keywords: Internal Auditing, Modern Trends, Cybersecurity, Risk Management, Corporate Governance, Libyan Telecommunications Companies.

قائمة محتويات الدراسة

الصفحة	الموضوع
ب	الآية القرآنية
ج	الإهداء
د	شكر وتقدير
هـ	مستخلص الدراسة
و	:ABSTRACT
ز	قائمة محتويات الدراسة
ي	قائمة الجداول
ك	فهرس الأشكال
1	الفصل الأول الإطار العام للدراسة
2	1- المقدمة:
3	2 - الدراسات السابقة:
14	التشابه والاختلاف بين الدراسات السابقة والدراسة الحالية
16	3- ما يميز هذه الدراسة عن الدراسات السابقة:
17	مشكلة الدراسة:
18	4- أهداف الدراسة:
18	5- أهمية الدراسة:
19	6- فرضيات الدراسة:
19	7- أسلوب جمع وتحليل البيانات:
19	أسلوب جمع البيانات:
20	8- مجتمع وعينة الدراسة:

21	9- نموذج الدراسة:
21	10- حدود الدراسة:
22	11- مصطلحات الدراسة:
24	الفصل الثاني: الإطار النظري والدراسات السابقة
25	المبحث الأول: المراجعة الداخلية
26	المبحث الأول: المراجعة الداخلية
26	تمهيد:
26	1.2.1. مفهوم المراجعة الداخلية
27	1.2.2: مراحل التطور الزمني للمراجعة الداخلية
29	1.2.3: أهداف المراجعة الداخلية:
31	1.2.4. أهمية المراجعة الداخلية:
33	1.2.5: أنواع المراجعة الداخلية:
34	1.2.6: وظائف المراجعة الداخلية:
34	1.2.7: مقومات المراجعة الداخلية
36	المبحث الثاني: الاتجاهات الحديثة للمراجعة الداخلية
36	تمهيد:
37	2.2.1: إدارة المخاطر كاتجاه حديث للمراجعة الداخلية:
38	2.2.1.: مفهوم إدارة المخاطر
39	2.2.2.: أهداف إدارة المخاطر:
40	2.2.3.: أهمية إدارة المخاطر
41	2.2.4.: أنواع إدارة المخاطر:
41	2.2.5.: المقومات الأساسية لإدارة مخاطر المنشأة
42	2.2.6.: منهجية إدارة المخاطر:
42	2.2.7.: التعامل مع المخاطر
43	2.2.8.: العوامل المؤثرة على دور المراجعة الداخلية في عملية إدارة المخاطر:

43	2.2.9.: دور المراجعة الداخلية في إدارة المخاطر كأحد الاتجاهات الحديثة للمراجعة الداخلية
45	3.2.1المبحث الثالث: الحوكمة كاتجاه حديث للمراجعة الداخلية
45	3.2.1.: مفهوم الحوكمة
46	3.2.2.: أهداف حوكمة الشركات
46	3.2.3.: أهمية حوكمة الشركات
47	3.2.4: أسباب وجود الحوكمة:
48	3.2.3.1: إضافة القيمة كاتجاه حديث للمراجعة الداخلية
48	3.2.3.2: مفهوم إضافة القيمة
49	3.2.3.3: مؤشرات إضافة المراجعة الداخلية قيمة للمنشأة
50	3.2.3.4: دور المراجعة الداخلية في إضافة قيمة للمنشأة
50	3.2.3.5: مقومات إضافة القيمة
51	الفصل الثالث: الأمن السيبراني
53	1.3: المبحث الأول: ماهية الأمن السيبراني
53	تمهيد:
54	1.3.1: مفهوم الأمن السيبراني:
57	1.3.2: المفاهيم المرتبطة بالأمن السيبراني:
58	1.3.3: أهداف الأمن السيبراني:
58	1.3.4: أهمية الأمن السيبراني:
59	1.3.5: أهمية دراسة الأمن السيبراني:
59	1.3.6: أهم المسارات الوظيفية المتاحة بعد دراسة الأمن السيبراني:
60	1.3.7: خصائص الأمن السيبراني:
61	1.3.8: أنماط الأمن السيبراني:
62	1.3.9: عناصر الأمن السيبراني
63	2.3: المبحث الثاني: إدارة مخاطر الأمن السيبراني:

64	2.3.1: المخاطر التي تهدد الأمن السيبراني:
65	2.3.2: أنواع مخاطر الأمن السيبراني:
66	2.3.3: أنواع الجرائم السيبرانية:
67	2.3.4: أسباب الجرائم السيبرانية:
67	2.3.5: أبعاد الأمن السيبراني
68	2.3.6: آليات (متطلبات) تحقيق الأمن السيبراني
69	2.3.7: أهمية الرقابة في تعزيز تدابير الأمن السيبراني:
70	3.3المبحث الثالث: محددات جودة العلاقة بين المراجعة الداخلية والأمن السيبراني:
74	3.3تحليل العلاقة بين جودة المراجعة الداخلية المستخدمة في الحد من مخاطر الأمن السيبراني وتأثير ذلك على ترشيد قرارات المستثمرين:
75	الفصل الرابع: الدراسة الميدانية
76	تمهيد
76	المبحث الأول/ الإجراءات المنهجية المتبعة في الدراسة
76	أولاً: نبذة مختصرة عن شركات الاتصالات قيد الدراسة.
78	ثانياً: منهجية الدراسة
83	ثالثاً: ثبات أداء الدراسة (الاستبانة)
84	رابعاً: الأساليب الإحصائية المستخدمة في تحليل البيانات الأولية:
85	المبحث الثاني: عرض البيانات الأولية للدراسة واختبار فرضيات الدراسة
85	أولاً: وصف الخصائص
91	ثانياً: وصف متغيرات الدراسة
97	ثالثاً: اختبار فرضيات الدراسة
103	ثانياً- مناقشة النتائج
107	المبحث الثالث: النتائج والتوصيات
107	أولاً- النتائج
108	ثانياً: التوصيات

109	مقترحات دراسات مستقبلية:
110	قائمة المصادر والمراجع
121	الملاحق

قائمة الجداول

الصفحة	عنوان الجدول
29	جدول رقم (1) مراحل تطور المراجعة الداخلية
78	جدول رقم (2) حركة توزيع الاستبانة على أفراد العينة
79	جدول رقم (3) محتوى الاستبانة
79	جدول رقم (4) مقياس ليكرت الخماسي
80	جدول رقم (5) تحديد الإجابات وفق مقياس ليكرت الخماسي
81	جدول رقم (6) معامل الارتباط بين كل فقرة من فقرات إدارة المخاطر والدرجة الكلية
82	جدول رقم (7) معامل الارتباط بين كل فقرة من فقرات حوكمة الشركات والدرجة الكلية
83	جدول رقم (8) معامل الارتباط بين كل فقرة من فقرات إضافة قيمة للمراجعة والدرجة الكلية
84	جدول رقم (9) معاملات الثبات لمتغيرات الدراسة
85	الجدول رقم (10) التوزيع التكراري لمفردات عينة الدراسة حسب المؤهل العلمي
86	الجدول رقم (11) التوزيع التكراري لمفردات عينة الدراسة حسب التخصص العلمي
87	الجدول رقم (12) يبين التوزيع التكراري لمفردات عينة الدراسة حسب سنوات الخبرة
88	الجدول رقم (13) يبين التوزيع التكراري لمفردات عينة الدراسة المسمى الوظيفي
89	الجدول رقم (14) التوزيع التكراري لمفردات عينة الدراسة حسب الدورات التدريبية
90	الجدول رقم (15) يبين التوزيع التكراري لمفردات عينة الدراسة حسب مجال الدورات التدريبية
91	الجدول رقم (16) المتوسط الحسابي والانحراف المعياري لفقرات إدارة المخاطر

الصفحة	عنوان الجدول
93	الجدول رقم (17) المتوسط الحسابي والانحراف المعياري لفقرات حوكمة الشركات
95	الجدول رقم (18) المتوسط الحسابي والانحراف المعياري لفقرات إضافة قيمة للمراجعة
98	جدول رقم (19) اختبار T للمحور الأول
98	جدول رقم (20) اختبار T للمحور الأول
100	جدول رقم (21) اختبار T للمحور الثاني
101	جدول رقم (22) اختبار T للمحور الثالث

فهرس الأشكال

الصفحة	عنوان الشكل
21	شكل (1) يوضح أنموذج الدراسة
85	الشكل رقم (2) التوزيع التكراري لمفردات عينة الدراسة حسب المؤهل العلمي
86	الشكل رقم (3) التوزيع التكراري لمفردات عينة الدراسة حسب التخصص العلمي
87	الشكل رقم (4) التوزيع التكراري لمفردات عينة الدراسة حسب سنوات الخبرة
88	الشكل رقم (5) التوزيع التكراري لمفردات عينة الدراسة حسب المسمى الوظيفي
89	الشكل رقم (6) التوزيع التكراري لمفردات عينة الدراسة حسب عدد الدورات التدريبية
90	الشكل رقم (7) التوزيع التكراري لمفردات عينة الدراسة حسب مجال الدورات التدريبية

الفصل الأول

الإطار العام للدراسة

1-المقدمة:

الأمن والاستقرار عنصران ضروريان في الحياة لابد منة توفيرهما حتى تتمكن الدولة من الارتقاء بنفسها وبمواطنيها، إن الأمن والخوف نقيضان لا يجتمعان، وقد ذكر الله تعالى أهمية الأمن للناس في كثير من الآيات القرآنية منها قوله تعالى: (وإذ جعلنا البيت مثابة للناس وأمناً). سورة البقرة- الآية 125.

وفي ظل التطور التقني المتسارع في استخدام الحاسوب والإنترنت في المعاملات المالية وفي أنظمة المعلومات المحاسبية بصفة عامة تتزايد معه احتمال تعرض أمن المعلومات المحاسبية للمخاطر السيبرانية، وتعد المخاطر السيبرانية نتيجة طبيعية في ظل التطورات التكنولوجية السريعة والمتلاحقة حيث أصبحت من المخاطر الكبرى التي تواجه النشاط الاستثماري والشركات والمؤسسات الاقتصادية في العالم، حيث أن الاعتماد المتزايد على الأنظمة والشبكات المعتمدة على أجهزة الحاسب الآلي صاحبه ازدياد في التهديدات والمخاطر السيبرانية التي تؤدي إلى اختراق البيانات وانتهاك خصوصيتها، مما يعطل العمل الإداري داخل المؤسسات الاقتصادية (crossler et.al, 2018).

وكنتيجة حتمية لحاجة بيئة الأعمال إلى تكيف أدواتها والسعي الدائم نحو الحد من مخاطر الأمن السيبراني والذي هو ف الأساس عملية ضمان وسلامة الفضاء السيبراني من التهديدات يمكن أن تلعب وظيفة المراجعة الداخلية دورا هاما في تقييم الاضطرابات السيبرانية وتوفير تأكيد فيما يتعلق بأمن المعلومات، وفي تكوين رؤى حول كيفية تحسين وحوكمة أمن معلومات المنشأة وتنسيق جهود إدارة المخاطر، وتقوم المراجعة الداخلية بعملية فحص المعلومات المحاسبية وفقا لمجموعة من الأدلة والقرائن، من قبل شخص مؤهل علمياً مهنيًا، يعمل على إضفاء الثقة على البيانات المالية الخاصة بفترة زمنية معينة بغرض التعرف على مدى تعرضها للمخاطر الإلكترونية ، وذلك بناءً على مجموعة من المعايير الموضوعية التي تشير إلى ضرورة امتداد وظيفة المراجعة الداخلية لتساعد الإدارة في تحديد وتقييم المخاطر الهامة التي تتعرض لها الشركة، ومن بين هذه المخاطر (المخاطر السيبرانية) وما تحتويه من احتمالات تضمين تلك المخاطر من اختراق للبيانات والتلاعب بها وانتهاك خصوصيتها (صالح، 2022).

ومن هذا المنطلق تبرز أهمية المراجعة الداخلية كأداة فعالة للحد من المخاطر والتهديدات السيبرانية وذلك في كون المراجعة الداخلية تعمل وفق تقييم مستقل ومنهجي منظم للعمليات

المؤسسية وأنظمة الرقابة الداخلية وإدارة المخاطر، وكننتيجة حتمية وحاجة بيئة الأعمال في توظيف أدواتها والسعي الدائم في الحد من المخاطر السيبرانية والذي يُعد هو الأساس في حماية الفضاء السيبراني وضمان سلامته، وبالتالي فإن المراجعة الداخلية تلعب دوراً فعالاً في الكشف ومعالجة المخاطر السيبرانية من خلال أساليب محددة وأليات منظمة تعمل علي تحديد نقاط الضعف في أنظمة التحكم والسيطرة وتقديم الاقتراحات والحلول لها (Moreira, 2019). ولذا جاءت هذه الدراسة للتعرف على دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في شركات الإتصالات الليبية .

2 - الدراسات السابقة:

أولاً: الدراسات العربية

1- دراسة (الوليد، 2017)، بعنوان: "الاتجاهات الحديثة للمراجعة الداخلية ودورها في زيادة كفاءة نظام الرقابة الداخلية"

هدفت الدراسة إلى التعرف على الاتجاهات الحديثة للمراجعة الداخلية ودورها في إدارة المخاطر ومدى انعكاسها على زيادة كفاءة نظام الرقابة الداخلية، واستخدمت الدراسة المنهج الوصفي التحليلي، وتوصلت الدراسة إلى نتائج منها: ساهمت المراجعة الداخلية في تخفيض المخاطر وساعدت إدارة المراجعة الداخلية في وضع الخطط والسياسات لتحديد الاستراتيجية المتبعة في إدارة المخاطر، المراجعة الداخلية تقدم النصح والتوصيات لإدارة المصرف بشأن زيادة نظام الرقابة الداخلية.

2- دراسة (صالح، 2018)، بعنوان: "الاتجاهات الحديثة للمراجعة ودورها في إدارة المخاطر"

هدفت الدراسة إلى التعرف على مفهوم وأنواع الاتجاهات الحديثة للمراجعة الداخلية ودورها في إدارة المخاطر، واعتمدت الدراسة على المنهج الوصفي التحليلي، واختبرت الدراسة الفرضيات الأتية: توجد علاقة ذات دلالة إحصائية بين الدور الحوكمي للمراجعة الداخلية وإدارة المخاطر، توصلت الدراسة إلى أن المراجعة الداخلية تسهم في مساعدة الإدارة في اتخاذ القرارات الرشيدة، وأظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين الدور الحوكمي للمراجعة الداخلية وإدارة المخاطر، مما يشير إلى أن تعزيز هذا الدور يؤدي إلى تحسين فعالية إدارة المخاطر، وبينت الدراسة أن المراجعة الداخلية تسهم بشكل فعال في دعم الإدارة عند اتخاذ

القرارات، من خلال توفير معلومات دقيقة وتقييمات موضوعية للمخاطر المحتملة، وأكدت النتائج أن وجود نظام مراجعة داخلية قوي يساعد المؤسسات على التنبؤ بالمخاطر المالية قبل حدوثها، مما يتيح اتخاذ التدابير الوقائية في الوقت المناسب، وأوصت الدراسة بضرورة الاستفادة القصوى من عمل المراجعة الداخلية لإبراز أهمية دور العمل الرقابي في التنبؤ بالمخاطر المالية قبل حدوثها بزمان كاف.

3-دراسة (بانقا،2019) بعنوان: "مخاطر الهجمات الإلكترونية (السيبرانية) وأثارها الاقتصادية دراسة حالة دول مجلس التعاون الخليجي"

هدفت الدراسة إلى تسليط الضوء على المخاطر السيبرانية واثارها الاقتصادية، كذلك كيفية إدارتها، واستخدمت الدراسة دول الخليج كدراسة حالة، وتصلت الدراسة إلى عدد من النتائج أهمها: تحسين أداء دول مجلس التعاون الخليجي في مواجهة الجرائم السيبرانية، وأوصت الدراسة أن الدليل العلمي للأمن السيبراني يشير إلى وجود ثغرات قانونية وتنظيمية وتدريبية وتعاونية والتي يجب ووضوع الحلول والقدرات ضد الهجمات السيبرانية.

4-دراسة (بن عطا، 2021) بعنوان : دور الإتجاهات الحديثة في المراجعة الداخلية وأساليب المخاطر في البنوك الإسلامية "

هدفت الدراسة إلى التعرف على دور الاتجاهات الحديثة للمراجعة الداخلية وأساليب إدارة المخاطر في البنوك الإسلامية ومعرفة العلاقة بينهما وتم استخدام المنهج الوصفي التحليلي، وتوصلت الدراسة إلى أن أساليب إدارة المخاطر في البنوك الإسلامية تختلف عن تلك المستخدمة في البنوك التقليدية، وأن الإتجاهات الحديثة للمراجعة الداخلية تساعد إدارة المخاطر في البنوك الإسلامية في تحديد الأساليب المناسبة لمواجهة المخاطر المحتملة، واوصت الدراسة إلى الإلتزام بتطبيق معايير المراجعة الداخلية حتى يستطيع المراجع الداخلي من تحسين عمليات البنك والتي من بينها عمليات إدارة المخاطر.

5- دراسة (الشورة،2020)، بعنوان " الأمن السيبراني في البنوك الإسلامية الأردنية"

تجد الدراسة ان الخطر السيبراني مازال يتقدم وهذا دليل دكاء وهيمنة المخترقين من خلال إيجاد ثغرات ونقاط ضعف قد تكون غير مهمة أو ملفتة بالنسبة إلينا كمستخدمين للتكنولوجيا الرقمية، وتوصلت الدراسة أن سبب تزايد المخاطر السيبرانية على مستوى الأردن يعود لقلة الخبرة

المهنية في هذا المجال وأن الأمن السيبراني مازال في فترة النمو والتطور، وأوصت الدراسة بالتأكيد على أهمية الأمن السيبراني وأنه ضرورة ملحة وبجاجة إلى التعاون بين القطاعين الخاص والعام لوضع بنية تحتية رقمية متطورة، إلى زيادة الوعي والتثقيف في هذا المجال واعتماده كمساق جامعي.

6- دراسة (عثمان، 2022)، بعنوان: "محددات فعالية وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني"

هدفت الدراسة إلى إلقاء الضوء واستكشاف فعالية دور المراجعة الداخلية في مراجعة الأمن السيبراني والحصول على دليل مستقل وموضوعي على الالتزام بسياسات الأمن السيبراني، اعتمدت الدراسة على **المنهج الوصفي التحليلي**، حيث تم تحليل البيانات المتعلقة بممارسات المراجعة الداخلية في مجال الأمن السيبراني. كما تم استخدام **المنهج الاستكشافي** لاستكشاف الأدوار الجديدة للمراجعة الداخلية في التعامل مع المخاطر السيبرانية، وقد استندت الدراسة إلى جمع البيانات من خلال الاستبيانات والمقابلات مع خبراء المراجعة الداخلية وأمن المعلومات، بالإضافة إلى تحليل تقارير المراجعة ذات الصلة، وتم تحليل النتائج باستخدام أدوات إحصائية مناسبة لقياس فعالية المراجعة الداخلية في هذا المجال، وقد توصلت الدراسة إلى أن وظيفة المراجعة الداخلية تلعب دوراً رئيسياً وفعالاً في تقييم الاضطرابات السيبرانية وفي تكوين رؤى حول كيفية تحسين وحوكمة أمن المعلومات وجهود إدارة المخاطر.

توصي الدراسة بضرورة تعزيز دور المراجعة الداخلية في مراجعة سياسات وإجراءات الأمن السيبراني بشكل دوري لضمان الالتزام بالمعايير المعتمدة. كما توصي بتدريب المراجعين الداخليين على أحدث تقنيات الأمن السيبراني وتطوير مهاراتهم بما يتماشى مع التهديدات السيبرانية المتجددة. تشدد الدراسة على أهمية تعزيز التعاون بين إدارات المراجعة الداخلية وأقسام تكنولوجيا المعلومات لضمان الكشف المبكر عن المخاطر السيبرانية ومعالجتها بفعالية. بالإضافة إلى ذلك، تدعو الدراسة إلى إنشاء نظام رقابة داخلي متكامل يدعم الجهود الوقائية في التصدي للهجمات السيبرانية ويوفر آليات للاستجابة السريعة. وأخيراً، تؤكد الدراسة على ضرورة دمج نتائج تقييم الأمن السيبراني ضمن تقارير المراجعة الداخلية الدورية لرفع الوعي لدى الإدارة العليا حول المخاطر المحتملة.

7- دراسة (محمد، 2022)، بعنوان: "التحديات التي تواجه المراجعين الداخليين في مواجهة المخاطر السيبرانية في المصارف الليبية"

هدفت هذه الدراسة إلى معرفة التحديات التي تواجه المراجعين الداخليين في التعامل مع المخاطر السيبرانية في المصارف الليبية، وأوضحت الدراسة أن الاعتماد على نظام المراجعة التقليدية يضعف من قدرة المصارف على مواجهة التهديدات السيبرانية مثل الاختيال الإلكتروني والهجمات السيبرانية، وتوصلت الدراسة إلى أن العديد من المصارف مازالت تفتقر إلى الكفاءات التكنولوجية المناسبة لمواكبة هذه التهديدات، واعتمدت الدراسة على المنهج الوصفي التحليلي، حيث تم تحليل البيانات المتعلقة بممارسات المراجعة الداخلية في المصارف الليبية، مع التركيز على التحديات المرتبطة بالمخاطر السيبرانية. تم جمع البيانات من خلال استبيانات ومقابلات مع المراجعين الداخليين وخبراء تكنولوجيا المعلومات، إلى جانب تحليل تقارير المراجعة السابقة بهدف تقييم مدى جاهزية المصارف لمواجهة التهديدات السيبرانية. استخدمت الدراسة أدوات تحليل إحصائية لاستخلاص النتائج وتفسيرها في سياق المخاطر التكنولوجية، كما أوصت الدراسة بتقديم برامج تدريبية متخصصة لتعزيز وعي المراجعين الداخليين بأهمية الأمن السيبراني وتطوير آليات رقابية مبتكرة لتقليل المخاطر.

8- دراسة (الشيخ، 2020) بعنوان: "الأنشطة الحديثة للمراجعة الداخلية ودورها في تحسين كفاءة الأداء المالي وترشيد القرارات: دراسة ميدانية على عينة من المصارف السودانية:"

هدفت الدراسة إلى دور الأنشطة الحديثة للمراجعة الداخلية في تحسين كفاءة الأداء المالي وترشيد القرارات، اتبعت الدراسة المنهج الإستنباطي لصياغة المشكلة وصياغة فرضيات البحث والمنهج الوصفي للجانب الميداني، توصلت الدراسة إلى وجود علاقة ذات دلالة إحصائية بين الدور (الحوكمي ، إضافة قيمة) وتحسين الأداء المالي بالمصارف السودانية، واوصت الدراسة بتفعيل الأنشطة الحديثة للمراجعة الداخلية (إضافة قيمة إقتصادية، الدور التوكيدي، الخدمات الاستشارية) لما لها من دور لمجابهة المخاطر والسلامة المصرفية.

9-دراسة (الزيود، 2021)، بعنوان: " أثر التدقيق الداخلي في الحد من مخاطر السيبرانية في البنوك التجارية الأردنية"

هدفت الدراسة إلى التعرف على أثر التدقيق الداخلي المتمثل (كفاءة التدقيق الداخلي، وحيادية التدقيق الداخلي، والمركز التنظيمي للتدقيق الداخلي، وتخطيط التدقيق الداخلي) في

الحد من المخاطر السيبرانية في البنوك التجارية الأردنية، وتوصلت الدراسة إلى عدم وجود أثر لحياذية التدقيق الداخلي في الحد من المخاطر السيبرانية في البنوك التجارية الأردنية، وأوصت الدراسة بضرورة حث إدارة البنوك على زيادة مستوى الوعي والمسؤولية اتجاه المخاطر السيبرانية وأثرها على أدائها وإمكانياتها، وحث إدارة البنوك على الرفع من مستوى الوعي بأهمية أثر التدقيق الداخلي في الحد من المخاطر السيبرانية.

10-دراسة (عمر، 2023)، بعنوان: "دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر أمن المعلومات المحاسبية"

هدفت الدراسة إلى تحليل تأثير الاتجاهات الحديثة في المراجعة الداخلية على تقليل مخاطر أمن نظم المعلومات المحاسبية وأثرها على التقارير المالية، وركزت أيضاً على الدور الذي تلعبه تكنولوجيا المعلومات وحوكمة الشركات في تعزيز الشفافية والدقة، حيث تم استخدام المنهج التاريخي والاستنباطي والاستقرائي والوصفي التحليلي لتحليل بيانات العينة المأخوذة من بنك الخرطوم، حيث توصلت الدراسة إلى مجموعة من النتائج من أهمها أن الالتزام باليات المحاسبة لحوكمة الشركات يعزز الشفافية والدقة في القوائم المالية، كما أن هناك علاقة ارتباط بين إدارة المخاطر وبين أمن نظم المعلومات المحاسبية، وأوصت هذه الدراسة بتعزيز حوكمة الشركات كإحدى الاتجاهات الحديثة في المراجعة الداخلية لتحقيق الشفافية والثقة في المعلومات المالية المفصح عنها.

11- دراسة (الشيخ وأحمد، 2023)، بعنوان: "أثر إطار عمل (COSO) للرقابة الداخلية في الحد من مخاطر المحاسبة السحابية: الدور الوسيط للأمن السيبراني في البنوك التجارية الأردنية"

حيث تناولت هذه الدراسة أثر إطار COSO للرقابة الداخلية في الحد من مخاطر المحاسبة السحابية واتبعت الدراسة المنهج الوصفي والتحليلي عن طريق طرح استبانة موجهة للعاملين في البنوك التجارية الأردنية وتحليلها تحليلًا إحصائياً، وتوصلت الدراسة إلى مجموعة من النتائج أهمها وجود تأثير ذو دلالة إحصائية لتنفيذ عناصر الرقابة الداخلية وفق إطار COSO في تقليل مخاطر المحاسبة السحابية، وأن الأمن السيبراني يلعب دوراً وسيطاً في تعزيز فعالية الرقابة الداخلية وتحقيق الاستقرار في القطاع المصرفي، وأوصت الدراسة على أنه يجب

علي البنوك التجارية الأردنية أن تقوم بتطوير سياسات لممارسات الموارد البشرية تشمل اختيار وتدريب الموظفين لتعزيز نظام الرقابة الداخلية.

12- دراسة (أبو الخير، 2023)، بعنوان: "أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية"

هدفت الدراسة إلى اختبار أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية، اعتمدت الدراسة على المنهج الوصفي التحليلي لدراسة تأثير جودة المراجعة الداخلية على الحد من المخاطر السيبرانية في البنوك الإلكترونية، مع تحليل مدى مساهمتها في تحقيق الاستقرار المالي. كما تم توظيف المنهج الاستكشافي لاستكشاف التحديات الجديدة المرتبطة بالمخاطر السيبرانية والتطورات المتسارعة في هذا المجال. جمعت البيانات من خلال استبيانات ومقابلات مع مسؤولي المراجعة الداخلية وإدارات المخاطر في البنوك الإلكترونية، بالإضافة إلى تحليل تقارير المراجعة ذات الصلة. تم استخدام أدوات تحليل إحصائية لاختبار الفرضيات وتفسير النتائج في سياق تأثير جودة المراجعة على استقرار النظام المالي في هذه المؤسسات، توصلت الدراسة إلى مجموعة من النتائج النظرية والعملية أهمها: التطور الحادث في المخاطر السيبرانية يحفز المنظمات المالية وخاصة البنوك الإلكترونية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجلس إدارات تلك البنوك، الأمر الذي يؤدي إلى الاستقرار المالي في تلك البنوك، أوصت الدراسة أن العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بقطاع البنوك بهدف فهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني.

13- دراسة (الكرعاوي والعيساوي، 2024)، بعنوان: "دور التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني وانعكاسه في خفض كلفة التأمين"

حيث هدفت هذه الدراسة إلى معرفة العلاقة بين التدقيق الداخلي وإدارة مخاطر الأمن السيبراني في الوحدات الاقتصادية، وتحديد كيفية مساهمة التدقيق الداخلي في تقليل تكاليف

التأمين من خلال تقليل المخاطر السيبرانية، حيث أتتبت الدراسة المنهج الوصفي التحليل، وتوصلت الدراسة إلي مجموعة من النتائج أهمها وجود تأثير ذو دلالة إحصائية للتدقيق الداخلي على إدارة مخاطر الأمن السيبراني وأن التدقيق الداخلي يسهم في خفض تكاليف التأمين من خلال الحد من المخاطر السيبرانية التي تواجه الوحدات الاقتصادية، وتوصي الدراسة بضرورة تعزيز دور التدقيق الداخلي في الوحدات الاقتصادية من خلال تطوير آليات فحص وتقييم نظم الأمن السيبراني بانتظام لضمان فاعلية الضوابط الوقائية، كما تؤكد على أهمية تدريب المدققين الداخليين على التقنيات الحديثة في مجال الأمن السيبراني لزيادة قدرتهم على اكتشاف الثغرات المحتملة ومعالجتها بفعالية، وتدعو الدراسة أيضًا إلى تعزيز التعاون بين إدارات التدقيق الداخلي وإدارات تكنولوجيا المعلومات لتنسيق الجهود في مواجهة التهديدات السيبرانية، بالإضافة إلى ذلك، تشدد على ضرورة مراجعة سياسات التأمين بشكل دوري بناءً على نتائج التدقيق الداخلي لتخفيض التكاليف وضمان التغطية الفعالة للمخاطر السيبرانية المحتملة

14- دراسة (هبة، 2021) بعنوان: " أثر جودة مستوى التوكيد على برنامج إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين"

هدفت الدراسة إلى اختبار وتحليل جودة التوكيد (المقاسة من خلال حجم مكتب المراجعة الذي يوفر هذا التوكيد، ومكتب المراجعة ينتمي إلى إحدى مكاتب المراجعة الأربعة الكبار في مقابل مكتب مراجعة آخر بخلاف هذه المكاتب) وبمستوى التوكيد (توكيد معقول في مقابل توكيد محدود) على برنامج إدارة مخاطر الأمن السيبراني على رغبة المستثمرين غير المحترفين في الإستثمار وتقييمهم لأسهمهم ، وتوصلت الدراسة إلى وجود دليلا على أن لجودة التوكيد المرتفعة ومستوى التوكيد المعقول تأثير جوهري وإيجابي على رغبة المستثمرين في الإستثمار وتقييمهم لأسهمهم،

وأوصت الدراسة بضرورة وضع الشركات تدابير لمواجهة المخاطر السيبرانية التي يمكن ان تعوق جودة المراجعة، وذلك لأن جودة المراجعة ومستوى التوكيد له تأثير جوهري على رغبة المستثمرين في الإستثمار وتقييمهم للأسهم.

15- دراسة (صالح علي صالح، 2022) بعنوان : "أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرارات الإستثمار بأسهم الشركات المقيدة بالبورصة المصرية"

هدفت الدراسة إلى تحليل علاقة محددات فعالية المراجع الداخلي للأمن السيبراني، وقد توصلت الدراسة إلى إشتقاق مقياس لدعم فعالية توكيد المراجعة الداخلية على الأمن السيبراني بالإعتماد على معايير الممارسة المهنية للمراجعة الداخلية التي توفر إطاراً إلزامياً لوظيفة المراجعة الداخلية وهي (Cobit5) و (Iso2/27001) . وأوصت الدراسة بضرورة تحديد مجموعة من الإجراءات لقياس فعالية توكيد المراجعة الداخلية على الأمن السيبراني خلال مراحل أداء التكليف الثلاثة بدء بالتخطيط ثم التنفيذ وأخيراً إعداد التقرير .

ثانياً: الدراسات الأجنبية

1- دراسة (Jones & Smith, 2019) بعنوان: "The Role of Internal Auditing in Cybersecurity Management"، بمعنى: "دور التدقيق الداخلي في إدارة الأمن السيبراني"

تناولت هذه الدراسة العلاقة بين جودة المراجعة الداخلية وتقليل المخاطر السيبرانية في المؤسسات، حيث تم تحليل كيفية اعتماد المؤسسات على ممارسات المراجعة الداخلية للكشف عن المخاطر والتخفيف منها، وأشارت الدراسة إلى أن المراجعة الداخلية التي تعتمد على أدوات وتقنيات حديثة مثل الذكاء الاصطناعي والتحليل البياني تساعد بشكل كبير في تحديد التهديدات الأمنية مبكراً والتعامل معها قبل أن تتسبب في أضرار كبيرة، كما ركزت الدراسة على أهمية تكامل جهود فرق المراجعة الداخلية مع فرق تكنولوجيا المعلومات لضمان بيئة آمنة ومحمية ضد الهجمات السيبرانية، واعتمدت الدراسة على المنهج الوصفي التحليلي لتحليل العلاقة بين جودة المراجعة الداخلية وتقليل المخاطر السيبرانية في المؤسسات، وتم استخدام هذا المنهج لدراسة تأثير الأدوات والتقنيات الحديثة، مثل الذكاء الاصطناعي والتحليل البياني، على قدرة المراجعة الداخلية في الكشف المبكر عن التهديدات الأمنية، كما تم جمع البيانات من خلال استبيانات ومقابلات مع مختصين في المراجعة الداخلية وتكنولوجيا المعلومات، مع الاستفادة من التحليل الإحصائي لاختبار الفرضيات وتفسير النتائج في سياق بيئة العمل السيبرانية.

حيث توصلت الدراسة إلى أن تبني التكنولوجيا الحديثة يعزز قدرة المراجعة الداخلية على كشف الثغرات الأمنية، كما إن التعاون بين فرق المراجعة الداخلية وتكنولوجيا المعلومات يعزز من أدوات الأمن السيبراني، كذلك تلعب جودة المراجعة الداخلية دوراً مهماً في تقليل

المخاطر السيبرانية، وتوصي الدراسة بضرورة تعزيز استخدام الأدوات التكنولوجية الحديثة في المراجعة الداخلية، بما في ذلك الذكاء الاصطناعي وتقنيات التحليل البياني، لدعم القدرة على الكشف المبكر عن المخاطر السيبرانية والتعامل معها بفعالية، كما تؤكد على أهمية تكامل جهود فرق المراجعة الداخلية مع فرق تكنولوجيا المعلومات لضمان وجود بيئة عمل آمنة ومحمية من التهديدات السيبرانية، بالإضافة إلى ذلك تشدد الدراسة على ضرورة تطوير مهارات المراجعين الداخليين من خلال التدريب المستمر لمواكبة التطورات التقنية وتعزيز جودة المراجعة بما يساهم في تقليل المخاطر السيبرانية بشكل فعال.

2- دراسة (Hayek & Smith, 2020) بعنوان: "Cybersecurity Risks and Internal Audit: A New Paradigm"، بمعنى: "مخاطر الأمن السيبراني والمراجعة الداخلية نموذج جديد"

هدفت هذه الدراسة إلى معرفة الدور الذي تلعبه المراجعة الداخلية في إدارة المخاطر السيبرانية، حيث ركزت على كيفية تأثير جودة المراجعة الداخلية على تقليل تلك المخاطر، وأوضحت الدراسة أن المراجعة الداخلية الجيدة تلعب دوراً أساسياً في تقييم أنظمة الأمن السيبراني واكتشاف الثغرات الموجودة في النظام، كما تم التركيز على أهمية مطابقة سياسات وإجراءات الأمن السيبراني للمعايير الدولية، مما يؤدي إلى تقليل احتمالات تعرض المؤسسات للهجمات السيبرانية، واعتمدت الدراسة على المنهج الوصفي التحليلي لدراسة الدور الذي تلعبه المراجعة الداخلية في إدارة المخاطر السيبرانية، وتم جمع البيانات من خلال استبيانات ومقابلات مع خبراء في المراجعة الداخلية والأمن السيبراني داخل المؤسسات، بالإضافة إلى تحليل تقارير المراجعة الداخلية ذات الصلة، وتم استخدام هذا المنهج لتقييم كيفية تأثير جودة المراجعة الداخلية على تقليل المخاطر السيبرانية من خلال تحليل دور المراجعين الداخليين في اكتشاف الثغرات الأمنية وتقييم فعالية أنظمة الأمن السيبراني، كما تم فحص التزام المؤسسات بالمعايير الدولية للأمن السيبراني وكيفية تأثير ذلك على تقليل احتمالات تعرضها للهجمات السيبرانية، وتوصلت الدراسة إلى أن وجود مراجعين داخليين ذوي كفاءة عالية ومعرفة شاملة بالأمن السيبراني يعزز قدرة المؤسسات على مواجهة التهديدات السيبرانية، وأوصت الدراسة بتحسين جودة المراجعة الداخلية للكشف المبكر للتهديدات السيبرانية، وكذلك أوصت بزيادة الامتثال للمعايير الدولية الذي بدوره

يقلل من احتمالية وقوع الهجمات السيبرانية أيضا يجب الاهتمام بتوفير التدريب الكافي للمراجعين الداخليين علي أحدث ممارسات الأمن السيبراني.

3- دراسة (Lois et al, 2021) بعنوان: "the role of internal auditors in reducing it risk"، بمعنى: "دور المراجع الداخلي في الحد من مخاطر تكنولوجيا المعلومات"

هدفت هذه الدراسة إلى ضرورة فحص المتغيرات التي تؤثر على الأمن السيبراني والمرتبطة بالمراجعة الداخلية، واعتمدت الدراسة على المنهج الوصفي التحليلي لفحص العلاقة بين المراجعة الداخلية والأمن السيبراني، وتم جمع البيانات من خلال استبيانات ومقابلات مع المراجعين الداخليين ومتخصصي تكنولوجيا المعلومات لتحديد مدى تأثير التعاون بينهما على فاعلية سياسات الأمن السيبراني، وقد توصلت الدراسة إلى أن العلاقة الجيدة بين متخصصي تكنولوجيا المعلومات والمراجعين الداخليين منخفضة للغاية فيما يتعلق بمعايير سياسات الأمن التي تم مراجعتها من قبل المراجع الداخلي، وقد أوصت الدراسة على ضرورة استشارة المراجعين الداخليين وتعاونهم مع الإدارة في تشكيل السياسات لتدابير الأمن السيبراني والحد من مخاطره.

4- دراسة (al et Vuko, 2021) بعنوان: "Effectiveness of internal auditor in managing Cybersecurity risks"، بمعنى: "فعالية المراجع الداخلي في إدارة مخاطر الأمن السيبراني"

هدفت هذه الدراسة إلى تحليل العوامل التي تفسر فعالية المراجع الداخلي في توفير أمانات وتأكيدات حول إدارة مخاطر الأمن السيبراني، وقد قامت الدراسة بإجراء استبيان في مجال تكنولوجيا المعلومات ورئيسا تنفيذيا للمراجعة من مختلف الصناعات والمؤسسات على مستوى العالم لدراسة العلاقة بين فعالية مراجعة الأمن السيبراني (Auditing Security Cyber (CSA)، وبعض العوامل المؤثرة في جودة المراجعة الداخلية، وقد انتهت الدراسة إلى أن القوى المعيارية والتي تتمثل في شهادات الأمن السيبراني للمراجعين الداخليين والعوامل البشرية تفسر بشكل كبير فعالية مراجعة الأمن السيبراني، وتوصي الدراسة بضرورة تعزيز برامج تدريب المراجعين الداخليين على أحدث معايير وشهادات الأمن السيبراني لتطوير مهاراتهم وقدرتهم على تقييم المخاطر بشكل فعال، كما تشدد الدراسة على أهمية تحسين التعاون بين فرق المراجعة الداخلية والإدارة التنفيذية لضمان تطبيق السياسات والمعايير الأمنية بشكل موحد، وتوصي أيضًا

بتخصيص موارد إضافية لتعزيز الوعي حول الأبعاد البشرية للأمن السيبراني وتأثيرها على فعالية المراجعة، مع التأكيد على أهمية إنشاء بيئة تعليمية تدعم التعلم المستمر في هذا المجال. أخيراً، توصي الدراسة بضرورة اعتماد أدوات وتقنيات متقدمة في عملية المراجعة لتحسين دقة وفعالية التقييمات الأمنية.

5-دراسة (Prigerson et al ,2021) بعنوان: Timelines And Reliability Of corporate Financial Statement And The Expertise Of Audit Committee Information "بمعنى قضايا تتعلق بتوقيت وموثوقية البيانات المالية للشركة وخبرة لجان المراجعة في تكنولوجيا المعلومات"

الهدف من الدراسة هو فحص ما إذا كانت خبرة لجان المراجعة في مجال تكنولوجيا المعلومات تؤثر في موثوقية القوائم المالية للشركات وحسن توقيتها أم لا، وتوصلت الدراسة إلى أن المستثمرين يستجيبون بشكل أكبر للتقارير المالية في الشركات التي لديها خبرة في شكل لجان مراجعة خبيرة في تكنولوجيا المعلومات وذلك لوجود دلالة على استجابة أعلى للأرباح، وأوصت الدراسة بضرورة اختيار لجان مراجعة ذو خبرة في مجال تكنولوجيا المعلومات حتى تضيق قدر كبير من الثقة على التقارير المالية.

6-دراسة (Rosati et al.,2022) بعنوان: Cyber-Security Incidents and Audit Quality.بمعنى:أثر حوادث الأمن السيبراني على جودة المراجعة"

ركزت الدراسة على تحديد أثر حوادث الأمن السيبراني على جودة المراجعة. وتضمنت عينة الدراسة 329 منشأة أمريكية تعرضت لحوادث أمن سيبراني في الفترة بين 2005 إلى 2014. وتوصلت الدراسة إلى أن حوادث الأمن السيبراني لا تؤثر على جودة المراجعة المراجعة، واعتمدت في ذلك على أن حوادث الأمن السيبراني قد تدل على وجود ضعف في هيكل الرقابة الداخلية الخاص بالمنشأة في تلك الحالة سوف يقوم المراجع بأداء المزيد من الاختبارات وذلك لدعم جودة المراجعة. وأوصت الدراسة في حالة حدوث جريمة تتعلق بالأمن السيبراني سوف يزيد المراجعون من جهودهم وذلك للحفاظ على مستوى مقبول من مخاطر المراجعة، لذا عند القيام بالمزيد من إجراءات واختبارات المراجعة، لن يتسبب ذلك في تقليل جودة المراجعة.

التشابه والاختلاف بين الدراسات السابقة والدراسة الحالية:

1-أوجه التشابه:

يتضح من استعراض الدراسات السابقة العربية والأجنبية أنها تلتقي مع الدراسة الحالية في اهتمامها بإبراز الدور المتنامي للمراجعة الداخلية في مواجهة المخاطر المعاصرة، وبخاصة المخاطر السيبرانية، كما تشترك معظمها في التأكيد على أن تطوير وظيفة المراجعة الداخلية، ورفع كفاءة المراجعين، وتعزيز التكامل بين المراجعة الداخلية وإدارة المخاطر وتكنولوجيا المعلومات، كلها عوامل تسهم في الحد من التهديدات الإلكترونية وتحسين قدرة المؤسسات على الوقاية والاستجابة. كذلك اتفقت غالبية هذه الدراسات في اعتمادها على المنهج الوصفي التحليلي، مع توظيف الاستبانة أو المقابلات أو تحليل التقارير بوصفها أدوات مناسبة لدراسة العلاقة بين المراجعة الداخلية والمخاطر السيبرانية .

كما يظهر وجود تشابه موضوعي بين الدراسة الحالية وعدد من الدراسات العربية مثل دراسة الوليد (2017) وصالح (2018) وبن عطف (2021) وعمر (2023)، إذ ركزت هذه الدراسات على الاتجاهات الحديثة للمراجعة الداخلية وعلاقتها بإدارة المخاطر أو دعم الحوكمة أو حماية المعلومات. ويتكرر هذا التقاطع أيضًا في دراسات عثمان (2022) والزيود (2021) وأبو الخير (2023) والكرعاوي والعيساوي (2024)، التي اقتربت بصورة أوضح من موضوع الدراسة الحالية من خلال ربط فعالية المراجعة الداخلية بمواجهة مخاطر الأمن السيبراني أو خفض آثارها على المؤسسات. وعلى المستوى الأجنبي، تتفق دراسات Jones & Smith (2019) و Hayek (2020) و Vuko وآخرين (2021) مع الدراسة الحالية في إبراز أهمية تطوير أدوات المراجعة الداخلية، ورفع التأهيل المهني للمراجعين، وتقوية التعاون مع إدارات تكنولوجيا المعلومات للحد من المخاطر السيبرانية .

2-أوجه الاختلاف:

أما من حيث الاختلاف، فتتباين الدراسات السابقة من عدة جوانب. أول هذه الجوانب يتمثل في بيئة التطبيق؛ فغالبية الدراسات العربية أجريت في البنوك التجارية أو الإسلامية أو الإلكترونية، أو في بيئات مالية ومصرفية، مثل دراسات بن عطف (2021)، الشورة (2020)، الزيود (2021)، الشيخ وأحمد (2023)، وأبو الخير (2023)، في حين أن الدراسة الحالية تتجه

إلى شركات الاتصالات الليبية، وهي بيئة تختلف من حيث طبيعة البنية الرقمية، وحجم الاعتماد على الشبكات، ودرجة التعرض للهجمات السيبرانية. كما أن بعض الدراسات ركزت على المصارف الليبية تحديداً، مثل دراسة محمد (2022)، لكنها تناولت التحديات التي تواجه المراجعين الداخليين، ولم تتناول بصورة مباشرة دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني داخل قطاع الاتصالات .

ويظهر الاختلاف أيضاً في المتغيرات والأبعاد محل الدراسة؛ فبعض الدراسات تناولت المراجعة الداخلية من منظور الحوكمة وإدارة المخاطر فقط، مثل صالح (2018)، بينما ربطت دراسات أخرى المراجعة الداخلية بمتغيرات مختلفة، مثل كفاءة الأداء المالي وترشيد القرارات في دراسة الشيخ (2020)، أو الاستقرار المالي في دراسة أبو الخير (2023)، أو خفض كلفة التأمين في دراسة الكرعوي والعيساوي (2024)، أو قرارات المستثمرين وجودة التوكيد والإفصاح في دراستي هبة (2021) وصالح علي صالح (2022). وفي المقابل، فإن الدراسة الحالية تركز بصورة أكثر تحديداً على العلاقة المباشرة بين الاتجاهات الحديثة للمراجعة الداخلية والحد من مخاطر الأمن السيبراني، بما يجعلها أكثر تحديداً في الربط بين المتغير المستقل والمتغير التابع داخل بيئة ميدانية واحدة .

ومن أوجه الاختلاف المهمة كذلك نتائج الدراسات؛ فعلى الرغم من اتفاق معظمها على وجود أثر إيجابي للمراجعة الداخلية أو لجودتها أو لتطويرها في الحد من المخاطر السيبرانية، فإن بعض النتائج لم تكن متطابقة تماماً. فدراسة الزيود (2021) مثلاً توصلت إلى عدم وجود أثر لحياذية التدقيق الداخلي في الحد من المخاطر السيبرانية، كما أن دراسة Rosati وآخرين (2022) رأت أن حوادث الأمن السيبراني لا تؤدي بالضرورة إلى انخفاض جودة المراجعة، بل قد تدفع المراجعين إلى تكثيف الإجراءات والاختبارات للحفاظ على المستوى المقبول من مخاطر المراجعة. وهذا الاختلاف في النتائج يكشف أن العلاقة بين المراجعة الداخلية والمخاطر السيبرانية ليست علاقة أحادية أو بسيطة، وإنما تتأثر بطبيعة القطاع، ومستوى الجاهزية التقنية، وكفاءة العنصر البشري، ونظام الرقابة الداخلية السائد في المؤسسة .

3- ملامح الدراسة الحالية عن الدراسات السابقة:

وبناءً على ذلك، تتميز الدراسة الحالية عن الدراسات السابقة في عدة نقاط؛ فهي أولاً تجمع بين متغيرين يرتبطان ببعضهما ارتباطاً مباشراً وهما الاتجاهات الحديثة للمراجعة الداخلية

ومخاطر الأمن السيبراني، وثانيًا تطبيق هذا الموضوع على شركات الاتصالات الليبية بدلاً من الاقتصار على البنوك أو المؤسسات المالية، وثالثًا تسعى إلى تقديم معالجة ميدانية في البيئة الليبية التي ما تزال بحاجة إلى مزيد من الدراسات التطبيقية في هذا المجال، خصوصًا في ظل التوسع الرقمي والاعتماد الكبير على نظم المعلومات والاتصالات. ومن ثم فإن الدراسة الحالية لا تكرر ما سبق، بل تسد فجوة تطبيقية ومعرفية تتعلق بقطاع الاتصالات الليبي، وتقدم امتدادًا عمليًا للدراسات السابقة في سياق أكثر اتصالاً بواقع التهديدات السيبرانية الراهنة، حيث تساهم الدراسة الحالية في دعم فكرة ان المراجعين يمكنهم تقليل مخاطر التحريف الجوهري وما يترتب على ذلك من تضليل وعدم مصداقية تقرير إدارة المخاطر من خلال زيادة جهودهم في المراجعة وهو ما لم تتناوله أي من الدراسات السابقة.

كما أن المخاطر السيبرانية تُعدّ ظاهرة حديثة تستوجب دراستها بشكل معمق لمعرفة كيفية الحد منها، خصوصاً وأن التهديدات السيبرانية تطال جميع أفراد المجتمع، لذلك جاءت هذه الدراسة استجابة لهذه الحاجة الملحة بهدف تعزيز أمن شبكات الاتصالات وتقليل تأثير هذه المخاطر على الأفراد والمؤسسات.

مشكلة الدراسة:

أدى التطور غير المسبوق في بيئة الأعمال إلى اتجاه العديد من المنشآت والمؤسسات الاقتصادية إلى مواكبة التكنولوجيا الحديثة وذلك من خلال استخدام أساليب تكنولوجية متطورة في مباشرة أعمالها لجعلها أكثر كفاءة وتخزين بياناتها الحساسة والهامة على الشبكات الإلكترونية؛ وكذلك صاحب هذا التطور السريع في التكنولوجيا تطور سريع أيضا للتهديدات السيبرانية وتطور وتنوع أساليب المحترفين في شن هجماتهم والاستفادة من أي ثغرات موجودة على الشبكات الإلكترونية والتي تهدد بتلف وفقدان هذه البيانات الأمر الذي جعل لزاما على بيئة الأعمال ضرورة تبني بنية رقمية فعالة لحماية هذه البيانات ومنع أو تقليل الآثار المترتبة على الأحداث التي قد تعطل سير العمل (Kahyaoglu & Caliyurt, 2018)، ومن الأساليب والأنظمة التي تتبناها هذه المؤسسات وتسعى إلى تطويرها؛ هي نظام المراجعة الداخلية للتقليل من المخاطر السيبرانية؛ لما في ذلك حماية لثروة الملاك وسمعة هذه المؤسسات وترشيد صائب لقرارات المستثمرين تجاهها كما أنه من الممكن أن يمتد التأثير السلبي للهجمات السيبرانية؛ على فقد أصحاب المصالح الثقة في المنشأة التي تعرضت للهجمات السيبرانية؛ وكذلك في الصناعات التي تنتمي إليها هذه المنشأة، فيما يعرف بتأثير عدوى اختراق الأمن السيبراني (Kelton & Pennington, 2020).

ومن ضمن التحديات التي تواجه الدولة الليبية هو تحديث مؤسساتها العامة لمواجهة التحديات الجديدة في الفضاء السيبراني، ولقد حصلت ليبيا على معدل متدني في مؤشر الأمن السيبراني العالمي لسنة 2020م الصادر من الاتحاد الدولي للاتصالات التابع للأمم المتحدة (محمد، 2022).

حيث أن المشكلة الحقيقية تبدأ من سياسات المنشأة الداخلية وتقودنا المشكلة إلى التساؤل عن استراتيجيات المراجعة الداخلية في الوقت الراهن ودورها من حيث دعم إدارة المخاطر في الكشف المبكر عن التهديدات السيبرانية .

ومن هذا المنطلق ووفقا للعلاقة بين نظام المراجعة الداخلية والمخاطر السيبرانية يتم طرح التساؤل الرئيسي التالي: هل يوجد دور للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني شركات الاتصالات قيد الدراسة؟

ويتفرع عن هذا التساؤل مجموعا من التساؤلات الفرعية، وهي كما يأتي:

1. هل يوجد دور لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.
2. هل يوجد دور لحوكمة الشركات في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة..
3. هل يوجد دور لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

4-أهداف الدراسة:

سعت هذه الدراسة بشكل رئيسي إلى التعرف على معرفة دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني شركات الاتصالات قيد الدراسة.

ويتفرع من هذا الهدف مجموعة من الأهداف الفرعية، وهي كما يأتي:

1. معرفة دور إدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.
2. معرفة دور حوكمة الشركات في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة..
3. معرفة دور إضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

5- أهمية الدراسة:

- الأهمية العلمية:

اكتسب هذه الدراسة أهمية كبيرة نظراً لكونها تتناول موضوعاً حيويًا ومواكبًا للتطورات التكنولوجية الحديثة، وهو العلاقة بين الاتجاهات الحديثة للمراجعة الداخلية ومخاطر الأمن السيبراني؛ فعلى المستوى النظري، تسهم الدراسة في سد فجوة معرفية في أدبيات المراجعة

الداخلية وإدارة المخاطر السيبرانية، حيث تقدم رؤية شاملة لدور المراجعة الداخلية في التصدي للتحديات والتهديدات السيبرانية المتزايدة، كما تعزز هذه الدراسة الفهم الأكاديمي حول تأثير عناصر مثل إدارة المخاطر؛ الدور الحوكمي؛ إضافة قيمة على تقليل المخاطر السيبرانية، ما يُثري الإطار النظري ويُمهّد الطريق لأبحاث مستقبلية.

- الأهمية العملية:

على المستوى العملي فإن الدراسة تُقدم حلولاً واقعية يمكن أن تُسهم في تحسين المراجعة الداخلية في شركات الاتصالات الليبية، مما يعزز قدرتها على اكتشاف المخاطر السيبرانية والاستجابة لها بفعالية، وتساعد النتائج المتوقعة صانعي القرار والمديرين في وضع سياسات وإجراءات أكثر كفاءة لحماية أصول المؤسسات الرقمية من التهديدات المتزايدة، مما يُعزز الثقة التنظيمية ويُحسن السمعة المؤسسية.

بالإضافة إلى ذلك، تأتي أهمية هذه الدراسة في سياقها الاستراتيجي، حيث تمكّن تلك الشركات من مواكبة التطورات التكنولوجية السريعة والامتثال للمعايير الدولية المتعلقة بالحوكمة وضوابط الأمن السيبراني، وبالتالي فإن هذه الدراسة تُساهم بشكل كبير في تعزيز الأمن المؤسسي ودعم استدامة المؤسسات في مواجهة التحديات الرقمية الراهنة والمستقبلية.

6- فرضيات الدراسة:

الفرضية الرئيسية:

- يوجد دور ذو دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

الفرضيات الفرعية:

1. يوجد دور ذو دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.
2. يوجد دور ذو دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة..
3. يوجد دور ذو دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

7- أسلوب جمع وتحليل البيانات:

أسلوب جمع البيانات:

اعتمد هذه الدراسة على المنهج الوصفي التحليلي كمنهج لها، ولكي يتم وضع إطار نظري لهذه الدراسة، سيتم الاعتماد على المصادر المتمثلة في الكتب، والرسائل العلمية، والدراسات المنشورة في المجالات العلمية المحكمة العربية والانجليزية، والمؤتمرات، والدوريات، والتقارير، والقرارات، والمواقع الالكترونية المختلفة، بما يتلاءم مع أهداف هذه الدراسة لجمع البيانات الثانوية، أما في الجانب التطبيقي لهذه الدراسة قام الباحث بتصميم استمارة استبيان لغرض جمع البيانات الأولية من عينة الدراسة، وستشمل الاستمارة جزأين أساسيين حيث سيتم استخدام الجزء الأول في جمع البيانات الشخصية عن المبحوثين والمتمثلة في المؤهل الأكاديمي، التخصص العلمي، عدد سنوات الخبرة، المكان الوظيفي، أما الجزء الثاني من الاستمارة فيتكون من متغيرين؛ المتغير الأول (المستقل) والمتمثل في الاتجاهات الحديثة للمراجعة الداخلية، ويشمل (4) محاور: المحور الأول الدور الحوكمي، والمحور الثاني إدارة المخاطر، والمحور الثالث إضافة قيمة، وأما المتغير (التابع) مخاطر الأمن السيبراني.

التحليل الوصفي للبيانات:

اعتمد هذه الدراسة على استخدام بعض أساليب الإحصاء الوصفي لمعرفة وتوضيح خصائص متغيرات الدراسة المختلفة مثل، التوزيعات التكرارية لتحديد عدد التكرارات، والنسبة المئوية للتكرار التي تتحصل عليه كل إجابة، منسوبا إلى إجمالي التكرارات، وذلك لتحديد الأهمية النسبية لكل إجابة ويعطي صورة أولية عن إجابة أفراد مجتمع الدراسة على العبارات المختلفة، المتوسط الحسابي لتحديد درجة تمركز إجابات المبحوثين عن كل فقرة، حول درجات المقياس، وذلك لتحديد مستوى كل محور من محاور الدراسة، المتوسط الحسابي المرجح لتحديد اتجاه الإجابة لكل عبارة من عبارات المقياس وفق مقياس التدرج الخماسي، الانحراف المعياري لقياس تشتت الإجابات ومدى انحرافها عن متوسطها الحسابي، اختبار (T) (One Sample T test): لتحديد جوهرية الفروق بين متوسط الاستجابة ومتوسط القياس (3) في المقياس الخماسي، معامل ألفا كرونباخ للتأكد من ثبات أداة الدراسة، معامل الارتباط لإيجاد العلاقة بين كل محور من محاور الاستبيان وإجماليه، وتحديد العلاقة بين المتغير المستقل والمتغير التابع، تباين

الانحدار الخطي والمتعدد لتحديد أثر المتغير المستقل (دور الاتجاهات الحديثة للمراجعة الداخلية) على المتغير التابع (مخاطر الأمن السيبراني).

8- مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في جميع الموظفين بإدارات شركات الاتصالات الليبية / بمدينة طرابلس وهي: (المدار، لبيانا، هاتف ليبيا) البالغ عددهم (220) موظف وموظفة للمسميات الوظيفية (محاسبين ومراجعين، وكل من لديه علاقة بموضوع الدراسة)

9- أنموذج الدراسة:

تتمثل متغيرات الدراسة في الآتي:

1- المتغير المستقل:

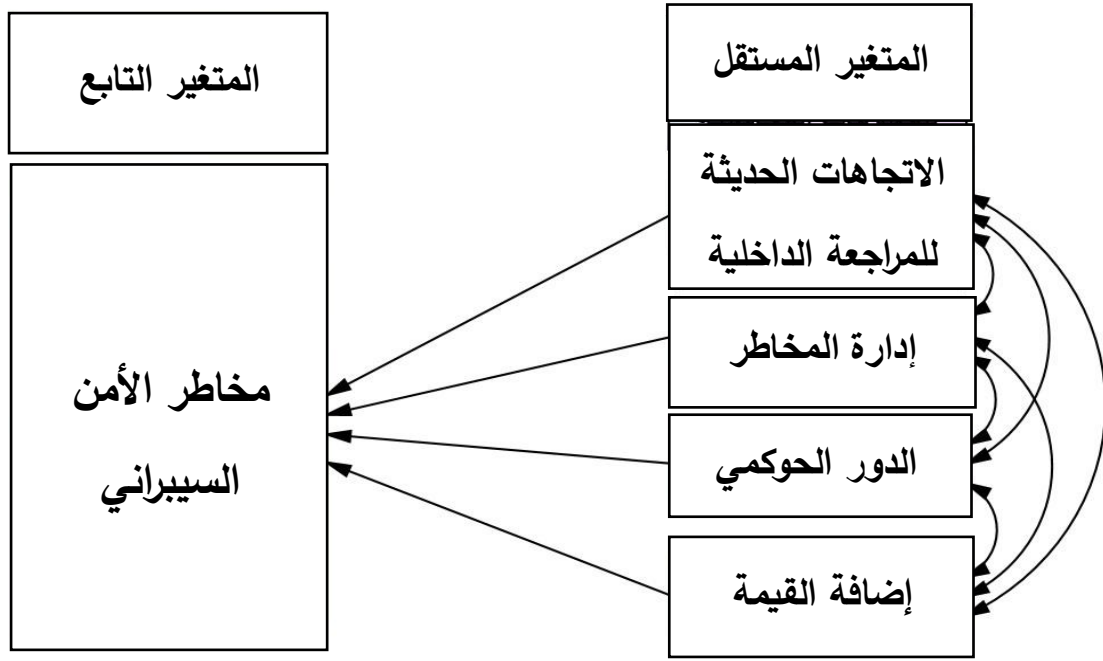
يمثل هذا المتغير في دور الاتجاهات الحديثة للمراجعة الداخلية؛ وسيتم قياسها كما يأتي:

- إدارة المخاطر.
- الحوكمة.
- إضافة قيمة.

2- المتغير التابع:

يتمثل في مخاطر الأمن السيبراني، ويمكن توضيح متغيرات الدراسة من خلال النموذج

الآتي:



شكل (1) يوضح أنموذج الدراسة
المصدر: تصميم الباحث.

10- حدود الدراسة:

تمثلت حدود الدراسة فيما يأتي:

- الحدود الزمنية: الحدود الزمنية للدراسة خلال سنة 2025م.
- الحدود المكانية: الحدود المكانية للدراسة شركات الاتصالات الليبية.
- الحدود الموضوعية: اقتصر الحدود الموضوعية للدراسة على دور الاتجاهات الحديثة للمراجعة الداخلية، ومخاطر الأمن السيبراني.

11- محتويات الدراسة:

سيتم تقسيم الدراسة الحالية إلى الفصول الآتية:

الفصل الأول: الإطار العام للدراسة.

الفصل الثاني: الإطار النظري للاتجاهات الحديثة للمراجعة الداخلية.

الفصل الثالث: الإطار النظري لمخاطر الأمن السيبراني.

الفصل الرابع: الدراسة الميدانية.

12- مصطلحات الدراسة:

- **دور المراجعة الداخلية:** "دور المراجعة الداخلية يشير إلى المسؤولية التي تقع على عاتق إدارة المراجعة الداخلية لضمان أن عملياتها وأدواتها ومخرجاتها تفي بأعلى معايير الجودة والمصداقية، ويهدف هذا الدور إلى تعزيز الثقة في التقارير والنتائج التي تقدمها المراجعة الداخلية، مما يساعد المنظمة على تحقيق أهدافها بكفاءة وفعالية".
- **حوكمة الشركات:** "كما عرفت حوكمة الشركات بأنها "النظام الذي يتم من خلاله توجيه أعمال المنظمة ومراقبتها على أعلى مستوى من أجل تحقيق أهدافها والوفاء بالمعايير اللازمة للمسؤولية والنزاهة والشفافية
- **مفهوم إضافة القيمة:** "تعني قدرة المنشأة على تحقيق قيمة إضافية للمساهمين، وتعتبر نشاط مستقل واستشاري مصمم لإضافة قيمة للمنشأة ولتحسين عملياتها وهو يساعد الشركة على أنجاز أهدافها من خلال وجود منهج منظم ودقيق لتقويم وتحسين فعالية إدارة المخاطر، الرقابة، وعمليات الحوكمة".
- **إدارة (تحليل) المخاطر:** "إدارة المخاطر هي عملية منهجية تهدف إلى تحديد وتقييم ومراقبة المخاطر المتعلقة بحدوث عمليات الاحتيال في المنظمة، ووضع الضوابط والإجراءات اللازمة لمنعها أو اكتشافها والتعامل معها بفعالية".
- **مخاطر الأمن السيبراني:** "مخاطر الأمن السيبراني تشير إلى التهديدات أو الثغرات التي يمكن أن تستهدف الأنظمة الرقمية، الشبكات، أو البيانات، مما يؤدي إلى اختراقها أو تعطيلها أو إلحاق ضرر بالمنظمة أو الأفراد، وتتزايد هذه المخاطر مع تطور التكنولوجيا واعتماد المؤسسات المتزايد على الحلول الرقمية".

الفصل الثاني:

الإطار النظري والدراسات السابقة

المبحث الأول: المراجعة الداخلية

المبحث الثاني: الاتجاهات الحديثة للمراجعة الداخلية

المبحث الثالث: الحوكمة كاتجاه حديث للمراجعة الداخلية

المبحث الأول:

المراجعة الداخلية

- مفهوم المراجعة الداخلية
- مراحل التطور الزمني للمراجعة الداخلية
- أهداف المراجعة الداخلية
- أهمية المراجعة الداخلية
- أنواع المراجعة الداخلية
- وظائف المراجعة الداخلية
- مقومات المراجعة الداخلية

المبحث الأول:

المراجعة الداخلية

تمهيد:

تُعَدّ المراجعة الداخلية من الركائز الأساسية التي تعتمد عليها المؤسسات الحديثة في تعزيز كفاءة الأداء، وحماية الأصول، وتحسين جودة المعلومات، ودعم الإدارة في ممارسة وظائفها الرقابية والتنظيمية على نحو أكثر فاعلية. وقد شهد هذا المفهوم تطوراً ملحوظاً عبر الزمن، فلم يعد يقتصر على مجرد فحص السجلات والتحقق من صحة العمليات المالية، بل أصبح نشاطاً مهنيًا متكاملًا يجمع بين الدور التأكيدي والدور الاستشاري، ويسهم في تقييم نظم الرقابة الداخلية، وتعزيز الحوكمة، ودعم إدارة المخاطر، وإضافة قيمة حقيقية للمؤسسة. وانطلاقاً من هذه الأهمية، يتناول هذا المطلب مفهوم المراجعة الداخلية، ومراحل تطورها، وأهدافها، وأهميتها، وأنواعها، ووظائفها، ومقوماتها، بما يساعد على بناء إطار نظري واضح لهذا المتغير في الدراسة.

1.1.1. مفهوم المراجعة الداخلية

عرفت المراجعة الداخلية كمهنة منذ زمن بعيد إلا أن المراجعة الداخلية كمفهوم علمي لم يظهر إلا في الآونة الأخيرة وبصفة خاصة بعد إنشاء معهد المراجعين الداخليين الأمريكي في عام 1941، وقد تدرجت المراجعة الداخلية في دورها من القيام بالمراجعة المالية لتشمل أيضاً العمليات السائدة في المنشأة ثم أخذت تناقش المشاكل التي تواجهها عند القيام بهذه المراجعة مما ساعد على ظهور المبادئ الأساسية ومستويات الأداء الفني، وقد أدى ذلك بالمراجعين إلى تكوين أول منظمة مهنية لهم، وهي: "معهد المراجعين الداخليين في الولايات المتحدة الأمريكية سنة 1941م" (عبدالمغيث، 2022).

تولى معهد المراجعين الداخليين في الولايات المتحدة الأمريكية (IIA) مسؤولية تطوير مهنة المراجعة الداخلية، حيث نشأ عام 1941 بغرض تطويرها والاعتراف بها، والترويج لها كمهنة، وإيجاد أنظمة وقواعد ووضع معايير دولية لضبطها، وبرز دور (IIA) حينما أصدر في 1947 نشرة مسؤوليات المراجع الداخلي التي تحدد (طبيعة المراجعة الداخلية، أهدافها، مسؤوليات المراجع الداخلي). وفقاً للمعهد الدولي للمراجعين الداخليين (IIA)، تعرف المراجعة الداخلية بأنها:

"نشاط مستقل وموضوعي يوفر تأكيدات واستشارات مصممة لإضافة قيمة إلى المؤسسة وتحسين عملياتها. تساعد المراجعة الداخلية المؤسسة في تحقيق أهدافها من خلال تطبيق منهج منظم لتقييم وتحسين فعالية عمليات إدارة المخاطر والرقابة والحوكمة" (موسى، 2025).

كما عرفها الاتحاد الدولي للمحاسبين (IFAC) International Federation of Accountants بأنها: نشاط تأكيدي واستشاري يهدف إلى تقييم وتحسين فاعلية إدارة الوحدة للمخاطر وفحص وتقييم ورصد كفاية فاعلية الرقابة الداخلية (أيوب وفاتح، 2019).

كذلك يمكن تعريف المراجعة الداخلية بأنها نشاط رقابي مستقل يهدف إلى تقييم الأنشطة المالية والمحاسبية والتشغيلية، بالإضافة إلى قياس أداء الإدارات والأقسام داخل المنشأة، وذلك لخدمة الإدارة العليا وتحسين كفاءة العمل. يُعد المراجع الداخلي أحد موظفي المنشأة، وبالتالي يفترق إلى مستوى الاستقلالية الذي يتمتع به المراجع الخارجي. بناءً على هذا التعريف، يمكن تصنيف المراجعة الداخلية إلى أربعة أنواع رئيسية:

- **المراجعة المالية:** تُعنى بفحص السجلات المالية والتأكد من صحتها ودقتها.
- **مراجعة الامتثال:** تهدف إلى التحقق من الالتزام باللوائح والقوانين والسياسات الداخلية.
- **مراجعة الأداء:** تركز على تقييم كفاءة العمليات التشغيلية وفعاليتها.
- **مراجعة نظم المعلومات:** تتضمن فحص أمن الأنظمة الإلكترونية وفعاليتها لضمان حماية المعلومات واستمرارية العمل.

من العرض السابق يرى الباحث أن المراجعة الداخلية تُعد وسيلة رقابية محايدة ذات طابع وقائي، حيث تغطي العمليات المالية والمحاسبية وتعمل على دعم الإدارة. كما تُعتبر ركيزة أساسية لضمان نجاح المؤسسات واستدامتها. ولا تقتصر وظيفتها على كشف الأخطاء فقط، بل تسهم بشكل استراتيجي في تحسين الأداء وتعزيز الحوكمة والحد من المخاطر.

1.2.2: مراحل التطور الزمني للمراجعة الداخلية

تُعرف المراجعة الداخلية كمفهوم تطوّر عبر السنوات وفق تعريفات متعددة أصدرها معهد المراجعين الداخليين منذ تأسيسه. ففي عام 1941، وُصفت المراجعة الداخلية بأنها نشاط تقويمي مستقل يُمارس داخل المؤسسة بهدف مراجعة العمليات المالية والمحاسبية وغيرها من العمليات، بغرض توفير خدمات وقائية وبناءة للإدارة. اعتُبرت آنذاك أداة للرقابة الداخلية تقيس وتقيم مدى

فعالية وسائل الرقابة الأخرى، مع التركيز بشكل أساسي على الجوانب المالية والمحاسبية، وأحيانًا الجوانب التشغيلية. وعلى مدار الزمن، تطورت هذه الرؤية؛ ففي عام 1957، أدخل المعهد أول تعديل على التعريف ليصبح المراجعة الداخلية نشاطًا تقويميًا محايدًا داخل المؤسسة يركّز على مراجعة العمليات المحاسبية والمالية وغيرها. وتم اعتباره جزءًا من نظام الرقابة الإدارية الشاملة، حيث يعمل على قياس وتقييم فعالية نظم الرقابة الأخرى. ثم جاءت النسخة المحدثه والأكثر شمولية لتعريف المراجعة الداخلية في عام 1999، هذا التعريف قدّم رؤية متطورة حيث وصف المراجعة الداخلية بأنها نشاط استشاري وموضوعي يهدف إلى تقديم ضمانات وتحسين العمليات داخل المنشأة. وتهدف المراجعة الداخلية في هذا السياق إلى تحقيق أهداف المؤسسة من خلال اتباع منهج منظم ومنضبط لتقييم وتعزيز كفاءة إدارة المخاطر ونظم الرقابة والتحكم (Gay,2020).

يتضح من التعريف الحديث والصادر عن معهد المراجعين الداخليين أنه يعكس التقدم والتطورات التي شهدتها المراجعة الداخلية، كما يراعي احتياجات الإدارة بوصفها العميل الرئيسي لهذه العملية. يُظهر التعريف مرونة في تحديد الجهة المسؤولة عن تنفيذ المراجعة الداخلية، سواء كانت داخل المنشأة ممثلة في إدارة المراجعة الداخلية، خارجيًا عن طريق التعاقد، أو بالاعتماد على مصادر مشتركة داخل المنشأة. هذه المرونة تمنح المنشأة حرية اختيار الطريقة الأنسب وفقًا لظروفها واحتياجاتها. التعريف الأخير لا يخفي أهمية تقييم الرقابة الداخلية، بل يعزز أهمية الحوكمة المتزايدة، مشيرًا إلى الدور الأساسي لأنظمة الرقابة في دعم إدارة المخاطر (عبدالغيث، 2022).

يلاحظ الباحث أن مهنة المراجعة مرت بعدة مراحل تطور وهي عبارة عن عملية منظمة تتم وفق خطة محددة لجمع أكبر قدر من الأدلة لأبداء رأي فني محايد عن مدى عدالة وصدق القوائم المالية للشركة.

جدول رقم (1) مراحل تطور المراجعة الداخلية

المرحلة الأولى منذ عام 1941 حتى 1971	انحصر دور المراجعة الداخلية خلال هذه الفترة في التأكد من دقة وصحة البيانات المسجلة في الدفاتر والسجلات، مع التركيز بشكل أساسي على العمليات المالية فقط.
المرحلة الثانية منذ عام 1971 حتى 1981	شهد دور المراجعة الداخلية تطوراً ليشمل التحقق من دقة وسلامة حسابات المنشأة والقوائم المالية، مع الاهتمام بملكية الأصول والعمل على حمايتها.
المرحلة الثالثة منذ عام 1981 حتى 1999	استمر نطاق المراجعة الداخلية في التوسع ليضم تقييم مدى كفاءة وفعالية مختلف الجوانب المتعلقة بالرقابة الداخلية، بهدف تعزيز ودعم النظام الرقابي بالمنشأة.
المرحلة الرابعة منذ عام 1999 حتى الآن	أصبح دور المراجعة الداخلية أكثر تطوراً وتحول إلى دور استشاري يركز على تقديم قيمة مضافة للإدارة. يهدف هذا الدور إلى تحسين كفاءة عمليات الرقابة ودعم إدارة المخاطر وتعزيز مبادئ والحوكمة.

المصدر: إعداد الباحث، 2026م.

1.2.3: أهداف المراجعة الداخلية:

تهدف المراجعة الداخلية بشكل أساسي إلى دعم الإدارة في تحقيق أهدافها. من خلال إجراء مراجعات شاملة لجميع العمليات المالية داخل المنشأة، تسعى المراجعة الداخلية إلى مساعدة الإدارة العليا في الوصول إلى أقصى مستوى ممكن من الكفاءة الإنتاجية. لتحقيق هذا الهدف، يتم التركيز على التأكد من عدة أمور، تشمل حماية الإدارة ومصالح الشركة من مخاطر الغش، والأخطاء، والضياع، والانحراف عن الإجراءات، ومخالفة السياسات المحددة. تُبرز المراجعة كذلك نقاط الضعف من خلال فحص دقة البيانات المحاسبية واختبار الأساليب المتبعة لحماية الأصول. وللاضطلاع بهذه المسؤوليات بكفاءة، يحتاج المراجع الداخلي إلى درجة عالية من المهارة والخبرة (الريح، 2019).

تعد أهداف المراجعة الداخلية من المهام الأساسية التي يجب تنفيذها لتحقيق أفضل النتائج. وفقاً لما حدده معهد المراجعين الداخليين (IIA)، فإن الهدف العام للمراجعة الداخلية يتمثل في تحسين العمليات المؤسسية وإضافة قيمة إليها. بالإضافة إلى ذلك، تم إدراج بعض الأهداف الأخرى، ومنها ما يلي (أبو زيد وأبوزقية، 2024) نقلاً (الشوا، 2014):

- ضمان الالتزام بالسياسات والإجراءات ووسائل الرقابة الداخلية المعتمدة على جميع المستويات الإدارية.
- دعم المؤسسات في تحقيق أهدافها بشكل فعال.
- مساندة المسؤولين في أداء مهامهم وتحمل مسؤولياتهم بكفاءة وفعالية.
- تعزيز الرقابة وتحسين إدارة المخاطر داخل المؤسسات مع الحفاظ على تكاليف معقولة.
- رفع قيمة المؤسسة وتحسين كفاءة عملياتها التشغيلية.
- تقييم وتعزيز فعالية إدارة المخاطر وحوكمة الشركات.

يرى الباحث أن تعريف معهد (IIA) الصادر في عام 2001، يشير إلى وجود مجموعة من الأهداف المهمة التي يمكن استخلاصها، والتي تشمل مساعدة المنشأة في تحقيق أهدافها، تقييم وتحسين عمليات إدارة المخاطر والرقابة والحوكمة، بالإضافة إلى تعزيز القيمة. ومن منظور آخر، يعتقد الباحث أن الهدف الأساسي للمراجعة الداخلية يكمن في دعم الإدارة في أداء مسؤولياتها بشكل فعال، وذلك خاصة في مجالات حماية الأصول، الحفاظ على سجلات محاسبية دقيقة يمكن الوثوق بها، وتنفيذ العمليات بكفاءة. ويتم تحقيق ذلك من خلال تقديم تحليلات وتوصيات للإدارة تتعلق بالأنشطة التي تخضع للفحص. في ضوء ذلك، يلخص الباحث أهداف المراجعة الداخلية على النحو التالي:

1. ضمان صحة البيانات المحاسبية والإحصائية.
2. حماية أموال المنشأة عبر وضع وتنفيذ أنظمة رقابية فعالة تساهم في حماية الموارد المالية من أي تلاعب أو اختلاس قد يرتكبه الموظفون.
3. متابعة تنفيذ السياسات والخطط الموضوعية وتقييم مدى فعاليتها.

1.2.4. أهمية المراجعة الداخلية:

تتمثل أهمية المراجعة الداخلية في الآتي:

1. توسّع حجم الشركات وامتدادها الجغرافي بشكل كبير أدى إلى زيادة الفجوة بين الإدارة العليا وجميع العاملين(الجرعاني،2015).
2. تتطلب إدارة الشركة توفر بيانات ومعلومات موثقة في التقارير لضمان تحقيق الدقة في العمل، ما يستدعي وجود نظام مراجعة داخلية قوي وسليم(حسين وآخرون، 2016).
3. تُعد المراجعة الداخلية المصدر الرئيسي للمعلومات الموثوقة، خاصة بعد تحول المراجعة الخارجية إلى خيار اختياري واعتماد أسلوب اللامركزية في المؤسسات الكبيرة، مما يساهم في تحسين توزيع الموارد المتاحة بشكل أمثل (داما،2018).
4. تتبع المراجعة التأكد من الالتزام بالإجراءات الموضوعية ومن كفاءة وفعالية الأداء الإداري.

5. أسهمت إعادة تفعيل مبادئ حوكمة الشركات في تعزيز الحاجة إلى دور المراجعة الداخلية. فبموجب تطبيق هذه المبادئ، يقع على عاتق المساهمين، ممثلين في الجمعية العامة لشركات المساهمة، مسؤولية اختيار كل من المراجع الخارجي والمراجع الداخلي بناءً على توصية تقدمها لجنة المراجعة، وليس بتشريح الإدارة التنفيذية للشركة كما تتشكل لجنة المراجعة من أعضاء مجلس الإدارة من غير التنفيذيين حتى تكون مستقلة، وبالتالي تقوم بتوفير الاستقلالية لكل من المراجع وظيفة رقابية تمتد إلى الجوانب المالية والتشغيلية بالشركة كلها(محمد علي،2019).

6. بعض الشركات لها فروع متباعدة عن المركز الرئيسي مما أدى إلى ضرورة الحاجة لتتبع سير العمل بتلك الفروع، ومعرفة ما يتم بها من معاملات، والتأكد من أن العمل يتم وفقاً للسياسات والخطط الموضوعية من المركز مما يحتم وجود نظام مراجعة داخلية فعال بتلك الفروع لغرض الرقابة اللازمة عليها(فضل الله والعريبي، 2024).

أهمية المراجعة الداخلية بالنسبة للإدارة:

تم إنشاء المراجعة الداخلية في الأصل داخل الشركة لضمان كفاءة سير العمليات، والتحقق من سلامة الأصول وحمايتها من الإهمال أو فقدان أو سوء الإدارة أو الاختلاس(أبو راوي،2011).

تظهر أهمية المراجعة الداخلية من خلال الخدمات التي تقدمها للإدارة وهي كما يلي (سيد، 2012):

- أ. **خدمات تقويمية:** تهدف هذه الوظيفة إلى تقييم مدى كفاءة نظم الرقابة وإجراءاتها داخل الشركة، بالإضافة إلى قياس مستوى الالتزام بالسياسات الإدارية المعتمدة.
- ب. **خدمات وقائية:** تركز وظيفة المراجعة الداخلية على ضمان توفير الحماية الكافية للأصول وصيانة السياسات الإدارية من أي انحرافات تحول دون تطبيقها بشكل فعلي.
- ت. **خدمات تطويرية:** تتولى هذه الوظيفة تقديم اقتراحات لتحسين الأنظمة المعتمدة داخل الشركة، مع ضمان توفير المعلومات الدقيقة للإدارة وتعزيز سلامتها.

أهمية المراجعة الداخلية بالنسبة للمراجع الخارجي:

يُعد نظام المراجعة الداخلية عاملاً أساسياً بالنسبة للمراجع الخارجي، الذي يتولى تقديم تقرير مستقل عن القوائم المالية للمنشأة. ومن المعروف أن المراجعة الخارجية قد تطورت في العصر الحديث من كونها مراجعة تفصيلية شاملة إلى مراجعة اختبارية تعتمد على العينات. يأتي هذا التحول نتيجة لتزايد حجم الشركات، وتعدد عملياتها وتعقيداتها، مما استوجب تقليل تكلفة المراجعة. بناءً على ذلك، أصبح المراجع الخارجي يعتمد بصورة متزايدة على دور المراجع الداخلي لتجنب تكرار الجهود وإنجاز العمل بكفاءة أكبر (سالم، 2012).

إن وجود إدارة مستقلة للمراجعة الداخلية يحقق مجموعة من المنافع والفوائد أهمها (محمد علي، 2019):

1. تجنب التكاليف المرتفعة التي تتطلبها عملية المراجعة الداخلية المستمرة من قبل المراجع الخارجي.

2. التأكد من دقة المعلومات الواردة في التقارير المالية، بالإضافة إلى تقيد الوحدات المحاسبية المختلفة بالتعليمات المحددة لإعداد هذه التقارير بملء ودقة وكفاءة.

3. التأكد من دقة المعلومات الواردة في التقارير المالية، بالإضافة إلى تقيد الوحدات.

يخلص الباحث إلى أن أهمية المراجعة الداخلية تظهر من خلال النقاط التالية:

- تتحمل إدارة المنشأة المسؤولية الأساسية عن تصميم وتنفيذ نظام فعال للرقابة الداخلية بهدف منع واكتشاف الأخطاء الجوهرية، بما يساهم في ضمان إعداد قوائم مالية موثوقة والالتزام

بالقوانين واللوائح ذات الصلة. وتعتبر المراجعة الداخلية عنصراً محورياً لنجاح هذا النظام وتحقيق أهدافه بكفاءة.

في ظل الأزمات المالية وما تبعها من تداعيات اقتصادية، انعكس ذلك على مستخدمي القوائم المالية، مما أدى إلى تراجع الثقة في مصداقية المعلومات المحاسبية. نتيجة لذلك، لم يعد دور المراجعة الداخلية يقتصر على تقديم خدمات التأكيد فقط، بل تطور ليصبح جزءاً لا يتجزأ من الإدارة. إذ تسهم المراجعة الداخلية في تقديم خدمات إضافية مثل تقييم أداء العاملين وتزويد الإدارة بالمعلومات الدقيقة والملائمة حول المخاطر المحتملة التي قد تواجه المنشأة.

1.2.5: أنواع المراجعة الداخلية:

تساير المراجعة الداخلية حاجات المنشأة المتنامية، ويتضح ذلك من خلال أنواع المتعددة:

1. **المراجعة المالية:** تشمل مراجعة العمليات والوثائق المالية والمحاسبية.
2. **المراجعة الإدارية:** تشمل فحص الإجراءات الرقابية الخاصة بالنشاطات غير المالية والمحاسبية (الوردات، 2014).
3. **مراجعة الالتزام:** تهدف للتأكد من أن المنشأة تعمل على بما يتفق مع القوانين والتعليمات المنظمة لعملها أو الالتزامات التعاقدية المفروضة عليها، بالإضافة إلى السياسات والإجراءات المقررة من الإدارة.
4. **مراجعة العمليات:** تهدف إلى اختبار ما إذا كانت وظائف المنشأة تنجز أهدافها بشكل فعال وبكفاءة.
5. **مراجعة نظم المعلومات:** تهدف إلى اختبار أمن تشغيل بيانات نظم المعلومات ونزاهتها بالإضافة إلى البيانات التي اخرجتها هذه النظم (نورالدين، 2015).
6. **مراجعة الأداء:** تتضمن مراجعة الاقتصادية والفعالية وهي مراجعة برنامج أو نشاط يتعلق أساساً في الفعالية الاقتصادية لوظيفة معينة. ومراجعة البرامج وهي مراجعة برنامج أو نشاط محدد يركز على المخرجات من حيث كفاءتها.
7. **مراجعة البيئة:** تركز على التحقق من الالتزام بالقوانين البيئية المعمول بها، وتقييم نظم إدارة البيئة لضمان أن العمليات الحالية لن تواجه مخاطر بيئية مستقبلية. كما تشمل مراجعة الأضرار البيئية المحتملة المرتبطة بتسهيلات المعالجة والتخزين والتخلص من النفايات. تُعنى أيضاً

بمراجعة الجهود المبذولة للحد من التلوث ومتابعة الالتزامات البيئية، بالإضافة إلى مراجعة تأثير المنتجات من منظور بيئي (بن عطف، 2021).

1.2.6: وظائف المراجعة الداخلية:

تتمثل وظائف المراجعة الداخلية في وظيفتين أساسيتين

أ. **وظيفية تأكيدية:** تركز العملية على تقييم الأدلة بشكل موضوعي بهدف تقديم رأي مستقل أو استخلاص استنتاجات تتعلق بعملية معينة، نظام، أو موضوعات أخرى ذات صلة. يتولى المراجع الداخلي تحديد طبيعة ونطاق مهمة التأكيد، ويشترك في خدمات التأكيد ثلاثة أطراف رئيسية: الجهة أو الأفراد المشاركون في العملية، المراجع الداخلي أو الفريق المسؤول عن التقييم، والجهة أو الأفراد المستفيدون من نتائج التقييم (عطف، 2021).

ب. **وظيفة استشارية:** تتمثل في تقديم توجيهات تُنفَّذ بناءً على طلب محدد من العميل. وتتحدد طبيعة ونطاق المهمة الاستشارية وفقاً لما يتم الاتفاق عليه مع العميل. وتشمل الخدمات الاستشارية طرفين رئيسيين: الأول هو الشخص أو المجموعة التي تقدّم الخدمة، ويُطلق عليها "المراجع الداخلي"، والثاني هو الشخص أو المجموعة التي تطلب النصيحة وتستلمها، وهو ما يُشار إليه بعملية المهمة (الوردات، 2017).

1.2.7: مقومات المراجعة الداخلية

يمكن تلخيص أهم ركائز المراجعة الداخلية في النقاط التالية (محمد، 2017):

1. **قسم مستقل للمراجعة الداخلية:** يمثل استقلال قسم المراجعة الداخلية أساساً مهماً لضمان

جودة عمله وقيمه. لضمان هذا الاستقلال، يمكن اتباع الآتي:

أ. تعيين المراجع الداخلي: بما أن المراجعة الداخلية تمثل الوسيلة التي تستخدمها الإدارة لمتابعة الأداء والتحقق من الالتزام، فإن تعيين المراجع الداخلي يجب أن يكون من مسؤولية الإدارة العليا للشركة.

ب. تجنب القيام بالأعمال التنفيذية: على المراجع الداخلي إدراك أن دوره يقتصر على تقديم المشورة وتحليل العمليات دون أن يتدخل مباشرة في تنفيذها. عليه الامتناع عن القيام بأي أعمال تقع ضمن اختصاصات الأقسام الأخرى بالشركة.

2. فريق مؤهل للمراجعة الداخلية: يجب أن يتضمن قسم المراجعة الداخلية أفرادًا يمتلكون المؤهلات العلمية والخبرة المهنية المناسبة، لضمان تنفيذ مهام المراجعة بدقة وكفاءة.
3. نظام رقابة داخلية فعال: يجب أن يتمتع نظام الرقابة الداخلية بالكفاءة لتوفير معلومات دقيقة وموثوقة، والالتزام بالخطط والسياسات والإجراءات المطبقة في الشركة.
4. تقارير فعالة وواضحة: ينبغي إعداد تقارير ذات قيمة مضافة تستند إلى آراء مستقلة للمراجعين الداخليين، وتُعرض بشكل مفهوم ومحدد يلبي احتياجات الأطراف المعنية.
5. استمرارية المراجعة: تقوم أقسام المراجعة الداخلية بتنفيذ مهامها بشكل مستمر طوال العام، مع الحرص على تقييم العمليات فور تسجيلها في الدفاتر والسجلات.

المبحث الثاني:

الاتجاهات الحديثة للمراجعة الداخلية

تمهيد:

في ظل التغيرات المستمرة في بيئة الأعمال وارتفاع تكاليف المنافسة، أدركت معظم المؤسسات المالية أن اقتصار مهام المراجعة الداخلية على فحص وتدقيق نظم الرقابة الداخلية بات نهجاً تقليدياً. لذا، أصبح من الضروري أن تتحول المراجعة الداخلية إلى نشاط يضيف قيمة ملموسة ويلبي احتياجات أصحاب المصلحة المتعددة. لتحقيق ذلك، ينبغي أن تقوم المراجعة الداخلية بدور استراتيجي يتضمن تقييم وتحسين إدارة المخاطر، والرقابة، والحوكمة. يتضح هذا الدور من خلال التعريف الحديث للمراجعة الداخلية الذي يعتبرها نشاطاً مستقلاً وموضوعياً يجمع بين الخدمات التأكيدية والاستشارية. وتهدف المراجعة الداخلية إلى تعزيز قيمة المؤسسة وتحسين عملياتها عبر تطبيق منهجية منظمة لتقييم فعالية إدارة المخاطر والرقابة وحوكمة الشركات والعمل على تحسينها. بناءً على هذا التعريف، تغيرت النظرة التقليدية الضيقة للمراجعة الداخلية. مع اشتداد المنافسة والانفتاح العالمي، أصبح امتلاك الشركات لميزة تنافسية هدفاً استراتيجياً تسعى لتحقيقه. وبالتالي، فإن الشركات التي لا تركز على تطوير خدمات جديدة وتسويقها بشكل فعال تواجه خطر فقدان تنافسيتها وحتى خطر الزوال. في مواجهة هذه التحديات، تلعب المراجعة الداخلية دوراً استراتيجياً في تمكين المؤسسات المالية من تلبية احتياجات عملائها وإدارة المخاطر بفعالية (محمد علي، 2019).

وبناءً على ما سبق تعد المراجعة الداخلية أحد أهم آليات حوكمة الشركات التي تعتمد عليها للحد من تضارب المصالح وحماية جميع الأطراف، وقد شهدت المراجعة الداخلية تطوراً ملحوظاً خلال الآونة الأخيرة، كما تنوعت المهام التي تقوم بها داخل المنشأة، فلم تعد تنحصر مهامها في فحص العمليات المالية والمحاسبية، بل أصبحت إحدى الوسائل الإدارية المهمة التي يعتمد عليها مجلس الإدارة ولجنة المراجعة في تقييم كفاءة وفعالية نظام الرقابة الداخلية بهدف خدمة المنشأة. وهذا المنظور يعمل على توسيع نطاق عمل المراجعة الداخلية ليشتمل على إدارة المخاطر والرقابة والحوكمة، كما أن المعايير الصارمة لمهنة المراجعة الداخلية تضمن جودة المهنة (بن عطف، 2021).

وفي سياق متصل، تبرز أهمية المراجعة الداخلية في تقديم إسهامات جوهرية تتعلق بالقضايا الاستراتيجية داخل المنشأة، لاسيما في مجال الأمن السيبراني. فهي تُعد من الركائز الأساسية التي تلبي تطلعات مختلف الأطراف ذات المصلحة، وخاصة المستثمرين، من خلال إعداد تقارير تفصيلية حول كفاءة هيكل الرقابة الداخلية. كما تسهم المراجعة الداخلية في تقديم رؤية أكثر شمولية عن أداء الإدارات والأقسام والمراكز داخل المؤسسة، بالإضافة إلى تحديد المخاطر المحتملة التي قد تواجهها. وتتميز أيضاً بقدرتها على متابعة تنفيذ قرارات مجالس الإدارة بفعالية (شحاتة، 2020).

2.2.1: إدارة المخاطر كاتجاه حديث للمراجعة الداخلية:

أسفرت الأزمات المالية التي أثرت على المؤسسات الاقتصادية والمالية عن ضرورة تبني نهج جديد للمراجعة الداخلية، بحيث يمكّنها من مواجهة المخاطر التي تعيق تحقيق أهدافها. وقد تطلب ذلك الانتقال من التركيز على تقييم نظم الرقابة الداخلية والأنشطة التشغيلية إلى مستوى أكثر استراتيجية في الممارسات. تمثل هذا الانتقال من خلال اعتماد منهج المراجعة الداخلية القائم على المخاطر. ووفقاً لتعريف المراجعة الداخلية الصادر عن معهد المدققين الداخليين (IIA) (2001)، تبرز أهمية المراجعة الداخلية في إضفاء قيمة حقيقية على المنشأة، عبر تعزيز كفاءة نظم الرقابة الداخلية وإدارة المخاطر والحوكمة. ويتم ذلك من خلال تخفيض التكاليف، واكتشاف الاحتيال، وتقييم نظم الرقابة الداخلية، وتقديم المقترحات اللازمة لمساعدة المنشآت في تحقيق أهدافها عبر تحسين أدائها وعملياتها. ويعكس هذا النهج الحديث صورة مختلفة ومتطورة للمهنة في عدة أبعاد، كما ذكر النجار (2013) ومع بدء تنفيذ الاتفاقية العامة للتعريف والتجارة، توسع دور المراجعة الداخلية ليشمل التأكد من التزام المنشآت بالمعايير والمواصفات الدولية للجودة (وهدان، 2022).

وظيفة المراجعة الداخلية تعتبر عنصراً أساسياً يدعم الإدارة في أداء مهامها المتعلقة بالرقابة ومتابعة الأداء، كما تساعد على تقييم مدى نجاح الإدارة في الحفاظ على أصول الشركة وتحقيق الأهداف المحددة. توفر هذه الوظيفة للإدارة العليا المعلومات الضرورية لاتخاذ القرارات الدقيقة، بالإضافة إلى تقديم صورة واضحة عن فعالية نظام الرقابة الداخلية المعتمد في الشركة. تُشكل المراجعة الداخلية جزءاً حيوياً من هيكل الإدارة، حيث تقوم بأعمال إدارية تدعم الإدارة

العليا بتقديم معلومات دقيقة وفي الوقت المناسب بشأن المخاطر التي قد تواجه المنشأة؛ إلى جانب ذلك، تشمل مهامها التقليدية حماية أصول الشركة من أي تصرفات غير مرغوب فيها، وضمان التزام الموظفين بالسياسات والإجراءات المعمول بها (هيكل، 2012).

2.2.2: مفهوم إدارة المخاطر

كلمة خطر مستمدة من الكلمة الإيطالية (Risicare) بمعنى يجرأ أي هي اختبار وليست مصير فهي الخسارة المتوقعة في ظل حدث معين. تعددت التعريفات الخاصة بإدارة المخاطر وذلك بتعدد المعايير والأطر الدولية الخاصة بالمخاطر فقد عرفها المعيار البريطاني بأنها الجمع بين احتمال حدوث حدث ما مع نتائجه (محمد، 2017).

يمكن تعريف إدارة المخاطر على أنها هي "عملية اتخاذ القرار لمواجهة أي خطر من الأخطار التي تتعرض لها منشآت الأعمال أو الأفراد ويتم ذلك عن طريق التعرف على مصادر الخطر المختلفة، وتقدير ناتج تلك المسببات مقدماً، وما قد يترتب على تحققها في صورة حوادث ثم اختيار أفضل الأساليب والوسائل إلى منع و التقليل من الخسائر المادية والمالية المحتملة التي تنتج عن تحقق تلك الحوادث وذلك بأقل تكلفة ممكنة (عريقات وعقل، 2010).

عرفت لجنة COSO إدارة المخاطر الخاصة بالمنشأة بأنها عملية بمجلس إدارة الوحدة والإدارة والعاملين تنطوي على الرقابة الداخلية وتطبق ضمن استراتيجية المنشأة وهي مصممة لتوفير تأكيد معقول فيما يتعلق بتحقيق الأهداف في الأمور الخاصة بكفاءة وفاعلية العمليات وإمكانية الاعتماد على تقرير المالي والالتزام باللوائح والقوانين المطبقة (عبد الوهاب، 2009).

كذلك عرفت إدارة المخاطر من قبل معهد إدارة المخاطر بأنها مجموعة من الإجراءات والعمليات التي تستخدمها إدارة المنظمة بهدف مواجهة الفرص والتهديدات والآثار المترتبة عليها (سمرة، 2011).

يمكن للباحث تعريف إدارة المخاطر على أنها استراتيجية تعتمد على الإدارة بهدف تحديد الأحداث المحتملة التي قد تؤثر على المنشأة والسعي لتجنبها.

يرى الباحث أن مفهوم إدارة المخاطر يرتبط بمساندة الإدارة في تحقيق أهداف الأداء والربحية، مع تقليل احتمالية فقدان الموارد المتاحة. كما أنها تساهم في الوصول إلى المكانة المنشودة وتجنب الإخفاقات والأزمات التي قد تواجه المؤسسة خلال مسيرتها.

2.2.3: أهداف إدارة المخاطر:

يعتبر الهدف الأساسي لإدارة المخاطر هو الوصول إلى أفضل طريق للمحافظة على الأموال وحماية كفاءة أنشطة منشآت الأعمال؛ والأشخاص المالكين له؛ وحماية العاملين به من الخسائر المادية المحتملة الناشئة عن تحقق الأخطار البحتة (الصافية) التي تواجه بأقل تكلفة (عريقات وعقل؛ 2010).

والهدف من عملية ضبط المخاطر وإدارتها في الوحدات الاقتصادية هي المحافظة على أصولها وحمايتها من الخسائر التي يمكن أن تتعرض لها لتحقيق الهدف الأساسي لأي وحدة اقتصادية وهو البقاء والنمو.

وتهدف إدارة المخاطر إلى تقليل الآثار السلبية المترتبة على وقوع خطر ما؛ وهناك هدف مهم لهذه الإدارة ويتمثل في وضع السياسات والإجراءات العملية لمواجهة أي خطر؛ من أجل الحد من الخسائر المادية والبشرية التي يحتمل وقوعها نتيجة لحدوث هذا الخطر، مع توضيح الإستراتيجية الكاملة لجميع أفراد الشركة في كيفية التعامل مع هذا الخطر عند حدوثه، وعلى هذا فإن الهدف الرئيسي من تفعيل دور إدارة المخاطر بالمنشأة هو أن كل منشأة سواء هادفة للربح أو غير هادفة للربح أو ذات كيان حكومي، تحاول تعظيم قيمة المنظمة في ظل حالة من عدم التأكد والمخاطرة، وتتبع حالة عدم التأكد والمخاطرة من عدم قدرة إدارة المنشأة على تحديد احتمال وقوع الأحداث بدقة، وذلك الضغوط المرتبطة بها وتبعياتها. (شاهنده، 2013).

ويمكن أن تتلخص أهداف إدارة المخاطر في الآتي (عمر، 2023):

- البقاء: بوضع حد أقصى لتكلفة الخسائر التي تهدد بقاء المشروع.
- الاقتصاد: بتخفيض تكلفة إدارة الأخطار.
- الأمان: بتخفيض حالة القلق.
- الحفاظ على مستويات دخل مستقرة: من خلال ضمان استمرار المشروع عقب تعرضه لحادث بضمان توافر التمويل اللازم للخسارة عقب الحادث.
- القيام بالالتزامات الاجتماعية تجاه العمال والمجتمع: من خلال دفع أجور العمال خلال فترات التوقف وتركيب معدات أمان تزيد تكلفتها عن تعويض إصابة العمل.

في ضوء ما تقدم يستنتج الباحث أن إدارة المخاطر تعمل كوسيلة لمواجهة المخاطر قبل حدوثها.

2.2.4: أهمية إدارة المخاطر

تتمثل أهمية إدارة المخاطر في أنها لا تنتظر فقط للظروف الحالية من ظروف السوق وتقبل الرقابة على موجودات المنشأة ومدى استقرار المركز المالي لها؛ بل أنها تهتم بما تتعرض له المنشأة مستقبلاً من أخطار محتمل حدوثها حتى تستطيع مواجهة ذلك الخطر أو تفاديه؛ لذلك أصبحت الحاجة ملحة إلى إيجاد إطار عمل محدد وواضح من أجل التطبيق الفعال لإدارة المخاطر؛ وتبيان دورها في تحقيق الأهداف الاستراتيجية؛ وكذلك دعم قدرتها على الاستمرار في مزاوله نشاطها في دنيا الأعمال؛ الأمر الذي وجه مزيد من الإنتباه صوب التعامل مع المخاطر التي تواجهها المنشآت من أجل السيطرة عليها.

وتحمل إدارة المخاطر أهمية كبيرة للشركات؛ ويحقق تطبيق إدارة المخاطر الآتي: تحقيق أهداف الشركة؛ التركيز بشكل أكبر على أولويات الأعمال؛ تغيير الثقافة التنظيمية إلى نقاشات مفتوحة حول المخاطر؛ تحسين الإدارة المالية والتشغيلية من خلال التأكد من أن المخاطر تم تقديمها بشكل دقيق في عملية اتخاذ القرار؛ دعم عملية التخطيط من خلال كون إدارة المخاطر إحدى الوسائل لتحديد الفرص (النتائج الإيجابية للمخاطرة). (شيماء 2012).

تساعد إدارة المخاطر على التعامل مع ظروف عدم التأكد وما ينتج عنها من مخاطر وفرص، تحمي وتضيف قيمة للأصحاب المصالح من خلال الآتي (عبد الفتاح، 2012):

- أ. تحليل وتقييم المخاطر المتعلقة بالأنشطة والمنتجات والخدمات الجديدة والقائمة.
- ب. تقليص لفرص المنشآت للمفاجآت أو الأزمات الخائفة.
- ج. إعداد ومتابعة التقارير والجداول والمؤشرات لمتابعة قياس وإدارة المخاطر.
- د. يوفر التصميم الجيد والدقيق لإدارة المخاطر بالمنشأة تأكيداً معقولاً عن مدى تحقيق أهداف المنشأة بالتعامل مع المخاطر.
- هـ. زيادة إمكانية إنجاز الأهداف الاستراتيجية.
- و. توفير معلومات حول المخاطر لدى المصرف لاستخدامها لأغراض الإفصاح للجمهور.

2.2.5: أنواع إدارة المخاطر:

إن أنواع إدارة المخاطر تتمثل ف الاتي : (حمدي، 2007):

- أ- إدارة المخاطر التقليدية: إن إدارة المخاطر التقليدية تركز على تلك المخاطر الناتجة عن أسباب مادية أو قانونية (مثال: الكوارث الطبيعية أو الحوادث، الموت والدعاوى القضائية).
 - ب- إدارة المخاطر المادية: وهي أحد أشكال المخاطر التي تركز على تلك المخاطر التي يمكن إدارتها باستخدام أدوات المقايضة المالية.
 - ج- إدارة المخاطر المثالية: تركز إدارة المخاطر المثالية على إعطاء الأولويات، بحيث أن المخاطر ذات الخسائر الكبيرة واحتمالية حدوث خسائر عالية تعالج أولاً، بينما المخاطر ذات الخسائر الأقل واحتمالية حدوث أقل تعالج فيما بعد.
- وعليه يتضح للباحث أنه لا بد من تقديم اقتراحات لازمة لتطوير فعالية إدارة المخاطر بالمنشأة كما لا بد من تصميم نظم طبقاً للعوامل المؤثرة على دور المراجعة الداخلية في تفعيل إدارة المخاطر.

2.2.6: المقومات الأساسية لإدارة مخاطر المنشأة

يرى البعض أن أنشطة إدارة المخاطر أصبحت ضرورية لمساعدة المنشآت في تحقيق أهدافها غير أن ممارسة إدارة المخاطر بشكل فعال يتطلب تحقيق التكامل بين ثلاثة عناصر على الأقل هي (عمر، 2017):

1. دراسة وفهم أعمال وأنشطة المنشأة.
 2. إدراك النتائج أو التأثيرات المحتملة التي يمكن أن تتولد عن المخاطر.
 3. الفهم الجيد للإطار العام لنموذج الخطر.
- ويضيف آخر أن عملية إدارة المخاطر ما هي إلا منهج منظم ومنطقي يقوم على مجموعة من الإجراءات والأساليب المتعلقة بالمخاطر متضمنة الآتي:

- أ. إنشاء نطاق إدارة المخاطر.
- ب. التحديد والتحليل للمخاطر المرتبطة بأي نشاط.
- ج. التقييم والمعالجة للمخاطر المرتبطة بأي نشاط.
- د. المتابعة والمراجعة المستمرة لإدارة المخاطر.

هـ. الاتصال والتشاور في جميع مراحل عملية إدارة المخاطر.
يستخلص الباحث مما سبق أن إدارة المخاطر هي وسيلة نظامية لتحديد المخاطر، وكذلك تطبيق المنهج المناسب للتقليل منها وتتضمن هذه الوسيلة كل من الوقاية من المخاطر المحتملة والاكتشاف المبكر للمشاكل الفعلية والعمل على تصحيحها.

2.2.7: منهجية إدارة المخاطر:

لتنقيد عملية المراجعة إدارة المخاطر بالشكل الصحيح والفعال لابد من تحديد الخطوات العلمية والعملية اللازمة لذلك ويطلق على هذه الخطوات الإطار العام لإدارة المخاطر، وقد تعددت آراء الباحثين حول تحديد هذه الخطوات نذكر أهمها: (جيهان، 2014):

أ. تحديد المخاطر: ويقصد بها أن كافة المخاطر المرتبطة بالأنشطة قد تم تحديدها بوضوح.

ب. تقييم المخاطر: ويقصد بها أن المخاطر قد تم تقييمها وترتيبها حسب الأولويات بالاعتماد على معايير معينة كالحجم أو النطاق أو احتمال الحدوث.

ج. الاستجابة للمخاطر: أي أن كافة المخاطر قد تم الاستجابة لها من خلال وضع إجراءات وقائية مناسبة للحد منها.

د. التوثيق: من خلال توثيق كافة الخطوات السابقة ورفع التقارير عنها.

2.2.8: التعامل مع المخاطر

أن أهمية مدخل إدارة المخاطر داخل المنشأة يتركز في الطرق التي يقوم بها في التعامل مع هذه المخاطر حيث تتلخص هذه الطرق في الآتي:

1. النقل: وذلك من خلال وسائل تساعد على قبول المخاطر من قبل طرف آخر وعادة ما تكون طريقة العقود أو الوقاية المالية مثل التأمين.

2. التجنب: يقصد به تجنب الأنشطة التي قد تحتوي على مخاطر، مصل ذلك عدم شراء أصول أو دخول في استثمار معين.

3. التقليل: ويشمل على الطرق التي يستخدمها المصرف أو المنشأة في التقليل من حدة الخسائر التي قد تسببها مخاطر معينة.

4. القبول: ويعني قبول الخسائر عند حدوثها، وتعتبر هذه الاستراتيجية مقبولة في حالة المخاطرة الصغيرة.

2.2.9: العوامل المؤثرة على دور المراجعة الداخلية في عملية إدارة المخاطر :

إن العوامل التي تؤثر على دور المراجعة الداخلية في عملية إدارة المخاطر تتمثل في ما يلي (ياسر؛ 2013) :

أ: طبيعة نشاط المنظمة: تختلف طبيعة الخدمات التي يمكن تقديمها المنشأة فقد تقدم خدمات مالية أو تقدم خدمات صناعية أو غيرها من الخدمات.

ب: حجم المنشأة : تتأثر الخدمات التي تقدمها المراجعة الداخلية بحجم نشاط المنشأة إلا أنه يجب أن يزداد اهتمام إدارات المراجعة الداخلية بعملية إدارة المخاطر بصورة أكبر من المنظمات الصغيرة .

ج: حجم إدارة المنشأة : المنظمات التي لديها أقسام أو إدارات مراجعة داخلية صغيرة أو ناشئة أو المنظمات الصغيرة التي يجب أن تأخذ على عاتقها مسؤولية إدارة مخاطر المشروع باعتبار من أهم أنشطة الإدارة لذلك يجب تطوير تطبيقات إدارة المخاطر .

إن المراجعة الداخلية كمراجعة رسمية معتمدة من قبل الإدارة العليا بالمنشأة هي اللاعب الرئيسي في المراحل المختلفة التي تشتمل عليها إدارة المخاطر وفي هذا الصدد يذكر أن المراجعة الداخلية تقوم بدور فاعل للرقابة على فاعلية إدارة المخاطر على أسس مستمرة . (عبد الفتاح ؛ 2008).

2.2.10: دور المراجعة الداخلية في إدارة المخاطر كأحد الاتجاهات الحديثة للمراجعة الداخلية

تعتبر من الأدوار الحديثة لوظيفة المراجعة الداخلية هو رصد وتقييم فاعلية الوحدة الاقتصادية في عمليات إدارة المخاطر، قد قام معهد المراجعين الداخليين بتناول دور المراجعة الداخلية في إدارة مخاطر الوحدة الاقتصادية، من خلال معيار المراجعة رقم (2120) "إدارة المخاطر" حيث نص على ضرورة قيام نشاط المراجعة الداخلية بتقييم مدى فاعلية عمليات إدارة المخاطر المطبقة بالوحدة والمساهمة في تحسين تلك العمليات، تعتبر المراجعة الداخلية مسئولة عن إعطاء تأكيد موضوعي ومستقل للجنة المراجعة حول فاعلية إدارة المخاطر، حيث أشار

المعهد على أن المراجعة الداخلية من خلال دورها التأكيدي وكذلك الاستشاري تساهم بشكل فعال في إدارة مخاطر الوحدة الاقتصادية(هيكل،2012).

ويعد المنهج أو المدخل للتعامل مع المخاطر البحثية عن طريق توقع الخسائر العارضة والمحتملة وتصميم وتنفيذ إجراءات من شأنها أن تخفف حدوث الخسارة أو الأثر المالي للخسائر التي تقع للحد الأدنى ويتمثل دور المراجع الداخلي في إدارة المخاطر في الآتي(صاح،2014).

أ- تقييم المخاطر التي تم اكتشافها خلال عملية المراجعة الداخلية، والتقرير عن عملية التقييم إلى الإدارة التنفيذية أو لجنة المراجعة أو الاثنين معاً.

ب- تطوير خطة بشكل منتظم لتقييم المخاطر للمنظمة.

ج- التصدي لقيادة أنشطة إدارة المخاطر للمنظمة.

د- تسهيل عملية تقييم المخاطر بواسطة أساليب التقييم الذاتي للمخاطر.

هـ- تقييم المخاطر المرتبطة بإدخال التكنولوجيا الحديثة ووقف هذه العملية إذا كانت

المخاطر المرتبطة بها لا يمكن السيطرة عليها وتنفوق المستويات المقبولة.

أن وظيفة المراجعة الداخلية قد اتسع نطاقها من دورها التقليدي وهو المراجعة المالية

والإدارية إلى التركيز على إضافة قيمة للمنشأة متصلة بإدارة المخاطر وتطبيق مدخل المراجعة

على أساس الخطر.(سمير 2004).

المبحث الثالث

الحوكمة كاتجاه حديث للمراجعة الداخلية

تمهيد:

ظهرت الحاجة للحوكمة بسبب الفساد المالي والإداري الذي انتشر في الكثير من المؤسسات المالية على مستوى العالم، وقد أرجعت الكثير من الدراسات السبب في هذا الفساد إلى ما يسمى بمشكلة الوكالة وضعف آليات الرقابة على أعمال المديرين؛ حيث تنشأ مشكلة الوكالة أساساً نتيجة الفصل بين الملكية والإدارة، وما يصاحب ذلك من تعارض في المصالح. فالحوكمة يمكن اعتبارها مجموعة من الأدوات أو الآليات التي تتناول أو تعالج المشكلات المرتبطة بالوكالة، فالدور الأساسي لنظام الحوكمة هو ضمان التوازن أو تنظيم العلاقات بين القدرة على استغلال الفرص والحصول على المكافآت والعوائد (محمد، 2017).

3.2.1: مفهوم الحوكمة

حظى مفهوم حوكمة الشركات في العقود الماضية باهتمام العديد من الكتاب والباحثين، وبالرغم من تعدد الكتابات حول هذا المفهوم إلا أنه لم يتم التوصل إلى تعريف موحد ويرجع ذلك إلى ارتباط هذا المفهوم بالعديد من الأبعاد الاقتصادية أو المالية أو الاجتماعية والقانونية والتنظيمية فعرفت الحوكمة حسب تقرير لجنة كادبري في عام 1992م على أنها نظام متكامل للوقاية يشمل النواحي المالية وغير المالية، من خلاله يتم إدارة الشركة والسيطرة عليه (أبو راوي، 2011).

ومنهم من عرف الحوكمة بأنها مجموعة من المعايير والقواعد والقوانين المنظمة للأداء والممارسات العلمية والتنفيذية سواء الشركات أو المؤسسات ومن ثم الحفاظ على حقوق أصحاب المصالح وتحقيق الإفصاح والشفافية (محمد، 2017).

يرى الباحث من وجهة نظره أن الحوكمة عبارة عن أسلوب رقابي يتضمن مجموعة من القواعد والمبادئ والقوانين التي تنظم العلاقة بين الأطراف داخل وخارج الشركة للوصول إلى

الهدف بأعلى درجة من الكفاءة وبأقل التكاليف، وذلك من خلال وضع الخطط والسياسات بدرجة من الوضوح والشفافية.

كما عرفت حوكمة الشركات بأنها "النظام الذي يتم من خلاله توجيه أعمال الشركة ومراقبتها على أعلى مستوى من أجل تحقيق أهدافها والوفاء بالمعايير اللازمة للمسؤولية والنزاهة والشفافية (السيد، 2012).

3.2.2: أهداف حوكمة الشركات

تساهم حوكمة الشركات في ضمان الشفافية والإفصاح وتحسين مستوى التنمية الاقتصادية والاجتماعية ، وضمان تطبيق معايير سليمة لمنع الفساد وسوء الإدارة ، وتوفير الحماية للمساهمين ومنع تضارب الأهداف وتنازع السلطات وتعظيم المصالح المتبادلة. (بوقرة، غانم ، 2012).

تهدف حوكمة الشركات إلى تحقيق العديد من الأهداف للوحدات الاقتصادية منها (محمد، 2015) (حمود، 2012)

- ثبات ومصادقية القطاعات المالية على المستوى المحلي والدولي.
- جذب الاستثمار الأجنبي والمحلي وتقليل تهريب رأس المال.
- ضمان الشفافية والعدالة والمساواة وتحسين مستوى التنمية الاقتصادية والاجتماعية
- تحقيق إمكانية المنافسة في الآجل الطويل وهذا يؤدي إلى خلق حوافز للتطوير.
- مراعات العمل والعاملين وتوزيع الصلاحيات والمسؤوليات بما يضمن تعزيز الرقابة والتدقيق الداخلي.
- الحصول على التمويل والتنبؤ بالمخاطر المتوقعة.

في ضوء ما سبق يرى الباحث أن هناك عدة أهداف تتحقق لتطبيق مبدأ حوكمة الشركات، أهم هذه الأهداف: السلوك الأخلاقي، الرقابة والمسائلة، إدارة المخاطر.

3.2.3: أهمية حوكمة الشركات

تعد حوكمة الشركات من أهم العمليات الضرورية لحسن عمل المؤسسات وتأكيد نزاهة الإدارة فيها، وكذلك للوفاء بالالتزامات والتعهدات ولضمان تحقيق المؤسسات لأهدافها وبشكل قانوني واقتصادي وتظهر أهمية الحوكمة فيما يلي: (أبوروي، 2011).

1. محاربة الفساد الداخلي في المؤسسات، وعدم السماح بوجوده أو استمراره، بل القضاء عليه وعدم السماح بعودته مرة أخرى.
2. رفع مستوى الأداء للشركات وما يترتب عليه من دفع عجلة التنمية والتقدم الاقتصادي للدول التي تنتمي إليها تلك الشركات.
3. الشفافية والدقة والوضوح في القوائم المالية التي تصدرها الشركات، وما يترتب على ذلك من زيادة ثقة المستثمرين بها واعتمادهم عليها في اتخاذ القرارات.
4. جذب الاستثمارات الأجنبية وتشجيع راس المال المحلي على الاستثمار في المشروعات الوطنية.
5. توفير الإطار التنظيمي الذي يمكن من خلاله للشركة أن تحدد أهدافها أيضاً كيفية تحقيقها.
6. الوصول إلى أفضل ممارسات للسلطة في الشركة.
7. تسهيل الحصول على تمويل وبتكلفة أقل: وذلك من خلال التزام المؤسسات بالحكمية المؤسسية يولد الأمان لدى المستثمرين على أموالهم .

يتضح للباحث مما سبق الأتي:

1. دعم الميزة التنافسية للشركات والسوق المالية.
2. تساعد على توفير الحماية للأصول المنشأة وحقوق المساهمين .
3. تساهم على عدالة ومصداقية القوائم والتقارير المالية.

3.2.4.: أسباب وجود الحوكمة:

هناك مجموعة من الأسباب والدوافع التي توضح مفهوم حوكمة الشركات ومن هذه الدوافع مايلي (جيهان، 2014):

1. الفصل بين الملكية والإدارة: أدى انفصال ملكية الشركة عن إدارتها إلى ظهور ما يسمى بمشكلة المؤسسة والتي تعني تعارض مصالح المديرين التنفيذيين مع طموحات المساهمين إذا استغل بعض المديرين سلطاتهم الواسعة الممنوحة لهم في تحقيق عوائد خاصة بهم، وكذلك القيام بأعمال غير أخلاقية.
2. الفصل بين مسؤوليات كل من مجلس الإدارة والمديرين التنفيذيين.
3. زيادة القيمة الاقتصادية للمراجعة الداخلية.
4. الحاجة إلى تماثل المعلومات المالية والغير المالية.

5. الحاجة إلى معالجة الخلل في الهياكل المالية.
6. الحاجة إلى الإفصاح المحاسبي العادل.
7. التوجه نحو إرساء قواعد للشفافية المالية.
8. توسيع دائرة مراقبة الأداء التشغيلي والاستراتيجي.
9. تجنب تعرض المنشآت لحالاتي التعثر والفشل المالي.
10. تمكين المنشآت من الحصول على تمويل من جانب عدد أكبر من المستثمرين المحليين والأجانب.

وقد فرضت الدوافع السابقة ضرورة تبني مجموعة من المعايير والإرشادات والقواعد الدولية التي تتضمن ممارسة سلطة إدارة المنشأة.

3.2.3: إضافة القيمة كاتجاه حديث للمراجعة الداخلية

3.2.3.1: مفهوم إضافة القيمة

تعني قدرة المنشأة على تحقيق قيمة إضافية للمساهمين، وتعد نشاط مستقل وتوكيدي واستشاري مصمم لإضافة قيمة للمنشأة ولتحسين عملياتها وهو يساعد الشركة على إنجاز أهدافها من خلال وجود منهج منظم ودقيق لتقويم وتحسين فعالية إدارة المخاطر، الرقابة، وعمليات الحوكمة، فإن تعظيم المراجعة الداخلية، يعد بمثابة مقياس للتعرف على تعظيم القيمة منها ويؤكد أن إضافة القيمة تتحقق من خلال دعم إدارة التنظيم على تحقيق أهداف التنظيم الاستراتيجية وبما يتسق مع توقعات أصحاب المصلحة بأداء خليط من الأنشطة التأكيدية والتأمينية والاستشارية في إطار من الاستقلال والموضوعية (عمر، 2023).

أيضا يقصد بإضافة القيمة: أي نشاط أو عملية تعمل على تعظيم حق المساهم في موارد المنشأة، وذلك بعد الوفاء بكل المطالبات المستحقة على مواردها (الوكيل، 2011). ويرى الباحث أن هذا التعريف ركز على حقوق المساهمين دون مراعاة حقوق أصحاب المصالح الأخرى، وكذلك لم يوضح تعظيم هذه الحقوق.

وفي ضوء ما سبق يرى الباحث أن إضافة القيمة للمنشأة تعني المنفعة المتحققة للمنشأة وأصحاب المصالح المختلفة وأن القيمة تزداد عندما تتجاوز منافع الشيء تكلفته، ويساهم في حل مشاكل المنشأة، ومن أهم المشاكل التي تواجه المنشأة والتي تؤثر على تحقيق أهدافها هي مشكلة

أحكام السيطرة على المنشأة وكذلك مشكلة المخاطر التي تواجه المنشأة لذلك لابد من وضع حلول ناجحة لمعالجتها.

3.2.3.2: مؤشرات إضافة المراجعة الداخلية قيمة للمنشأة

إن الالتزام بالإطار النظري للمراجعة الداخلية يتطلب وجود مؤشرات ومقاييس يمكن أن تقيس ما تضيفه المراجعة الداخلية، وكذلك يتطلب تحديد بعض المتطلبات التي تساهك في تحقيق إضافة سواء كانت على مستوى الأداء أو على مستوى الفكر النظري فالمؤشرات تنقسم إلى جزئين أحدهما يختص بمؤشرات إضافة قيمة للمراجعة الداخلية والجزء الآخر يختص بمتطلبات إضافة المراجعة الداخلية قيمة للمنشأة. يمكن تقسيم المؤشرات إلى ما يلي (باعاجبة، 2013):

- 1- **مؤشرات المستفيدين في المراجعة الداخلية:** تعكس هذه المؤشرات درجة رضا المستفيدين الداخليين والخارجيين عن خدمات المراجعة الداخلية التي تقدمها ويمكن قياسها من خلال:
 - أ- درجة رضا المستفيدين الداخليين والخارجيين عن خدمات المراجعة الداخلية.
 - ب- عدد الخدمات التي تم تلبيتها للمستفيدين الداخليين والخارجيين في المراجعة الداخلية إلى إجمالي عدد الخدمات المطلوبة .
- 2- **مؤشرات الوفورات المالية للمراجعة الداخلية:** تعكس هذه المؤشرات نتائج المؤشرات السابقة في صورة مالية ويمكن قياسها من خلال :
 - أ- مقدار الوفرة في تكلفة المراجعة الداخلية مع التكلفة المخططة لها .
 - ب- مقدار المنشأة على تجنب المخاطر وتحمل التكاليف .
 - ج- تخفيض التكاليف التي يمكن أن تتحملها المنشأة عند حدوث المخاطر .
- 3- **مؤشرات تأهيل وتطوير المراجع الداخلي :** ويمكن قياس هذه المؤشرات من خلال النسب التالية :
 - أ- نسبة عدد المراجعين الداخليين الذين لديهم خبرة طويلة في مجال المراجعة الداخلية إلى إجمالي عدد المراجعين الداخليين بالمنشأة .
 - ب- نسبة عدد المراجعين الداخليين الحاصلين على شهادات مهنية ؛ وكذلك عدد الدورات التدريبية .

4- مؤشرات أنشطة المراجعة الداخلية : وتعكس هذه المؤشرات التي تقوم بها المراجعة

الداخلية في المنشأة وتقاس من خلال

أ-نسب عدد الإجراءات المقترحة للحد من احتمال وقوع المخاطر والتي يتم الأخذ بها إلى إجمالي عدد الإجراءات .

ب-نسبة عدد الإجراءات المقترحة لتخفيض الآثار المحتملة للمخاطر عند حدوثها ؛ والتي يتم الأخذ بها في المنشأة إلى إجمالي عدد الإجراءات.

3.2.3.3: دور المراجعة الداخلية في إضافة قيمة للمنشأة: (باعجاجة،2013):

إن اسهام دور المراجعة الداخلية في إضافة قيمة للمنشأة يهدف إلى تحسين أدائها، لذلك فقد تم التركيز من قبل معهد المراجعين الداخليين الأمريكي، وهو الجهة التي تنظم اعمال المراجعة الداخلية على خدمات التأكيد والخدمات الإستشارية وإدارة المخاطر في المنشأة لمساهمتها في إضافة قيمة للمنشأة.

3.2.3.4: مقومات إضافة القيمة

يمكن تقسيم مقومات القيمة المضافة إلى نوعين هما(خليل،2011):

أولاً: المقومات الأساسية: وتتمثل في

1. الالتزام بمعايير الأداء المهني.
2. توفير مجموعة متكاملة من المقاييس اللازمة لقياس أداء المراجعة الداخلية.
3. توفير القدر الملائم من المعرفة التقنية.
4. الإلمام بطبيعة نشاط المنظمة، ونوعية الصناعة والنشاط الاقتصادي الذي ينتمي إليه.
5. تقديم كل من خدمات المراجعة الداخلية الأساسية والاستشارات في ضوء الاستراتيجية العامة للمنظمة.

ثانياً: المقومات الإضافية: وتتمثل في

- أ. الفهم الجيد للمتطلبات الحقيقية لعملاء المراجعة الداخلية.
- ب. الإلمام بطبيعة ثقافة وأخلاقيات المنظمة والبيئة المحيطة بها.
- ج. الالتزام بمعايير وآداب السلوك الأخلاقي.

د. الإلمام بالمعلومات اللازمة لتقرير المخاطر والأزمات المتوقعة.

لذا يرى الباحث أن هذه المقومات سواء كانت الأساسية أو الإضافية تمثل القاعدة الثابتة التي يجب أن تنطلق منها أنشطة ومهام المراجعة الداخلية لكي تصبح نشاطاً مضيفاً للقيمة بالمنفعة مع ضرورة الاهتمام بأي عناصر أو أبعاد أخرى قد تدعم ذلك.

كذلك يجد الباحث الاهتمام بوظيفة المراجعة الداخلية في ظل مفهوم سلسلة القيمة المضافة الذي يهتم بالمراجع المختلفة لأداء خدمات المراجعة الداخلية التي يمكن أن تضيف قيمة للمنظمة، وكذلك الأطراف المستفيدة من تلك القيمة سواء يدعم من دور المراجعة الداخلية في تقديم الخدمات المختلفة والاستشارات والتوصيات التي تلبي رغبات الأطراف المختلفة المتعاملة معها مثل مجلس الإدارة والإدارة التنفيذية ولجان المراجعة والمراجع الخارجي، والعملاء والمساهمين والموردين وبالتالي يضيف قيمة للمنظمة ككل.

الفصل الثالث:

الأمن السيبراني (Cyber security)

المبحث الأول: ماهية الأمن السيبراني

المبحث الثاني: إدارة مخاطر الأمن السيبراني

المبحث الثالث: محددات العلاقة بين المراجعة الداخلية والأمن السيبراني

المبحث الأول:

ماهية الأمن السيبراني

تمهيد:

يُعد الأمن السيبراني من أبرز التحديات التي تواجه دول العالم في ظل التطور الرقمي والتكنولوجي السريع، مما يستدعي تعزيز منظومة الأمن السيبراني بشكل شامل. ويهدف هذا المجال إلى حماية سرية البيانات وسلامتها وتوافرها من أي تهديدات سيبرانية قد تطال الشركات. لتحقيق ذلك، يتطلب الأمر تحسين الضوابط الأمنية، ووضع إجراءات وتدابير فعّالة، وتطوير أدوات وتقنيات قادرة على التصدي للتهديدات السيبرانية المحتملة. كما يشمل ذلك تأمين الحماية اللازمة ضد محاولات الاختراق والقرصنة الإلكترونية التي تستهدف الأنظمة والمعلومات (homas G Calderon, et al., 2020). ومن هذا المنطلق، يتوجب على الشركات تبني أفضل الممارسات العالمية في إدارة المخاطر السيبرانية، ووضع استراتيجيات واضحة لتعزيز حماية الأنظمة والبرمجيات والشبكات والأجهزة المرتبطة بها. إضافة إلى ذلك، يجب أن تمتلك الشركات القدرة على الاستجابة الفعّالة لحوادث الأمن السيبراني الطارئة والقدرة على التعافي من آثارها لضمان استمرارية العمل وحماية المعلومات الحيوية (فريد، 2022).

عليه أصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعيشه في العالم مؤخراً، حيث يشهد العالم المتقدم بكافة أرجائه تطور كبير لا يمكننا بأي حال أن نغفله، ولكن يوجد جانب آخر مظلم لذلك التطور الرقمي الذي نشهده، يمكن أن يجعل كبرى الدول والشركات والمؤسسات التجارية والاقتصادية مهددة بالاختراق، ولعل هذا من أسباب أهمية دراسة الأمن السيبراني، والذي يعمل على حماية البيانات والشبكات والأنظمة الإلكترونية من الهجمات والاختراقات التي قد تؤدي بها وباستقرارها (السمحان، 2020).

وفي دراسة أجراها مكتب المحاسبة الحكومية (GAO) بعنوان "هناك حاجة إلى إجراءات عاجلة لمعالجة تحديات الأمن السيبراني التي تواجه الأمة" تمت معالجة أربع تحديات رئيسية للأمن السيبراني من خلال عشرة إجراءات مقترحة لحل المشكلات، وتشمل التحديات؛ وضع استراتيجية للأمن السيبراني، تعزيز الأنظمة الفيدرالية وحماية البنية التحتية الحيوية، حماية البيانات الحساسة وضمان خصوصية البيانات (<https://gov.2018>).

كذلك سعت الدول النامية إلى اتخاذ إجراءات مماثلة لضمان الأمن السيبراني، وواجهت تلك الدول بعض المشكلات التي تتمثل في عدم وجود مبادرة شاملة للأمن السيبراني، ونقص الدعم الكافي، وعدم وجود مبادرات تعليمية قادرة على مواكبة التطورات الحاصلة في مجال الاتصالات وتكنولوجيا المعلومات، وانعكس هذا الأمر في تراجع مستوى الأمن السيبراني وأصبح مستخدومي الأنترنت لتلك الدول أكثر عرضة لهجمات وجرائم سيبرانية (Smaili & Khalili, 2023).

في عام 2013 تعرضت شركة التجزئة الأمريكية العملاقة (Target) لاختراق بيانات، حيث سرقت تفاصيل بطاقات الائتمان والخصم والبيانات الشخصية لـ 70 مليون عميل من قواعد بيانات الشركة، وقدرت الأضرار الإجمالية بأكثر من 18 مليار دولار (www.imd.org, 2021). وفي عام 2022، تصدر الأمن السيبراني قائمة المخاطر الحرجة في تقرير الاتحاد الأوروبي لمعاهد التدقيق الداخلي (ECIIA)، كما أشار تقرير مشهد التهديدات السيبرانية الصادر عن شركة (Positi Technologies)، إلى أن الجهات الحكومية في الشرق الأوسط تعتبر من الأهداف الرئيسية لمجرمي الأنترنت حيث أن 22% من إجمالي الهجمات السيبرانية قد استهدفت الدوائر الحكومية، وتشير تقديرات الخبراء إلى أن 78% من الهجمات السيبرانية على الشركات في منطقة الشرق الأوسط تستهدف أجهزة الحاسوب والخوادم ومعدات الشبكات، كما يعد مجرمو الأنترنت إلى اختراق الأنظمة عن طريق نشر برامج ضارة، أو استغلال نقاط الضعف لسرقة المعلومات السرية أو لتعطيل تشغيل الأجهزة، وتشتهر الهجمات في الشرق الأوسط باستخدام المساحات التي تحذف الملفات الموجودة على الأجهزة المخترقة (رزاق، 2024).

1.3.1: مفهوم الأمن السيبراني:

مفهوم الأمن لغة: الإطمئنان والسلام والسكينة. (البعليكي، 2017)

مفهوم السيبرانية: حسب ويكيبيديا هي كلمة مشتقة من الكلمة اللاتينية سايبير cyber ومعناها تخيلي أو افتراضي شاع استخدامه للتعبير عن الفضاء الذي يضم الشبكات المحوسبة وشبكات الاتصال والمعلومات وأنظمة التحكم عن بعد من خلال ثلاثة أطراف، الأجهزة، البرمجيات الرقمية وطاقم المطورين والمبرمجين. (البعليكي، 2017).

يمثل الأمن السيبراني النشاط الذي يؤمن حماية الموارد المالية والبشرية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانية الحد من الخسائر والأضرار التي تترتب في حالة تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن حتى لا تتحول الأضرار إلى خسائر دائمة (البغدادي، 2021). وقد عرفت دراسة (Frank, et al., 2019) الأمن السيبراني بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات. ويشير (أحمد، 2023) إلى أن الأمن السيبراني يتكون من سبعة عناصر رئيسية وهي: الأشخاص، السلطة، دعم الإدارة العليا، المنهجية الفعالة، التقنيات المناسبة المستخدمة، التوقيت المناسب للتواصل، والموازنة المناسبة المخصصة)، ويصنف الأمن السيبراني إلى عدة أنواع هي (أمن الشبكة، أمن التطبيقات، الأمن التشغيلي، الأمن السحابي، أمن البنية التحتية، أمن المعلومات، وأمن الأجهزة). ويرى (Badawy, 2021) أن الهجمات الإلكترونية مكلفة وقد يكون لها تأثير شديد الوضع المالي للمنشأة وقد تتسبب في تحريف جوهري في سجلات المنشأة والحد من قدرة المنشأة على الاستمرار، مما يشكل أهمية كبيرة للمستثمرين أثناء عملية اتخاذ القرار الاستثماري.

وأيضاً يمكن تعريف الأمن السيبراني وفقاً لما جاء بدراسة (Alina et al., 2017) إستناداً لأهدافه بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانية الحد من الخسائر والإضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الإضرار إلى خسائر دائمة.

تعرف السمحان الأمن السيبراني: بأنه اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية وذلك من خلال مجموعة من الوسائل المستخدمة تقنياً وتنظيماً وإدارياً في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال اتباع التدابير والإجراءات اللازمة لحماية البيانات (السمحان، 2020).

ويعرف المعهد الوطني للمعايير والتكنولوجيا الأمن السيبراني بأنه: منع الضرر الذي يلحق بأجهزة الكمبيوتر وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية

والاتصالات السلوكية وحمايتها وترميمها، بما في ذلك المعلومات الواردة فيها لضمان توفرها وسلامتها والمصادقة والسرية وعدم الإنكار (www.imd.org,2021).

وطبقاً لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات للأعوام 2014-2015، 2018-2019، مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات جيدة وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المنظمات والمستخدمين (Eling & wirfs,2016). وقد أكدت دراسة (البغدادي، 2021) أن الأمن السيبراني يمثل النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والإضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الإضرار إلى خسائر دائمة.

استناداً إلى ما سبق، يتفق الباحث مع رأي (Smaili, et. Al,2023) أنه يتمثل مفهوم الأمن السيبراني في حماية المعلومات الرقمية فضلاً عن سلامة البنية التحتية ونقل المعلومات، ويشمل مجموعة من التقنيات والعمليات المصممة لحماية الشبكات وأجهزة الكمبيوتر والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به لضمان السرية والنزاهة والقدرة على الاستفادة. كما يشير الباحث إلى أن دور الأمن السيبراني يتوسع ليشمل كافة الجوانب الاقتصادية، الاجتماعية، السياسية، والقانونية في المجتمعات الحديثة. بالإضافة إلى ذلك، يرتبط الأمن السيبراني ارتباطاً وثيقاً بسلامة موارد الثروة والتقدم، حيث يعتمد بشكل أساسي على القدرة على الاتصال والتواصل، وإدارة البيانات والمعلومات التي تعتبر أساس الإنتاج والإبداع وتعزيز القدرة التنافسية.

وفي هذا السياق يؤكد (AL-Moshaigeh, et.al,2019; Tuson,2021 ; Kamiya, wt.al,2021) أن مخاطر الأمن السيبراني تعتبر من أكبر المخاطر التي تواجهها المنشآت على غرار المخاطر المالية، حيث يمكن لمخاطر الأمن السيبراني أن تؤدي إلى ارتفاع التكاليف والتأثير السلبي على عوائد المنشآت والأضرار بقدرة المنشأة على الابتكار واكتساب العملاء والحفاظ عليهم، حيث أن الهجمات الإلكترونية مكلفة ولها تأثير واضح على المركز المالي للمنشآت مما يؤثر على القرارات الاستثمارية بشكل كبير.

1.3.2: المفاهيم المرتبطة بالأمن السيبراني:

- **الفضاء السيبراني:** يعرف الفضاء السيبراني (Cyberspace) أو الفضاء الإلكتروني بأنه عالم الحاسوب الافتراضي، أو الوسيلة الإلكترونية المستخدمة لتسهيل التواصل عبر شبكة الإنترنت، ويشمل الفضاء السيبراني شبكة حاسوب كبيرة مكونة من عدة شبكات حاسوب فرعية منتشرة في جميع أنحاء العالم (<https://mawdoo3.com>).

وعرف الاتحاد الدولي للاتصالات الفضاء السيبراني: المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى الإلكتروني، معطيات النقل والتحكم الرقمي (The International Telecommunication union, 2020).

- **الجريمة السيبرانية:** وهي استخدام الكمبيوتر كأداة لتحقيق أهداف غير قانونية، مثل ارتكاب الاحتيال، أو سرقة الهوية أو الملكية الفكرية، أو انتهاك الخصوصية.
- **الهجوم السيبراني:** محاولة معتمدة يقوم بها فرد أو منظمة، بهدف اختراق نظام المعلومات الخاص بفرد أو مؤسسة، غالباً ما يسعى من ينفذ تلك الهجمات إلى الحصول على فائدة جراء الهجوم على الطرف الآخر وتعطيل شبكته. وتحدث الهجمات السيبرانية يومياً ومنها ما يجري اكتشافه ومنها ما يزال غير مكتشف، وغالباً ما يستهدف المهاجمون الأنظمة الإلكترونية الضعيفة، ويطالبون بقدية مقابل إعادتها أو عدم تعطيلها، ما يسفر عن خسارة الشركات والأفراد الضحايا أموالاً طائلة (أبو شامة، 2021).

في دراسة (Rolf H Weber, 2016) التي هدفت إلى التعرف على التدابير التشريعية التي تقوم على حماية أمن المعلومات في بيئة الإنترنت من خلال إنترنت الأشياء، وخلصت الدراسة إلى أن سرعة التغيير والتطور التكنولوجي وتطور أساليب المهاجمين يتطلب ضرورة وجود أساليب جديدة لحماية المعلومات في بيئة الإنترنت إذ أن كل جهاز حاسب آلي متصل بالإنترنت يقع تحت تهديد هذه الجرائم مع وجود ثغرات عديدة تسهل هذه الهجمات، ويتطلب ذلك تعزيز الأمن المعلوماتي في بيئة الإنترنت بشكل عاجل وأيضاً المرونة المبتكرة بما يكفي للتصدي لهذه الهجمات.

1.3.3: أهداف الأمن السيبراني:

من أهم أهداف الأمن السيبراني: (<https://ab7as.net>)

1. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
2. التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
3. توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.
4. صمود البنية التحتية الحساسة للهجمات الإلكترونية.
5. توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
6. التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها .
7. سد الثغرات في أنظمة امن المعلومات.
8. مقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين.
9. حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
10. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
11. تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

1.3.4: أهمية الأمن السيبراني:

تكمن أهمية الأمن السيبراني في فهم المخاطر المستقبلية والعمل على إدارتها والتحكم بها بفاعلية. عند فهم المخاطر السيبرانية وإدراك تأثيرها المحتمل على الأنظمة والبيانات، يمكن للمؤسسات إتخاذ التدابير والإجراءات اللازمة للتعامل معها والتقليل من الآثار الناجمة عنها، وتتضمن أهمية الأمن السيبراني فيما يلي:

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيدي من العبث بها
- تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.

- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
 - استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.
 - توفير بيئة عمل آمنة جداً خلال العمل عبر الشبكة العنكبوتية.
- ويرى الباحث: أن أهمية الأمن السيبراني تظهر في توفر حماية فائقة للبيانات والمعلومات والأجهزة والشبكات، وتعزيز الثقة والسلامة في استخدام التكنولوجيا الرقمية .

1.3.5: أهمية دراسة الأمن السيبراني:

هناك عدد من الأسباب التي تجعل دراسة الأمن السيبراني من أبرز المجالات التي تحتاج لوجود خبراء مؤهلين لحماية أمن الشركات والمؤسسات والدول أيضاً، ومن أبرزها:

1. يشهد سوق العمل حاجة مستمرة لخبراء مجال الأمن السيبراني.
2. بالعمل في مجال الأمن السيبراني يمكن جني الكثير من الأرباح المالية.
3. الخبرة في مجال الأمن السيبراني ستكون غاية لكل مؤسسة مميزة.
4. يشمل الأمن السيبراني كافة المجالات العملية بالرغم من اختلافها وتنوعها.
5. تمكين الدارس من الحصول علي امتيازات فريدة في العمل.

1.3.6: أهم المسارات الوظيفية المتاحة بعد دراسة الأمن السيبراني:

يشهد هذا المجال اقبال وطلب كبير في شتى المجالات، ولذلك تشير التقارير والإحصاءات العالمية إلى زيادة كبيرة في طلب محترفي الأمن السيبراني، حيث أن سوق الأمن السيبراني قد نما وتطور في كافة دول العالم بشكل ملحوظ، ففي عام 2004 كان يقدر بـ 3,5 مليار دولار، بينما كان في عام 2015 يكلف 75 مليار دولار، ويتوقع أن يحقق ما يقارب 170 مليار دولار؛ في عام 2020 ومن المتوقع عقب دراسة الأمن السيبراني والحصول على درجة البكالوريوس سيجد الخريج العديد من الفرص الوظيفية المميزة في عدد من المجالات، وتتنوع المسارات الوظيفية التابعة لتلك الدراسة، حيث تشمل : مهندس الدعم السحابي، متخصص دعم تكنولوجيا المعلومات، مهندس الدعم الفني، مطور برامج وتطبيقات، مسؤول الشبكات، مسؤول الطب الشرعي الرقمي (<https://ab7as.net>) .

1.3.7: خصائص الأمن السيبراني:

وتعد حروب الفضاء الخارجي واحدة من وسائل وآليات الجيل الخامس من النزاعات، فلم تعد تنفرد أهداف المجاميع الخاصة للقوات الأمريكية في ردع أي هجوم أو اعتداء من قبل الخصم في القوات السيبرانية المعادية؛ لكن أيضاً دخلت مواقع التواصل وتطبيقات الإنترنت للتنظيم الإرهابي (داعش) الأمر الذي ساعد على إبقاء السرية للقنوات الخاصة بهم والهادفة إلى احتمالية تجنيد مزيد من الأصوليين الإرهابيين (كوستجان، 2018).

خصائص الأمن السيبراني العامة: من المبادئ الشائعة والتي تعد من أجل أن يكون البرنامج الأكثر ضرراً في تكوين أسلحة الفضاء الخارجي (العكابي، 2023):

1. يجب أن يكون تحت رعاية حكومية أو هيئة ناشطة غير حكومية يتم تطويره لها.
2. أن تكون الفائدة من هذا السلاح من أجل عمل تجسسي وتوظيف قوة فاعلة في تشكيل وصياغة مشاهد تبرز فعلهم العدواني.
3. هناك قوى ترعى بناء وتشكيل السلاح السيبراني والذي يتميز عن البرامج التي تتسم بالضرر، وأن يعمل السلاح السيبراني ضد أهداف معينة حيث أنه لا يستخدمه قراصنة، بل يتم استخدامه من قبل حكومات وقوى غير حكومية مثل التنظيمات الإرهابية والكيانات الفاعلة التي يتم إشراكها.
4. مراقبة النظام ومراقبة مشغليه والمعلومات الحساسة، مثل كلمات المرور، والمفاتيح الخاصة للبرامج وسرقة البيانات والملكية الفكرية لعملية الاتلاف الإلكتروني لواحدة أو أكثر تتكون مما يلي (عبدالصادق، 2016):
 - أ- البيانات الموجودة في أنظمة البنى التحتية.
 - ب- اتلاف أجهزة الكمبيوتر أو تدميرها بالكامل.
5. الاستهداف: ويكون استهدافها اختياري، قبل البدء بأي هجوم، يتم اختيار الأهداف أولاً وبالطرق المختلفة لكن ما يستخدمه القراصنة والمحتالون لسرقة المعلومات الشخصية أو المالية، تبين أنها عشوائية، وتوزيعها واسع.
6. التميز عن الفيروسات والبرامج الضارة الأخرى: يتميز السلاح السيبراني عن الفيروسات، ليست كل الفيروسات أسلحة سيبرانية، كما أن ليست جميع الأسلحة السيبرانية

فيروسات، فالأسلحة السيبرانية المهددة للأمن السيبراني هي برامج تتم تصميمها للقيام بوظائف مختلفة وتشمل (كوستجان، 2018).

أ. فايروسات الحاسوب: من وظائفها إزالة البرامج أو تعديل عبيها أو نسخها أو غير ذلك والغرض هو إلحاق الضرر بحواسيب الخصم، وفي بعض الأحيان قد تستخدمه إلى تعطيل شبكة الاتصال لدولة ما، بعد تطور الفضاء السيبراني صنعت من أجل تخريب بيانات الخصم وسرقتها أو قطع شبكتها، تتصف بالانتشار وصعوبة التخلص منها، لقدرتها الكبيرة على عمل التلوث والنسخ على المعلومات التي تركز على شبكات الاتصالات والتي تستهدف الأموال مثل المصارف وأشهر الديدان الستاكس نت التي استخدمت لتعطيل اثنين من المفاعلات النووية الإيرانية (السمحان، 2020).

ب. حصان طروادة: هي شيفرة وكذلك برنامج صغير متخفي داخل برنامج واسع ويعد من البرامج المشهورة عالمياً حيث يعمل على بعض الوظائف غير الظاهرة مثل يقوم بزرع فايروسات وديدان، ولا يمكن معرفة مكان وجوده لأنه تم برمجته بدقة كبيرة، ويخفي اثاره التي لا تتصف بأعمال تدميرية، ويقوم بتقليل القوة الدفاعية لدى الشخص الذي تم احتراقه من أجل انتهاك خصوصية معلوماته وبياناته المثبتة في جهازه فيقوم على سبيل المثال بإرسال بيانات عن نقاط الضعف المتواجدة داخل النظام (ماري ايكن، 2018).

1.3.8: أنماط الأمن السيبراني:

أشار كلاً من (السمحان، 2020)، (رزاق، 2024):

- ينطبق هذا المصطلح على مجموعة متنوعة من السياقات، بدءاً من قطاع الأعمال، وصولاً إلى الحوسبة المتنقلة، وبالإمكان عموماً تقسيمها إلى عدة فئات شائعة كما يلي:
- **أمن الشبكات:** هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية، سواء المهاجمين المستهدفين، أو البرامج الضارة.
- **أمان التطبيقات:** يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإن تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأولى قبل نشر البرامج أو الجهاز.
- **أمن المعلومات:** يحمي سلامة وخصوصية البيانات، سواء في مرحلة التخزين أو التناقل.

- الأمن التشغيلي: يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.

1.3.9: عناصر الأمن السيبراني(https://www.mah6at.net):

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك، ومن أهم عناصر الأمن السيبراني:

1. **التقنية(technology):** تشكل التكنولوجيا والتقنية دوراً في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها .

2. **الأشخاص (People):** يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتقادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بعمل نسخ احتياطية للبيانات.

3. **الأنشطة والعمليات(process):** يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

المبحث الثاني:

إدارة مخاطر الأمن السيبراني:

تعرف إدارة مخاطر الأمن السيبراني بأنها عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات (يعقوب وآخرون، 2022).

وعرفت الاستراتيجية الوطنية للأمن السيبراني في العراق بأنها احتمال وجود تهديد وهشاشة الفضاء الإلكتروني للبلد مما يضر بأمن نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية من خلال التهديدات السيبرانية والثغرات الموجودة في الفضاءات السحابية (أميرهم، 2022).

وقام المعهد الوطني للمعايير والتكنولوجيا (NIST) بإصدار النسخة المحدثه رقم 2.0 من إطار العمل للأمن السيبراني وهو إطار عمل يوفر طريقة للمؤسسات لفهم مخاطر الأمن السيبراني وإدارتها والتخفيف، من حديثها ولم يعد يقتصر على المؤسسات العاملة في البيئة التحتية الحيوية، والتي كان جمهورها المستهدف الأصلي، ويركز إطار الأمن السيبراني على مجموعة من الوظائف الأساسية: تحديد وحماية الكشف الاستجابة، الاسترداد، بالإضافة إلى إدارة الحوكمة التي تشمل صنع القرارات الاستراتيجية المتعلقة بالأمن السيبراني على مستوى المؤسسات (رزاق، 2024).

وتلعب المحاسبة والتدقيق دوراً مهماً في إدارة مخاطر الأمن السيبراني على اعتبار أنها من المخاطر الناشئة وهي الخطر الذي يؤدي إلى خسائر مالية فادحة فضلاً عن مخاطر السمعة والمخاطر التشغيلية، من خلال بناء إدارة فاعلة لمخاطر الأمن السيبراني (مشابهة لنظام الرقابة الداخلية) بإجراء الاختبارات اللازمة لفاعلية عناصر رقابة الأمن السيبراني باختيار نقطة مرجعية معيارية (ضوابط التكنولوجيا) داخل المنظمة.

وقد أعطى مجلس الرقابة على شركات المحاسبة AAOB أولويات مستقبلية لمخاطر الأمن السيبراني حيث تعمل على معالجة مخاطر الأمن السيبراني في عملية التدقيق وأصدر إرشادات لمساعدة المدققين على فهم هذه المخاطر وتخفيضها، حيث أوصى المجلس بأن يقوم

المدققين بتقييم مخاطر أنظمة تكنولوجيا المعلومات الخاصة بهم وتنفيذ الضوابط للحماية من التهديدات الإلكترونية، وأن يقوم المراجع بإجراء اختبار دوري لأنظمة تكنولوجيا المعلومات الخاصة بهم لضمان فعاليتها (<https://fastercapital.com>).

2.3.1: المخاطر التي تهدد الأمن السيبراني:

يشير مفهوم مخاطر الأمن السيبراني إلى التهديدات والهجمات الإلكترونية المسببة لتعطيل أنظمة التكنولوجيا للمؤسسات وخدماتها الإلكترونية، ولا تضر هذه المخاطر بتقنيات وأجهزة المؤسسات فحسب بل أيضاً تكبدها خسائر وتلحق أضراراً بسمعتها (رزاق، 2024). حيث يقصد بمخاطر الأمن السيبراني بأنها المخاطر التشغيلية أصول المعلومات، وتشكل مخاطر تؤثر بشكل كامل على سرية المعلومات وأنظمة المعلومات، لذلك تعتبر هذه المخاطر تكس أصول المؤسسات، مما يؤدي إلى إخلال في الأنظمة والمعلومات. (Hartmann, 2021).

وبحسب الرابطة الدولية لمشرفي التأمين IAIS فإن المخاطر السيبرانية: تعني أي مخاطر تنشأ عن استخدام البيانات الإلكترونية ونقلها بما في ذلك أدوات التكنولوجيا مثل شبكات الاتصالات كما أنها تشمل الأضرار المادية والاحتيال المرتكب عن طريق إساءة استخدام البيانات وأي مسؤولية تنشأ عن تخزين البيانات وتوفير المعلومات الإلكترونية وسلامتها وسريتها (IAIS, 2018).

وأشار المعهد الوطني للمعايير والتكنولوجيا بأنها مقياس لمستوى التهديد وأثره الذي وقع بالفعل أو من المحتمل أن يقع أو كلاهما والذي يستهدف واحدة أو أكثر من المعلومات أو العمليات أو القدرات أو سمعة المؤسسة.

ويرى الباحث أنه يمكن تعريف مخاطر الأمن السيبراني بأنها المخاطر التي تتسبب بخسائر مادية وخسائر معنوية في شهرة شركات الاتصالات الليبية وتتم من خلال مجموعة متسلسلة أو منظمات خبيرة في التسلسل على شبكات الأنترنت، تكون هذه المخاطر من خارج الشركة والتي تعمل على توقف التكنولوجيا وتعطل نظم المعلومات أو تدميره من خلال معرفة نقاط الضعف في أمن المعلومات أو البرامج المضادة، وقد تكون هذه المخاطر من داخل الشركة من خلال الوصول غير المصرح به إلى معلومات لا يصرح بالاطلاع عليها.

2.3.2: أنواع مخاطر الأمن السيبراني:

إن الهدف الرئيسي للأفراد والكيانات المتسللة أو المختصين بها أن يجدوا فرصة أو ثغرة لدى شركات الاتصالات، من أجل سرقة بياناتها أو معلوماتها أو تحويل أو تعديل البيانات المالية، أو من أجل الاختيال المالي أو الوصول إلى معلومات مالية أو غير مالية، أو لتعطيل الأنظمة لدى الشركات وتعطيل البنية التحتية. (IIA 2020).

حيث أن هناك أنواع كثيرة لمخاطر الأمن السيبراني، أهمها ما يلي: (الخرينج، داوود، ياسر، 2022):

- 1- مخاطر الأمن السيبراني التقني: وهو الذي يتزامن مع التقدم التكنولوجي والاتصالات، مع وجود مخاطر خاصة، ترتبط بشكل مباشر في هندستها الخاصة، والبيئة التي تعمل ضمنها.
 - 2- المخاطر القانونية: وهي تتمثل في غياب الهيكل التشريعي والهيكل التنظيمي المناسبين، وبالتالي فإن المخاطر القانونية تتمثل في غياب الأمن القانوني، وتناقض بعض الأحكام والقوانين، وتنازع الأنظمة القانونية، وفي اتساع إمكانات انتشار الجريمة عبر الإنترنت.
- ويمكن تقسيم مخاطر الأمن السيبراني لمجموعتين رئيسيتين وهما: (شحاتة، 2022):

أ- مجموعة مخاطر الأداء المرتبطة بتطبيق أدوات تكنولوجيا المعلومات الحديثة التي تعبر عن فشل تلك الأدوات في القيام بالمهام المخططة لها وتحقيق الاستفادة المرجوة منها.

ب- مجموعة المخاطر الأمنية التي تتضمن ثلاثة مخاطر أساسية وهي:

1. خطر خرقات الحماية المادية المتعلقة باختراق المكونات المادية للبنية التحتية التي تعتمد عليها الشركة في خدمات تكنولوجيا المعلومات كالبحت في مخلفات البنية التحتية للشركة من أقراص مرنة أو أجهزة خاصة بالشبكات الإلكترونية والتي قد تتضمن أي معلومات أو كلمات سر يمكن الاعتماد عليها لإتمام عملية الاختراق والتجسس الموجي الذي يشير لاستخدام أجهزة متخصصة لالتقاط كافة المخرجات اللاسلكية من نظام تكنولوجيا المعلومات كالموجات الصوتية.

2. خطر خرق الحماية المتعلقة بالعاملين المرتبط بالمخاطر الداخلية والخارجية والمتعلقة بسلوك العاملين داخل الشركة، مثل قرصنة البرامج الجاهزة، انتهاك التصريح التي تنتج عن ضعف هيكل الرقابة الداخلية، الهندسة الاجتماعية التي تشير لقيام العاملين بالشركة باستغلال علاقاتهم ووظيفتهم للوصول غير المصرح به للمعلومات واختلاس المعلومات.

3. خطر خرق الحماية المتعلقة بالمعلومات والاتصالات الذي يتضمن هجمات البيانات كالنسخ غير المصرح بها من البيانات، هجمات البرامج الجاهزة كالفيروسات والمصائد والأبواب الخلفية والقنوات السرية.

وتذهب دراسة (جيهان عادل إبراهيم)، أن المخاطر السيبرانية تتمثل في ثلاثة محاور وهي: مخاطر سيبرانية تتعلق بالسرية، ومخاطر سيبرانية تتعلق بالنزاهة، ومخاطر سيبرانية تتعلق باستمرار الأداء. ويرى الباحث أن هذه الأنواع الثلاثة من المخاطر السيبرانية لها تأثيرات مباشرة ومختلفة على الأهداف حيث يؤدي تعطل الأعمال إلى المنع من العمل مما ينتج عنه خسارة في الإيرادات كما يؤدي الاحتيال إلى خسائر مالية مباشرة في الوقت الذي يستغرق التحقيق في تأثيرات اختراق البيانات مؤقتاً، الأمر الذي ينتج عنه أضرار معنوية تمس السمعة وفضلاً عن تكاليف التقاضي وبصفة عامة فإن خطر فقدان الثقة في أعقاب الهجمات الإلكترونية، قد يكون غالباً بالنسبة للقطاع المالي بالنظر إلى اعتماد المؤسسات المالية على ثقة عملائها مما يؤثر على قرارات المستثمرين (أميرهم، 2022).

2.3.3: أنواع الجرائم السيبرانية: (<http://isf.gov.lb>):

1- الابتزاز الإلكتروني.

2- سرقة الهوية أو انتحال الشخصية: هي نوع من أنواع الغش التي تحصل عندما يستخدم شخص ما معلومات تعريف شخصية تعود لشخص آخر، مثل الاسم، رقم جواز السفر، بطاقة الهوية، بطاقة الائتمان، تفاصيل الحسابات الإلكترونية أو صورته، دون إذنه، بغية ارتكاب أعمال احتيالية، سرقة المال وبطاقات الائتمان، أو مجرد إلحاق الضرر والإساءة إلى السمعة كفتح حسابات مصرفية والحصول على قروض والقيام بأعمال غير مشروعة من خلال انتحال هوية الضحية بشكل كامل، أو استخدام حسابات بطاقات الائتمان العائدة للضحية بطرق غير مشروعة للقيام بعمليات شراء أو سحب مبالغ نقدية... الخ.

3- التصيد الاحتيالي عبر الإنترنت:

وفي دراسة السمحان يرى أن جرائم الأمن السيبراني تتعدد، ومن أهم هذه الجرائم: جرائم التعدي على البيانات المعلوماتية، التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج المعلوماتية، الجرائم الواقعة على الأموال، الاستغلال الجنسي للقاصرات، التعدي على

الملكية الفكرية للأعمال الرقمية، البطاقات المصرفية والنقود الإلكترونية، جرائم تمس المعلومات الشخصية، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، جرائم المقاومة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة، وجرائم تشفير المعلومات (السبحان، 2020).

2.3.4: أسباب الجرائم السيبرانية:

- الرغبة في جمع المعلومات وتعلمها .
- الاستيلاء على المعلومات والاتجار فيها .
- قهر النظام وإثبات التفوق على تطور وسائل التقنية .
- الحاق الأذى بأشخاص أو جهات .
- تحقيق أرباح ومكاسب مادية.
- تهديد الأمن القومي والعسكري.

2.3.5: أبعاد الأمن السيبراني (<http://ab7as.net>):

أولاً: الأبعاد العسكرية

تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشأة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.

ثانياً: الأبعاد السياسية

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار أمن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

ثالثاً: الأبعاد الاقتصادية

يرتبط الأمن السيبراني ارتباطاً وثيقاً بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فاعلم الدول تعتمد في تعزيز اقتصادها وازدهاره على

إنتاج وتداول المعرفة والمعلومات على المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

رابعاً: الأبعاد القانونية

ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

2.3.6: آليات (متطلبات) تحقيق الأمن السيبراني

(<https://www.arageek.com/>)

(/

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية:

أ. **الموثوقية:** وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية، والقاعدة الأساسية هي التحقق من عنوان URL، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدون s؛ فيجنب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.....الخ.

ب. **البريد الاحتيالي:** ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إن إحدى الطرق الأكثر شيوعاً التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها رسالة من شخص موثوق به .

ج. **التحديثات:** (date-to-up Always): وتعني الحرص دائماً على تحديث الأجهزة ، فغالباً ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.

د. النسخ الاحتياطي: ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت.

2.3.7: أهمية الرقابة في تعزيز تدابير الأمن السيبراني:

بين تقرير وحدة التفتيش المشتركة لدى دراسة الأمن السيبراني في مؤسسات منظومة الأمم المتحدة لعام 2021 في جنيف بأن هيئات الرقابة الداخلية والخارجية في مؤسسات منظومة الأمم المتحدة كانت مهمته بمسائل الأمن السيبراني حتى في حال عدم وجود إشارات محددة في تفويضها إلى الموضوع بحد ذاته، وقد صادف المفتشون عدة أمثلة على التحسينات المؤسسية التي أدخلت على إطار الأمن السيبراني في المنظمات المشاركة وهي تحسينات انبثقت عن توصيات الرقابة مثل إنشاء منصب رئيس موظفي أمن المعلومات، والتوصيات الخاصة بالتدريب، ووضع خارطة طريق يمكن تفعيلها، وما إلى ذلك.

وأشارت لجان المراجعة والرقابة تناولت مسائل الأمن السيبراني كجزء من تفويضها الذي يغطي الإدارة المركزية للمخاطر وليس في سياق الحوكمة المعينة بتكنولوجيا المعلومات والاتصالات.

وأن هذه اللجان تبنت موضوع الأمن السيبراني، ليس مجرد دعم الإدارة ولكن لاطلاع الهيئات التشريعية والإدارية على مخاطر الأمن السيبراني وتمكينها من المساهمة في التخفيف من المخاطر التي تواجه المنظمات ولتأكيد أن جميع هيئات الرقابة تضيف قيمة قصوى من وجهة نظر الأمن السيبراني، وأشار التقرير أنه من الضرورة أن يسترشد عمل موظفي الرقابة بما لدى خبراء الأمن السيبراني داخل المنظمة من معرفة وخبرة، وأن تصب هذه المعرفة والخبرة في ذلك العمل (<https://www.unjiu.org>).

المبحث الثالث:

محددات جودة العلاقة بين المراجعة الداخلية والأمن السيبراني:

مما لا شك فيه أن اتساع نطاق المراجعة الداخلية ليشمل مراجعة، وتقييم جميع الأنشطة والعمليات المؤسسية، بهدف تقييم وتحسين فاعلية إدارة المخاطر، وأنظمة الرقابة، وتطبيق الحوكمة، كل ذلك جعل وظيفة المراجعة الداخلية الفعالة مصدراً ذا قيمة عالية للمعلومات التي تحتاجها الأطراف ذات الصلة، وهو ما يبرر الاهتمام المتزايد في الفترة الأخيرة بأهمية المراجعة الداخلية وما يمكن أن تحققه من قيمة مضافة لجميع المنشآت، وذلك ما يوفره المراجع الداخلي من معلومات، وتوصيات واستشارات تساعد الوحدة الحكومية على التخطيط الاستراتيجي لأدائها ومتابعة هذا الأداء وتوجيهه لتحقيق الأهداف المخططة، واتخاذ ما يلزم من قرارات لتسيير الأعمال والأنشطة، ودعم عمليات إدارة المخاطر، وهذا ما أكدت عليه دراسة كل من (Yang et al., 2021; Betti et al., 2020).

وفي سياق متصل أوصت لجنة مبادئ الإدارة السليمة للمخاطر الصادرة عن (COSO, 2019; IIA, 2020) بأن إدارة مخاطر الأمن السيبراني يمكن أن تدار من خلال ثلاثة خطوط دفاعية، وهي كالتالي:

- الخط الدفاعي الأول يتمثل في مديرو وحدات الأعمال جنباً إلى جنب مع وظيفة تكنولوجيا المعلومات IT حيث أنهم بحاجة إلى اعتبار مخاطر الأمن السيبراني جزءاً لا يتجزأ من عملهم وإنشاء الهياكل والضوابط المناسبة لإدارة العمليات والمخاطر.
- الخط الثاني يتمثل في إدارة مخاطر وأمن المعلومات حيث توفر الخبرة لتنفيذ ومتابعة فعالية ضوابط الأمن السيبراني CS.

- الخط الدفاعي الثالث يتمثل في وظيفة المراجعة الداخلية حيث تزود مجلس الإدارة ولجنة المراجعة التابعة لها بتوكيد مستقل عن فعالية استراتيجية وسياسات وإجراءات وضوابط إدارة مخاطر الأمن السيبراني وهذا ينطوي على مراجعة مدى كفاية العمل الذي قام به أدوار الخطين الأول والثاني (Vuko et al., 2021).

تعد وظيفة المراجعة الداخلية أحد الركائز الأساسية لتلبية احتياجات مختلف أصحاب المصالح، خاصة المساهمين والإدارة حيث تعمل المراجعة الداخلية على إعداد تقرير عن مدى

فعالية هيكل الرقابة الداخلية، كما أنها تساهم بشكل كبير في توفير نظرة عامة وشاملة عن أداء مختلف الإدارات والأقسام داخل المنشأة والمخاطر التي تواجهها، وهذا علاوة على متابعة قرارات مجلس الإدارة بشكل مستمر (PWC,2018)(شحاتة، 2020).

وفي هذا الصدد يمكن القول أن جودة وظيفة المراجعة الداخلية فيما يتعلق بإدارة مخاطر الأمن السيبراني والحد من تلك المخاطر يركز على قيام مدير إدارة المراجعة الداخلية بتقديم النصح والإرشاد لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبراني المحيطة ببيئة أعمال المنشأة التكنولوجية وكيفية مواجهتها والحد من آثارها بما يدعم تحقيق أهداف المنشأة (Florakis et al.,2020; Li & Wang.,2018). وفي سياق متصل تعمل جودة المراجعة الداخلية على تمكن إدارات المنشآت من تصميم خطوط دفاع قوية لمواجهة مخاطر الأمن السيبراني طبقاً لطبيعة واحتياج البيئة التكنولوجية ونوعية وكثافة المخاطر التي تواجه المنشأة والتي تتمثل في (صالح، 2022):

(أ) تقييم النضج السيبراني: والذي يتمثل في تحديد الفجوات في الوضع الحالي للأمن السيبراني هذا علاوة على فهم محددات وأبعاد نقاط الضعف المطلوب التركيز عليها.

(ب) مراجعة التكنولوجيا الجديدة: حيث تقدم منصات التكنولوجيا الناشئة والتي تضم (السحابة والشبكات الاجتماعية والجوال والبيانات الضخمة وأنظمة الذكاء الاصطناعي وغيرها) مخاطر إلكترونية جديدة تستدعي القيام بعمليات مراجعة خاصة تشتمل على مراجعة عنصر الأمان قبل وبعد تنفيذ التكنولوجيا الجديدة.

(ج) مراجعة التكنولوجيا العميقة: من الأهمية قيام المراجعة الداخلية بتقييم المخاطر الأمنية المتعلقة بأنظمة التكنولوجيا مع التأكيد على الفهم الشامل للمخاطر الأمنية.

ومما لا شك فيه أن هناك العديد من العوامل التي تحدد فعالية المراجعة الداخلية بشأن الأمن السيبراني ولعل أهمها ما جاء بدراسة كل من (Islam et al.,2018; IIA,2017; Deloitte,2017):

1/3 التأهيل العلمي والعملي لفريق المراجعة الداخلية بالمصرف: أشارت منظمة المراجعة الداخلية (IAF,2021) إلى ضرورة أن يتقن المراجعون الداخليون ومعاهد ومنظمات المراجعة الداخلية أهمية الاستفادة من التكنولوجيا، حيث تتطلب مراجعة الأمن السيبراني بجودة عالية تأهيل فريق المراجعة الداخلية بالمصرف بمعرفة متطورة بتكنولوجيا المعلومات (IT)

ومخاطرها، وأن يكون لديهم القدرة على التحكم في تقنيات المراجعة الداخلية القائمة على التكنولوجيا الحديثة والمتاحة لأداء أنشطة المراجعة الداخلية بجودة عالية، الأمر الذي يترتب عليه القدرة على تطوير علاقات أعمق مع وظائف أمن نظم المعلومات ومن ثم المساهمة في بناء برنامج إدارة أمن سيبراني أكثر فعالية وجودة وبالتالي من المتوقع أن تؤدي المراجعة الداخلية التي تضم رؤساء مراجعة داخلية حاصلين على شهادات الأمن المناسبة مثل (الشهادات الأمنية CISM و CSP) وكذلك شهادات مراجعة أمن أنظمة المعلومات مثل: (شهادة CISA و QICA) إلى زيادة جودة مراجعة الأمن السيبراني.

2/3 مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية (Enterprise Risk Management)(ERM): نظراً لتطور دور المراجعة الداخلية حيث أصبح تركيزها الطبيعي

على الحوكمة وإدارة المخاطر والالتزام، فأصبحت ذات أهمية بالغة في الإشراف على جميع مكونات أطر عمل إدارة المخاطر المؤسسية ومن ثم فإن إدارة المخاطر المؤسسية لها تأثير كبير على أنشطة المراجعة الداخلية، الأمر الذي يترتب عليه تمتع المراجعة الداخلية بفعالية عالية في أداء أنشطتها، علاوة على قدرة الرؤساء التنفيذيين للمراجعة على تشغيل أقسامهم بشكل أكثر كفاءة من خلال الاستفادة من موارد إدارة المخاطر بالمصرف، هذا بالإضافة إلى أنه عند مشاركة المراجعة الداخلية في إدارة المخاطر ينهج المراجعون نهج التفكير الابتكاري الاستراتيجي مثل المديرين والتركيز على أهداف العمل بدلاً من أهداف المراجعة فقط وبالتالي يمكن للمراجعة الداخلية من خلال إجراء تقييم شامل للمخاطر السيبرانية تقديم وجهات نظر ونتائج موضوعية إلى لجنة المراجعة وأعضاء مجلس الإدارة واستخدام هذه النتائج لتطوير خطة المراجعة الداخلية بشكل موسع تضم مجالات المخاطر السيبرانية التي تواجهها المصارف خلال فترة مراجعة واحدة أو فترة مراجعة متعددة السنوات.

3/3 جودة وظيفة المراجعة الداخلية: أكدت دراسة كل من (صالح، 2022) (Islam et al., 2015; Christ et al., 2015; Ege, 2018) على أن وظيفة المراجعة الداخلية المصحوبة

بالجودة العالية يترتب عليها مجموعة من المنافع للمصارف لعل أهمها: تحسين حوكمة المصارف، جودة التقارير المالية، فعالية هيكل الرقابة الداخلية، القدرة على تقديم تقييمات أفضل للمخاطر، الحد من سوء السلوك الإداري وزيادة كفاءة المراجعة الداخلية، وفيما يتعلق بالأمن السيبراني يمكن أن تلعب المراجعة الداخلية دوراً مهماً وبارزاً في إدارة المخاطر السيبرانية من

خلال إجراء تقييم شامل للمخاطر الإلكترونية ويمثل برنامج توكيد الجودة والتحسين (The QAIP) (Quality assurance and Improvement Program) الخاص بالمراجعة الداخلية معياراً لتقييم جودة المراجعة الداخلية وبالتالي من المتوقع أن ترتبط المراجعة الداخلية عالية الجودة بشكل كبير وإيجابي بمراجعة الأمن السيبراني والحد من مخاطره.

4/3 حجم قسم المراجعة ومشاركته في تطوير بيئة الأعمال: من المهم أن تدرك منشأة

الأعمال أن الاستثمار التكنولوجي في المراجعة الداخلية له عائد ومردود إيجابي وبالتالي يكون لإدارة المراجعة الداخلية حجم يتناسب مع مكانتها وأهميتها لكل مصرف، ويزيد من فعالية إدارة المراجعة الداخلية تواصلها الدائم مع كافة الإدارات وخاصة مع إدارة المخاطر ولجنة المراجعة، فمن المعروف أن لجنة المراجعة تتمتع بتأثير هائل على المراجعة الداخلية حيث يقوم المديرون التنفيذيون للمراجعة بتقديم تقرير إلى لجنة المراجعة تخضع مجالات عمل المراجع الداخلي لمسؤوليات اللجنة ولذلك يجب أن يلعب المراجع الداخلي دوراً مركزياً في مساعدة لجنة المراجعة على الإشراف على الأمن السيبراني، والجدير بالذكر أن اجتماعات المراجعين الداخليين المتكررة مع لجنة المراجعة يقلل من احتمالية حدوث مشاكل تتعلق بمراجعة الأمن السيبراني، نظراً لتقارب المسافات بين لجنة المراجعة وإدارة المراجعة الداخلية ورفع التقارير إلى الإدارة العليا، هذا علاوة على دعم مشاركة المراجعين الداخليين في طرح وتطوير الرؤى حول مخاطر الأمن السيبراني.

ويرى الباحث أن المراجع الداخلي مطالب بتوفير تأكيدات معقولة عن مدى توافر متطلبات أمن الأنظمة والمعلومات وتأكيد كفاءتها وفعاليتها، لتحقيق متطلبات الأمن السيبراني، ومما لا شك فيه أن قيامه بهذا العمل يتطلب منه تطوير ذاته ليمتلك المهارات اللازمة لتقييم إدارة مخاطر الأمن السيبراني بشكل فعال، وفهم وتقييم إجراءات التعامل مع المخاطر المتوقعة نظراً لأن فرق المراجعة الداخلية التي تمتلك مهارات رقمية ولديها إدراك بأهمية الامكانيات الرقمية، وكيفية الاستفادة منها سوف تمثل قيمة مضافة للمصرف مما ينعكس بشكل قوي على جذب العديد من الاستثمارات ودعم كفاءة القرار الاستثماري.

تحليل العلاقة بين جودة المراجعة الداخلية المستخدمة في الحد من مخاطر الأمن السيبراني وتأثير ذلك على ترشيد قرارات المستثمرين:

نال موضوع إدارة مخاطر الأمن السيبراني والحوادث المتعلقة به اهتماماً بالغاً من جانب الباحثين والجهات المهنية والأكاديمية، نظراً لتأثيره الكبير على قرارات بعض أصحاب المصالح مثل المحللين الماليين وكذلك على الأداء المالي للمنشآت وسمعتها، وتعتبر مخاطر الأمن السيبراني من أكبر المخاطر التي تواجهها المنشآت حيث على غرار المخاطر المالية ومخاطر السمعة التي تتعرض لها المنشآت يمكن لمخاطر الأمن السيبراني أن تؤدي إلى ارتفاع التكاليف والتأثير السلبي على عوائد المنشآت والإضرار بقدرة المنشآت على الابتكار واكتساب العملاء والحفاظ عليهم حيث أن الهجمات الإلكترونية مكلفة ولها تأثير واضح على المركز المالي للمنشآت مما يؤثر على القرارات الاستثمارية بشكل كبير، وهذا ما أكدت عليه دراسة كل من (Kelton & Pennington,2020; Tuson,2021, Frank et al.,2019; Kamiya et al., 2021)(علي وعلي،2022).

وفي سياق متصل فقد أكدت دراسة (AL-Moshaigeh et al.,2019; Badawy,2021) على أن تعد الهجمات الإلكترونية مكلفة وقد يكون لها تأثير شديد على الوضع المالي للمنشأة وقد تتسبب في تحريف جوهري في سجلات المنشأة والحد من قدرة المنشأة على الاستمرار، ولهذا السبب تعتبر مخاطر الأمن السيبراني ذات أهمية كبيرة للمستثمرين أثناء عملية اتخاذ القرار الاستثماري، واستناداً إلى استطلاع تم إجرائه بمركز الجودة.

الفصل الرابع

الدراسة الميدانية

المبحث الأول/ الإجراءات المنهجية المتبعة في الدراسة

المبحث الثاني/ عرض البيانات الأولية للدراسة واختبار فرضيات الدراسة

المبحث الثالث/ النتائج والتوصيات

تمهيد

قسم هذا الفصل إلى ثلاثة مباحث: يستعرض المبحث الأول الإجراءات المنهجية المتبعة في الدراسة، بينما يصف المبحث الثاني عرض البيانات وتحليل البيانات الأولية للدراسة واختبار فرضيات الدراسة، أما المبحث الثالث فتمثل في النتائج والتوصيات، وتم التحليل الإحصائي باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية المعروف اختصاراً (SPSS) الاصدار (24)، حيث تم استخدام عدد من الأساليب الإحصائية التي تساعد في الوصول إلى نتائج عملية تخدم أهداف الدراسة وتختبر فرضياتها.

المبحث الأول/ الإجراءات المنهجية المتبعة في الدراسة

أولاً: نبذة مختصرة عن شركات الاتصالات قيد الدراسة.

في ضوء طبيعة الدراسة الحالية، فقد اقتصر مجتمع الدراسة على عدد من شركات الاتصالات العاملة بمدينة طرابلس، وهي: المدار الجديد، وليبيانا للهاتف المحمول، وهاتف ليبيا، وذلك لارتباط هذه الشركات المباشر ببيئة الاتصالات وتقنية المعلومات، واعتمادها الكبير على البنية الرقمية والأنظمة الإلكترونية في تقديم خدماتها وتشغيل أعمالها. وتعد هذه الشركات من المؤسسات الحيوية في قطاع الاتصالات الليبي، الأمر الذي يجعلها بيئة مناسبة لدراسة دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني، بالنظر إلى ما تتعرض له مؤسسات الاتصالات من مخاطر تشغيلية وتقنية ومعلوماتية متزايدة.

1- شركة المدار الجديد

تُعد شركة المدار الجديد من أبرز شركات الاتصالات في ليبيا، وهي شركة حكومية تأسست سنة 1995 وتتخذ من مدينة طرابلس مقراً لها. وتقدم الشركة خدمات الاتصالات الخلوية والبيانات، وتُعرّف نفسها بأنها من أوائل مشغلي الهاتف المحمول في ليبيا وشمال أفريقيا، كما تؤكد في موادها التعريفية سعيها إلى تقديم خدمات اتصالات مبتكرة وعالية الجودة، إلى جانب التوسع في الخدمات الرقمية والإلكترونية الموجهة للأفراد وقطاع الأعمال. وتكتسب الشركة أهمية خاصة في هذه الدراسة لكونها تعمل في بيئة رقمية تعتمد على الاتصال المستمر، وتقديم الخدمات عبر البنية التقنية الحديثة، وهو ما يجعل قضايا الرقابة الداخلية، وإدارة المخاطر، وحوكمة أمن المعلومات ذات صلة مباشرة بطبيعة نشاطها. (<https://www.almdar.ly>)

2- شركة ليبيا نا للهاتف المحمول

تُعد شركة ليبيا نا للهاتف المحمول إحدى الشركات الرئيسة في سوق الاتصالات الليبي، وقد بدأت نشاطها في سبتمبر 2004 بهدف بناء وتطوير شبكة اتصالات لاسلكية تدعم خدمات الهاتف المحمول في مختلف المناطق الليبية. وتشير الشركة في صفحتها التعريفية إلى توسعها في تقديم خدمات الإنترنت والرسائل والخدمات المضافة، فضلاً عن مواكبة التطورات التقنية من خلال خدمات الجيل الثالث المطور والجيل الرابع، وانتشار مراكز خدماتها في المدن الليبية. وتتبع أهمية إدراج ليبيا نا ضمن مجتمع الدراسة من كونها شركة تعتمد بدرجة كبيرة على النظم الرقمية والبنية الشبكية في تشغيل خدماتها، بما يجعل فاعلية المراجعة الداخلية في مجالات الحوكمة، والرقابة، وإدارة المخاطر، ذات أهمية كبيرة في الحد من المخاطر السيبرانية المرتبطة بطبيعة نشاطها. (<https://libyana.ly>)

3- شركة هاتف ليبيا

تُعد شركة هاتف ليبيا إحدى الشركات التابعة لـ الشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة (LPTIC)، وقد تأسست سنة 2008 بهدف تشغيل وصيانة المنظومات السيادية وتطوير الشبكة الوطنية للتراسل ووسائط الربط داخل المدن، فضلاً عن تقديم خدمات الهاتف الثابت والخدمات المرتبطة بالبنية التحتية للاتصالات. وتُظهر المواد التعريفية والخدمية للشركة أنها تضطلع بدور محوري في مجال خدمات التراسل، والألياف البصرية، وخدمات الهاتف الثابت، وهو ما يمنحها أهمية خاصة ضمن هذه الدراسة؛ لأن طبيعة أعمالها ترتبط مباشرة بالبنية الأساسية للاتصالات، الأمر الذي يجعل أمن المعلومات، واستمرارية الخدمات، وكفاءة أنظمة الرقابة وإدارة المخاطر، من الموضوعات الجوهرية في بيئة عملها. (<https://hlc.ly>)

ثانياً: منهجية الدراسة

1. منهج الدراسة

تم استخدام المنهج الوصفي التحليلي لأنه يتناسب مع طبيعة الدراسة، كونه لا يقتصر فقط على جمع البيانات لظاهرة معينة، بل يتناول تحليل هذه الظاهرة ورصدها، ويتناول علاقتها بالظواهر الأخرى، ناهيك عن كونه الأسلوب الأكثر استعمالاً.

2. مجتمع وعينة الدراسة

تمثل مجتمع الدراسة في جميع الموظفين بإدارات شركات الاتصالات الليبية / بمدينة طرابلس وهي: (المدار، لبيانا، هاتف ليبيا) البالغ عددهم (220) موظف وموظفة للمسميات الوظيفية (محاسبين ومراجعين، وكل من لديه علاقة بموضوع الدراسة) التي تم الحصول عليها من إدارة شؤون العاملين بشركات الاتصالات الليبية، ونظراً لصعوبة الوصول لجميع مفردات مجتمع الدراسة واستهدافهم جميعاً، لذلك تم استخدام أسلوب المعاينة بدلاً من أسلوب المسح الشامل، وحتى يكون حجم العينة مناسباً لحجم المجتمع المستهدف، والحصول على عينة ممثلة لمجتمع الدراسة تمثيلاً جيداً، فقد تم تحديد حجم العينة عشوائية بعدد (140) مفردة، بناءً على جدول: ((Krejcie nd Morgn (1970)) لتحديد حجم العينة، والجدول التالي يوضح ذلك:-

جدول رقم (2) حركة توزيع الاستبانة على أفراد العينة

البيان	الاستبانات الموزعة	الاستبانات المفقودة	الاستبانات غير الصالحة	الاستبانات الصالحة للتحليل	
				العدد	النسبة من عينة الدراسة
الإجمالي	140	10	6	124	89%

وبهذا يكون حجم الاستبيانات الصالحة للتحليل (124) مفردة من الاستبيانات الموزعة، أي بنسبة (89%).

3. أداة الدراسة (الاستبانة)

صممت استبانة لجمع البيانات، والمخصصة لموظفي شركات الاتصالات الليبية، احتوت على (4) محاور لقياس المتغير المستقل (دور الاتجاهات الحديثة للمراجعة الداخلية في

الحد من مخاطر الأمن السيبراني) في شركات الاتصالات الليبية، يضاف إليها مجموعة من الأسئلة المتعلقة بالخصائص الديموغرافية لموظفي إدارات شركات الاتصالات الليبية، والأسئلة العامة.

والجدول الآتي يبين ملخصاً محتوى الاستبانة: -

جدول رقم (3) محتوى الاستبانة

الجزء الأول	
المؤهل العلمي	
التخصص العلمي	
سنوات الخبرة	
المسمى الوظيفي	
عدد الدورات التدريبية	
مجال الدورات التدريبية	
الجزء الثاني: المتغير المستقل (دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني	
دور إدارة المخاطر في الحد من مخاطر الأمن السيبراني	وتمثله الفقرات: (1- 8)
دور حوكمة الشركات في الحد من مخاطر الأمن السيبراني	وتمثله الفقرات: (9- 17)
دور إضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني	وتمثله الفقرات: (18- 26)

واعتمدت الدراسة على مقياس ليكرت الخماسي لترميز إجابات العينة على فقرات الاستبانة والجدول الآتي يبين ذلك: -

جدول رقم (4) مقياس ليكرت الخماسي

لإجابة	لا أوافق بشدة	لا أوافق	أوافق لحد ما	أوافق	أوافق بشدة
الوزن	1	2	3	4	5

وتم تحديد إجابات أفراد العينة وفق مقياس ليكرت الخماسي وفق الجدول (5.4)، حيث إن طول الفترة المستخدمة هي (5/4) أي حوالي (0.80) وقد حسبت طول الفترة على أساس أن أوزان الاستجابات الخمس (1-2-3-4-5)، وقد حصرت فيما بينها أربع مسافات والجدول الآتي يبين ذلك: -

جدول رقم (5) تحديد الإجابات وفق مقياس ليكرت الخماسي

تقييم المستوى	المتوسط المرجح	اتجاه الرأي
منخفض جداً	من 1 إلى أقل من 1.80	لا أوافق بشدة
منخفض	من 1.80 إلى أقل من 2.60	غير أوافق
متوسط	من 2.60 إلى أقل من 3.40	أوافق لحد ما
مرتفع	من 3.40 إلى أقل من 4.20	أوافق
مرتفع جداً	من 4.20 إلى 5	أوافق بشدة

4. اختبار أداء الدراسة (الاستبانة)

أولاً: الصدق

يقصد به أن المقياس يقيس ما وضع لقياسه، أي يقيس السمة أو الظاهرة التي وُضع لقياسها ولا يقيس غيرها.

طرق حساب الصدق:

صدق الاتساق الداخلي

بعد إتمام إجراءات اختبار الصدق الظاهري (صدق المحكمين) تم توزيع عدد (31) استبانة على المجتمع الأصلي بالنسبة لموظفي شركات الاتصالات الليبية، وذلك لحساب صدق الاتساق الداخلي للمقاييس المستخدمة في الدراسة، من خلال حساب معامل الارتباط بين كل فقرة والدرجة الكلية للمقياس، والجدول الآتي توضح ذلك: -

الاتساق الداخلي لمحاوَر المتغير المستقل (دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني)

1. إدارة المخاطر

جدول رقم (6) معامل الارتباط بين كل فقرة من فقرات إدارة المخاطر والدرجة الكلية

ت	الفقرات	معامل الارتباط	مستوى الدلالة
1	تقييم المخاطر وتطوير استراتيجيات لإدارتها	0.803**	0.000
2	تعزيز كفاءة أساليب الرقابة لتقادي المخاطر	0.834**	0.000
3	تطوير عمليات التصدي للمخاطر داخل الشركة	0.806**	0.000
4	قياس وتحليل المخاطر المكتشفة وفهم طبيعتها	0.652**	0.000
5	تحليل العلاقات بين المخاطر لتقييم تأثيرها على بعضها البعض	0.853**	0.000
6	إعداد تقارير شاملة عن المخاطر وتقديمها لمجلس الإدارة	0.558**	0.000
7	تحسين عملية صناعة القرار، التخطيط، والأولويات	0.783**	0.000
8	تقييم تنفيذ تقنيات معالجة الخطر	0.768**	0.000

يوضح الجدول رقم (6) معامل الارتباط بين كل فقرة من فقرات البُعد والدرجة الكلية للمتغير، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية عند مستوى دلالة (0.000) أقل من مستوى معنوية (0.05) وبذلك يُعد المتغير صادق لما وضع لقياسه.

2. حوكمة الشركات

جدول رقم (7) معامل الارتباط بين كل فقرة من فقرات حوكمة الشركات والدرجة الكلية

ت	الفقرات	معامل الارتباط	مستوى الدلالة
1	توجيه أعمال الشركة ومراقبتها على أعلى مستوى	0.684**	0.000
2	الحفاظ على حقوق أصحاب المصالح والشفافية	0.807**	0.000
3	يتمتع المراجع الداخلي بالاستقلالية الكاملة في أداء واجباته داخل الشركة	0.567**	0.000
4	يتمتع المراجع بمعرفة كافية بطبيعة أعمال الشركة ونشاطاتها التشغيلية	0.688**	0.000
5	يقوم المراجع بتقييم شامل للعمليات ويقدم توصيات فعالة لتحسينها	0.763**	0.000
6	مكافحة الفساد الإداري	0.546**	0.000
7	يقدم المراجع توصيات جوهرية لتحسين العمليات وتقليل المخاطر	0.855**	0.000
8	تحسين مستوى الأداء	0.582**	0.000
9	يراقب المراجع التزام كافة إدارات الشركة بمقومات الجودة	0.827**	0.000

يوضح الجدول رقم (8.4) معامل الارتباط بين كل فقرة من فقرات البُعد والدرجة الكلية للمتغير، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية عند مستوى دلالة (0.000) أقل من مستوى معنوية (0.05) وبذلك يُعد المتغير صادق لما وضع لقياسه.

3. إضافة قيمة للمراجعة

جدول رقم (8) معامل الارتباط بين كل فقرة من فقرات إضافة قيمة للمراجعة والدرجة الكلية

ت	الفقرات	معامل الارتباط	مستوى الدلالة
1	تقديم تقييم مستقل وموضوعي لفعالية إجراءات الرقابة	0.698**	0.000
2	تطوير مبادئ إدارة الشركة بطريقة شاملة وشفافة	0.757**	0.000
3	القدرة على تحقيق قيم إضافية للمساهمين	0.826**	0.000
4	توفير معلومات موثوقة وشفافة حول مخاطر الشركة	0.775**	0.000
5	إرساء قواعد الشفافية لحماية مصالح جميع الأطراف المعنية	0.781**	0.000
6	تنفيذ سياسات لمنع وتقييد الممارسات التي تعرقل الحوكمة	0.808**	0.000
7	مناقشة المشاكل الناتجة عن وجودها في الشركة بشكل فوري وفعال	0.755**	0.000
8	ضمانة الحماية الكاملة للأصول والتشريعات	0.772**	0.000
9	ضمان الالتزام بالقوانين	0.647**	0.000

يوضح الجدول رقم (9.4) معامل الارتباط بين كل فقرة من فقرات البُعد والدرجة الكلية للمتغير، والذي يبين أن معاملات الارتباط المبيّنة بالجدول دالة إحصائية عند مستوى دلالة (0.000) أقل من مستوى معنوية (0.05) وبذلك يُعد المتغير صادق لما وضع لقياسه.

ثانياً: ثبات أداء الدراسة (الاستبانة)

وقد تم استخدام معامل ألفا كرونباخ لقياس (الاستبانة) ولكل بُعد من أبعادها، وقد كانت معاملات الثبات تتمتع بدلالات ثبات مقبولة لغايات البحث العلمي، حيث وُجد أن قيمة معامل ألفا كرونباخ للمتغيرات، إذ النسب تزيد عن النسبة المقبولة إحصائياً والبالغة (60%) حسب

(Sekaran)، وهذا يدل على إمكانية ثبات النتائج التي يمكن أن تترتب عند تطبيق الاستبانة (Sekaran, 2003).

جدول رقم (9) معاملات الثبات لمتغيرات الدراسة

محاور الدراسة	عدد الفقرات	قيمة ألفا كرونباخ
إدارة المخاطر	8	0.908
حوكمة الشركات	9	0.853
إضافة قيمة للمراجعة	9	0.904
المحاور ككل	26	0.949

واضح من النتائج الواردة بالجدول رقم (9) أن قيم معامل ألفا كرونباخ كانت جيدة ومقبولة لجميع المتغيرات، وبذلك يكون الباحث قد تأكد من صدق وثبات (الاستبانة) وبذلك تكون الاستبانة جاهزة للتحليل الإحصائي.

الأساليب الإحصائية المستخدمة في تحليل البيانات الأولية:

اعتمدت الدراسة في تحليل البيانات الأولية للدراسة على الأساليب الإحصائية الآتية:

1. النسبة المئوية: استخدم لمعرفة التوزيع النسبي لمفردات مجتمع الدراسة
2. المتوسط الحسابي: استخدم لقياس متوسط إجابات لمفردات مجتمع الدراسة على فقرات (الاستبانة).
3. الانحراف المعياري: استخدم لقياس الانحرافات في إجابات لمفردات مجتمع الدراسة على فقرات (الاستبانة)
4. معامل كرونباخ ألفا: استخدم للتحقق من ثبات أداة الدراسة (الاستبانة).
5. معامل الارتباط: استخدم في الاتساق الداخلي.
6. اختبار T للعينة الواحدة (One Sample T-Test): يستخدم لاختيار دلالة المتوسطات الحسابية وذلك لاختبار فرضيات الدراسة ويستخدم إذا كان حجم المجتمع أكثر من 30 مفردة.

المبحث الثاني:

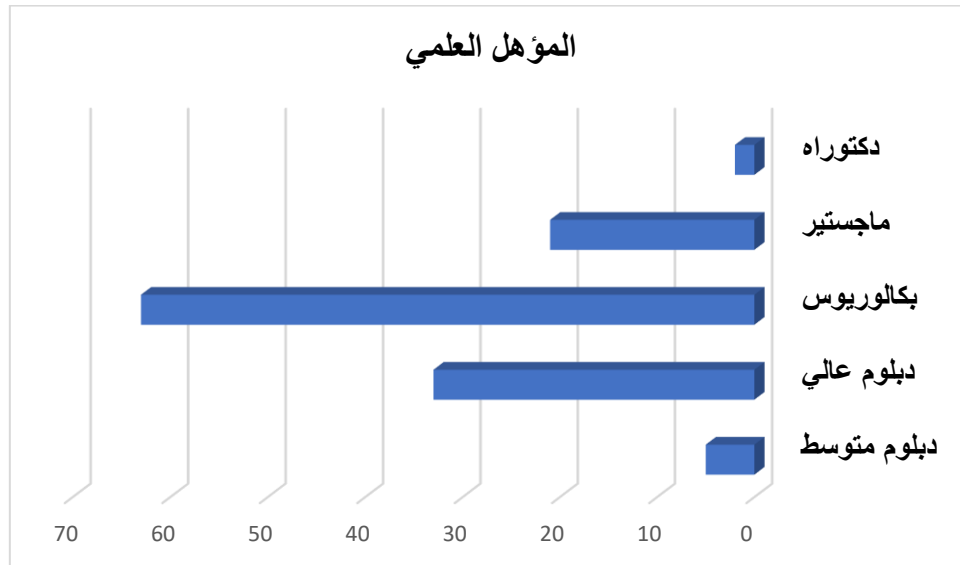
عرض البيانات الأولية للدراسة واختبار فرضيات الدراسة

أولاً: وصف الخصائص:

1. المؤهل العلمي:

الجدول رقم (10) التوزيع التكراري لمفردات عينة الدراسة حسب المؤهل العلمي

الرقم	المؤهل العلمي	التكرار	النسبة %
1	دبلوم متوسط	5	4.0
2	دبلوم عالي	33	26.6
3	بكالوريوس	63	50.8
4	ماجستير	21	16.9
5	دكتوراه	2	1.6
	المجموع	124	100.0



الشكل البياني رقم (2) التوزيع التكراري لمفردات عينة الدراسة حسب المؤهل العلمي

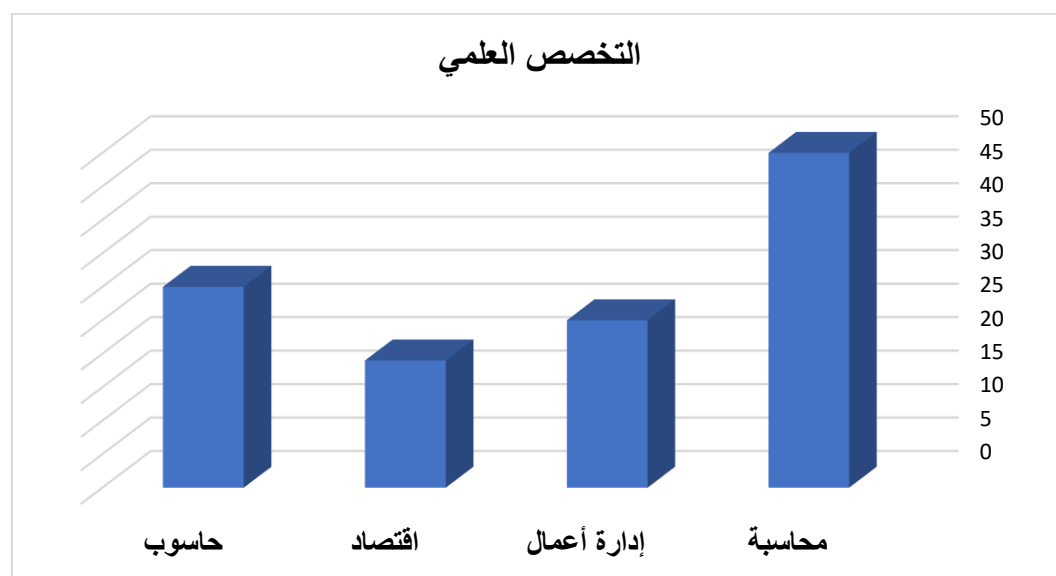
من خلال الجدول السابق نلاحظ أن أغلب مفردات عينة الدراسة يحملون التخصص العلمي (بكالوريوس) ويمثلون نسبته (50.8%) من إجمالي مفردات عينة الدراسة، ثم يليهم للمؤهل العلمي (دبلوم عالي)، ويمثلون بنسبة (26.6%)، ثم يلي ذلك للمؤهل العلمي (ماجستير) بنسبة

(16.9%)، وباقي النسب وزعت على المؤهلات العلمية (دبلوم متوسط) و(دكتوراه) بنسب متدنية من إجمالي مفردات عينة الدراسة.

2. التخصص العلمي

الجدول رقم (11) التوزيع التكراري لمفردات عينة الدراسة حسب التخصص العلمي

الرقم	التخصص العلمي	التكرار	النسبة %
1	محاسبة	50	40.3
2	إدارة أعمال	25	20.2
3	اقتصاد	19	15.3
4	حاسوب	30	24.2
	المجموع	124	100.0



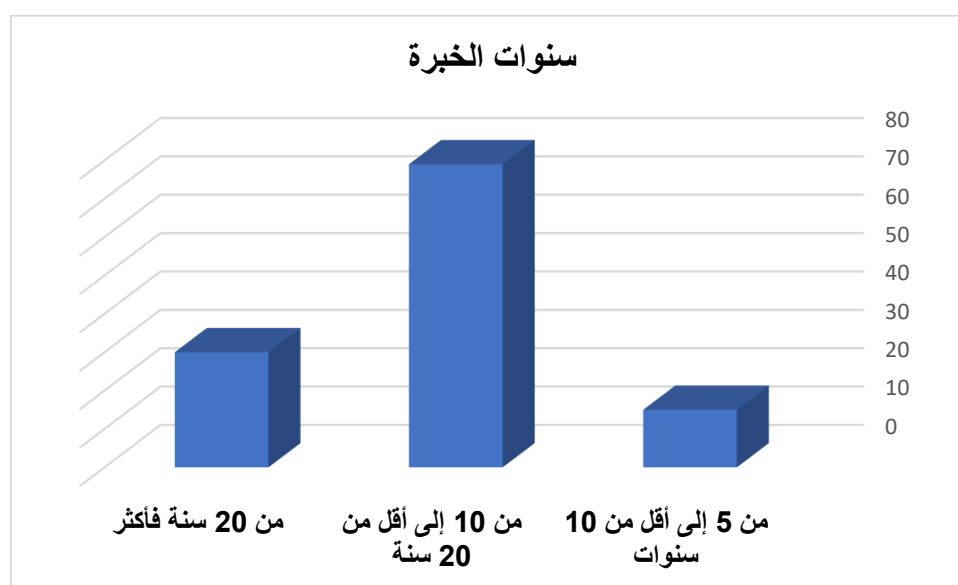
الشكل البياني رقم (3) التوزيع التكراري لمفردات عينة الدراسة حسب التخصص العلمي

من خلال الجدول السابق نلاحظ أن أغلب مفردات عينة الدراسة تخصصهم العلمي (محاسبة) ويمثلون بنسبة (40.3%)، من إجمالي العينة، ثم يليهم التخصص العلمي (حاسوب) بنسبة (24.2%)، ويليه للتخصص العلمي (إدارة أعمال)، ثم يليهم للتخصص العلمي (اقتصاد) بنسبة (15.3%) من إجمالي عينة الدراسة.

3. سنوات الخبرة

الجدول رقم (12) يبين التوزيع التكراري لمفردات عينة الدراسة حسب سنوات الخبرة

الرقم	سنوات الخبرة	التكرار	النسبة %
1	من 5 إلى أقل من 10 سنوات	15	12.1
2	من 10 إلى أقل من 20 سنة	79	63.7
3	من 20 سنة فأكثر	30	24.2
	المجموع	124	100.0



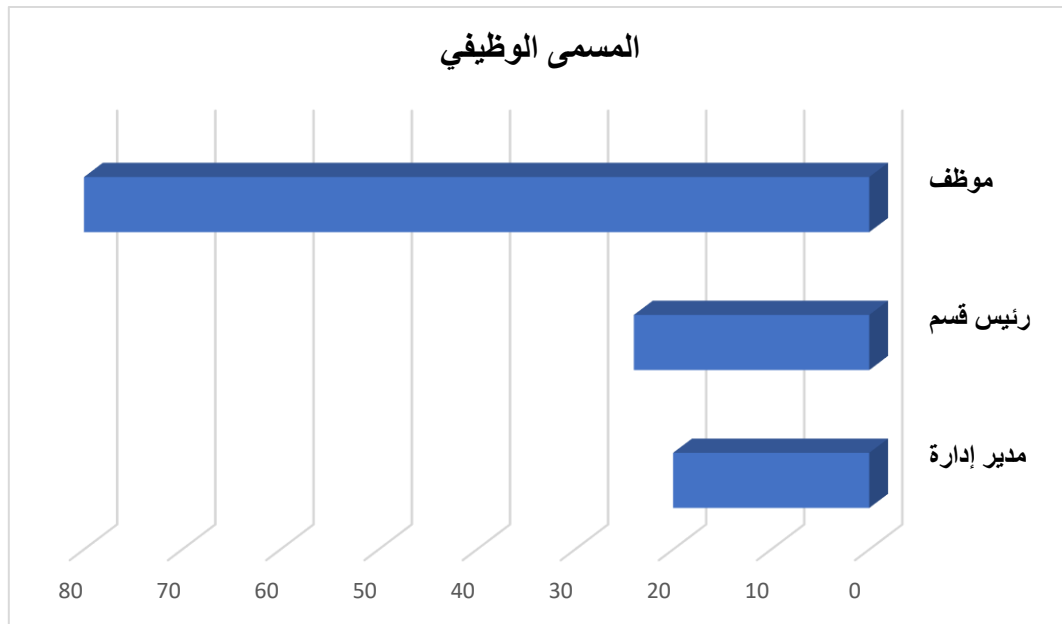
الشكل البياني رقم (4) التوزيع التكراري لمفردات عينة الدراسة حسب سنوات الخبرة

في الجدول والشكل البياني السابقين نلاحظ أن سنوات الخبرة تتراوح (من 10 إلى أقل من 20 سنة) بنسبة (63.7%) ويشكلون النسبة الأكبر من إجمالي مفردات عينة الدراسة، ثم يليه لسنوات الخبرة (من 20 سنة فأكثر)، بنسبة (24.2%) من إجمالي المفردات، وأقل نسبة لمن تتراوح خبرتهم (من 5 إلى أقل من 10 سنوات) وتشير هذه النسب على وجود سنوات خبرة جيدة لمفردات عينة الدراسة.

4. المسمى الوظيفي

الجدول رقم (13) يبين التوزيع التكراري لمفردات عينة الدراسة المسمى الوظيفي

الرقم	المسمى الوظيفي	التكرار	النسبة %
1	مدير إدارة	20	16.1
2	رئيس قسم	24	19.4
3	موظف	80	64.5
	المجموع	124	100



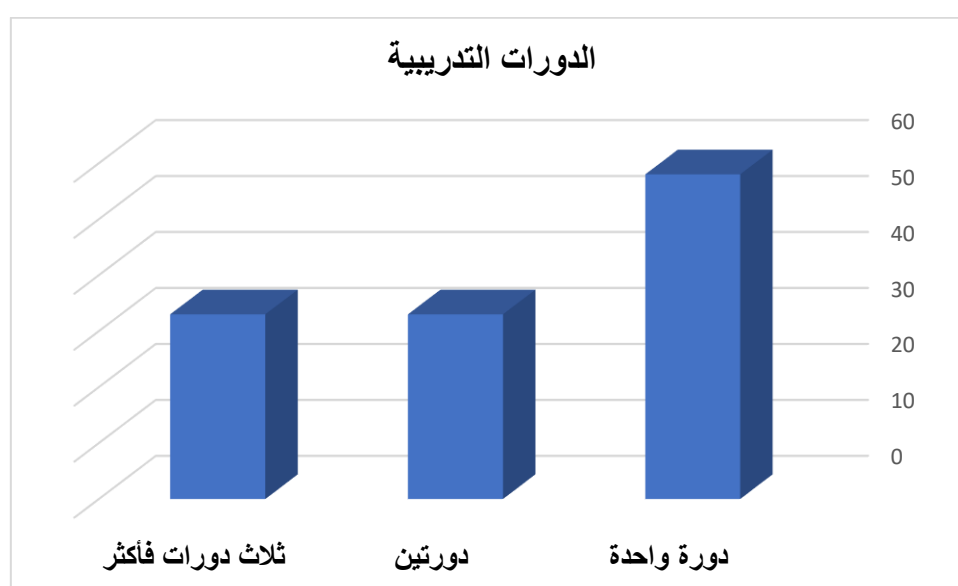
الشكل البياني رقم (5) التوزيع التكراري لمفردات عينة الدراسة حسب المسمى الوظيفي

يتضح من الجدول والشكل البياني السابقين أن أغلب المبحوثين كانوا (موظفين) ويمثلون نسبة (64.5%) ثم يليه للمسمى الوظيفي (رئيس قسم) بنسبة (19.4%) من إجمالي مفردات عينة الدراسة، ثم المسمى الوظيفي (مدير إدارة) بأقل نسبة بلغت (16.1%) من إجمالي عينة الدراسة.

5. عدد الدورات التدريبية

الجدول رقم (14) التوزيع التكراري لمفردات عينة الدراسة حسب الدورات التدريبية

الرقم	الدورات التدريبية	التكرار	النسبة %
1	دورة واحدة	58	46.8
2	دورتين	33	26.6
3	ثلاث دورات فأكثر	33	26.6
	المجموع	124	100



الشكل البياني رقم (6) التوزيع التكراري لمفردات عينة الدراسة حسب عدد الدورات التدريبية

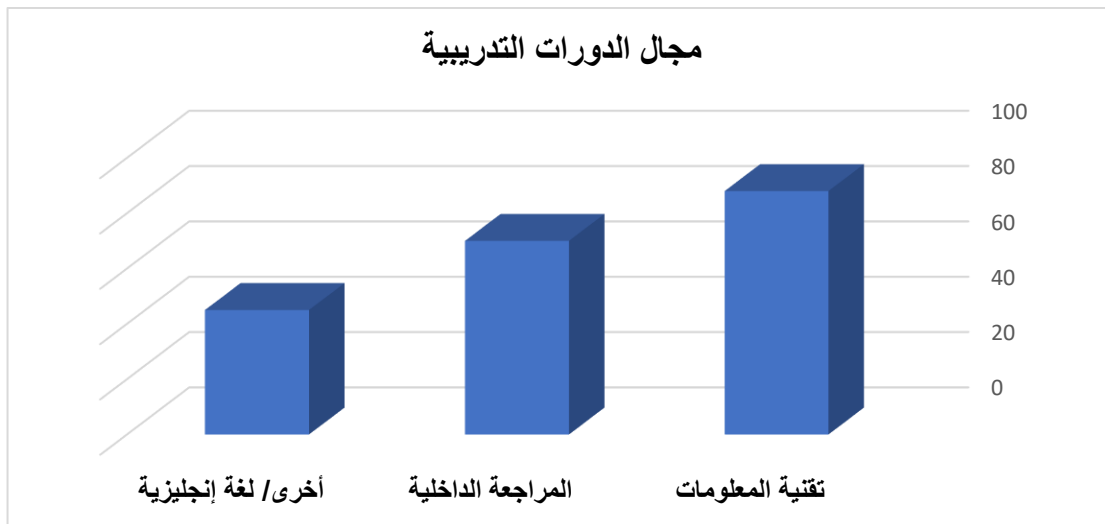
من الجدول والشكل البياني السابقين يتضح أن غالبية أفراد العينة تحصلوا على دورة تدريبية في مجال عملهم بنسبة أن (46.8%)، في حين جاءت بنسبة متساوية بلغت (26.6%) ممن تلقوا دورتين وثلاث دورات تدريبية فأكثر من إجمالي عينة الدراسة

6. مجال الدورات التدريبية

الجدول رقم (15) يبين التوزيع التكراري لمفردات عينة الدراسة حسب مجال الدورات التدريبية

الرقم	مجال الدورات التدريبية	التكرار	النسبة %
1	تقنية المعلومات	88	71.0
2	المراجعة الداخلية	70	56.5
3	أخرى/ لغة إنجليزية	45	36.3
	مجموع العينة	124	100

- يمكن للمستجيب اختيار أكثر من إجابة



الشكل البياني رقم (7) التوزيع التكراري لمفردات عينة الدراسة حسب مجال الدورات التدريبية

يتضح من الجدول والشكل البياني السابقين أن أغلب المبحوثين تلقوا دورات تدريبية في مجال تقنية المعلومات بنسبة (71%) ثم يليه في مجال (المراجعة الداخلية) بنسبة (56.5%) من إجمالي مفردات عينة الدراسة، ثم في مجالات أخرى/ لغة إنجليزية بأقل نسبة بلغت (36.3%) من إجمالي عينة الدراسة.

ثانياً: وصف متغيرات الدراسة

للإجابة على التساؤل الرئيسي: هل يوجد دور للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة؟
تم استخدام المتوسط الحسابي والانحراف المعياري لكل محور فرعي على حدى والجدول الآتية تبين ذلك: -

1. (دور للإدارة المخاطر في الحد من مخاطر الأمن السيبراني)

الجدول رقم (16) المتوسط الحسابي والانحراف المعياري لفقرات إدارة المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1 تقييم المخاطر وتطوير استراتيجيات لإدارتها	4.27	0.980	مرتفع جداً
2 تعزيز كفاءة أساليب الرقابة لنفاذ المخاطر	4.20	0.925	مرتفع جداً
3 تطوير عمليات التصدي للمخاطر داخل الشركة	4.20	0.847	مرتفع جداً
4 قياس وتحليل المخاطر المكتشفة وفهم طبيعتها	4.00	0.910	مرتفع
5 تحليل العلاقات بين المخاطر لتقييم تأثيرها على بعضها البعض	4.07	0.868	مرتفع
6 إعداد تقارير شاملة عن المخاطر وتقديمها لمجلس الإدارة	4.07	0.868	مرتفع
7 تحسين عملية صناعة القرار، التخطيط، والأولويات	4.10	0.885	مرتفع
8 تقييم تنفيذ تقنيات معالجة الخطر	4.00	0.947	مرتفع
المتوسط الحسابي العام	4.11	0.705	مرتفع

يتضح من الجدول السابق أن الفقرة التي تنص على "تقييم المخاطر وتطوير استراتيجيات لإدارتها" جاءت في المرتبة الأولى، بمتوسط حسابي بلغ (4.27) وانحراف معياري (0.980)، وبمستوى موافقة مرتفع جداً. في المقابل، جاءت الفقرتان "قياس وتحليل المخاطر المكتشفة وفهم طبيعتها" و"تقييم تنفيذ تقنيات معالجة الخطر" في المرتبة الأخيرة بالتساوي، بمتوسط حسابي بلغ (4.00) لكل منهما، وانحراف معياري بلغ على التوالي (0.910) و (0.947)، وبمستوى موافقة مرتفع.

وتُظهر هذه النتائج أن إجابات أفراد عينة الدراسة تجاه فقرات هذا البُعد جاءت عمومًا بدرجة موافقة مرتفعة، مع درجة تشّتت محدودة نسبيًا، بما يعكس تقاربًا في تقديرات الباحثين لأهمية إدارة المخاطر في الحد من مخاطر الأمن السيبراني. كما بلغ المتوسط الحسابي العام لبُعد إدارة المخاطر (4.11)، بانحراف معياري (0.705)، وهو ما يشير إلى أن هذا البُعد يحظى بمستوى موافقة مرتفع من وجهة نظر أفراد العينة. وعليه، يمكن القول إن إدارة المخاطر تمثل أحد الأبعاد الفاعلة للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات الليبية محل الدراسة.

تتفق هذه النتيجة مع عدد من الدراسات السابقة التي أكدت أن الاتجاهات الحديثة للمراجعة الداخلية تؤدي دورًا مهمًا في دعم إدارة المخاطر والحد من التهديدات المرتبطة بها؛ فقد بينت دراسة الوليد (2017) أن المراجعة الداخلية تسهم في تخفيض المخاطر، وتساعد الإدارة في وضع الخطط والسياسات المناسبة لإدارتها، كما توصلت دراسة صالح (2018) إلى وجود علاقة ذات دلالة إحصائية بين دور المراجعة الداخلية وإدارة المخاطر، وأن المراجعة الداخلية تدعم الإدارة في اتخاذ القرارات الرشيدة من خلال تقديم معلومات دقيقة وتقييمات موضوعية للمخاطر المحتملة. كذلك انسجمت هذه النتيجة مع دراسة بن عطاف (2021) التي أكدت أن الاتجاهات الحديثة للمراجعة الداخلية تساعد في اختيار الأساليب المناسبة لمواجهة المخاطر، ومع دراسة عثمان (2022) التي أوضحت أن وظيفة المراجعة الداخلية تؤدي دورًا رئيسيًا وفعالًا في تقييم الاضطرابات السيبرانية وتحسين حوكمة أمن المعلومات وجهود إدارة المخاطر. كما تتسق هذه النتيجة أيضًا مع دراسة عمر (2023) التي أثبتت وجود علاقة ارتباط بين إدارة المخاطر وأمن نظم المعلومات المحاسبية، فضلًا عن توافقها مع بعض الدراسات الأجنبية مثل Jones & Smith (2019) و Hayek & Smith (2020) اللتين أكدتا أن جودة المراجعة الداخلية وتوظيف الأدوات الحديثة يساهمان في الكشف المبكر عن التهديدات الأمنية وتقليل احتمالات التعرض للهجمات السيبرانية. وبناءً على ذلك، فإن ارتفاع المتوسط الحسابي لبُعد إدارة المخاطر في الدراسة الحالية يعد نتيجة منطقية ومتسقة مع الأدبيات السابقة، ويعكس إدراك الباحثين لأهمية هذا البعد في دعم قدرة شركات الاتصالات على التنبؤ بالمخاطر السيبرانية والتعامل معها بفاعلية.

2. (دور لحوكمة الشركات في الحد من مخاطر الأمن السيبراني)

الجدول رقم (17) المتوسط الحسابي والانحراف المعياري لفقرات حوكمة الشركات

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1 توجيه أعمال الشركة ومراقبتها على أعلى مستوى	3.93	0.944	مرتفع
2 الحفاظ على حقوق أصحاب المصالح والشفافية	4.00	0.830	مرتفع
3 يتمتع المراجع الداخلي بالاستقلالية الكاملة في أداء واجباته داخل الشركة	4.03	0.928	مرتفع
4 يتمتع المراجع بمعرفة كافية بطبيعة أعمال الشركة ونشاطاتها التشغيلية	3.83	0.986	مرتفع
5 يقوم المراجع بتقييم شامل للعمليات ويقدم توصيات فعالة لتحسينها	3.93	8180.	مرتفع
6 محاربة الفساد الإداري	3.80	0.961	مرتفع
7 يقدم المراجع توصيات جوهرية لتحسين العمليات وتقليل المخاطر	3.90	0.995	مرتفع
8 تحسين مستوى الأداء	4.13	0.776	مرتفع
9 يراقب المراجع التزام كافة إدارات الشركة بمقومات الجودة	3.90	0.029	مرتفع
المتوسط الحسابي العام	3.94	0.645	مرتفع

يتضح من الجدول السابق أن الفقرة التي تنص على: "تحسين مستوى الأداء" جاءت في المرتبة الأولى، بمتوسط حسابي بلغ (4.13) وانحراف معياري (0.776)، وبمستوى موافقة مرتفع. في المقابل، جاءت الفقرة التي تنص على: "محاربة الفساد الإداري" في المرتبة الأخيرة، بمتوسط حسابي بلغ (3.80) وانحراف معياري (0.961)، وبمستوى موافقة مرتفع كذلك. كما تشير النتائج إلى أن بقية الفقرات تراوحت متوسطاتها الحسابية بين (3.83) و (4.03)**، وهي جميعها تقع ضمن مستوى الموافقة المرتفع، بما يدل على إدراك أفراد العينة لأهمية حوكمة الشركات في دعم المراجعة الداخلية والحد من مخاطر الأمن السيبراني. وبلغ المتوسط الحسابي العام لهذا البعد (3.94)، بانحراف معياري (0.645)، وهو ما يعكس مستوى موافقة مرتفعاً من

جانب المبحوثين، ويؤكد أن حوكمة الشركات تمثل أحد الأبعاد الفاعلة للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات محل الدراسة.

تتفق هذه النتيجة مع عدد من الدراسات السابقة التي أكدت أهمية البعد الحوكمي في تفعيل دور المراجعة الداخلية والحد من المخاطر. فقد توصلت دراسة صالح (2018) إلى وجود علاقة ذات دلالة إحصائية بين الدور الحوكمي للمراجعة الداخلية وإدارة المخاطر، بما يعني أن تعزيز هذا الدور يسهم في تحسين فعالية التعامل مع المخاطر داخل المؤسسة. كما تتسجم هذه النتيجة مع دراسة عمر (2023) التي بينت أن حوكمة الشركات تعزز الشفافية والدقة في المعلومات، وأوصت بتعزيزها بوصفها أحد الاتجاهات الحديثة في المراجعة الداخلية. كذلك تتفق النتيجة مع دراسة عثمان (2022) التي أوضحت أن وظيفة المراجعة الداخلية تؤدي دوراً رئيسياً في تحسين وحوكمة أمن المعلومات وجهود إدارة المخاطر السيبرانية، وهو ما يدعم ما توصلت إليه الدراسة الحالية من أن حوكمة الشركات تسهم بدرجة مرتفعة في الحد من مخاطر الأمن السيبراني. كما يمكن الاستئناس بنتائج دراسة الشيخ وأحمد (2023) التي أثبتت أن تفعيل عناصر الرقابة الداخلية وفق إطار COSO يسهم في تقليل مخاطر المحاسبة السحابية، وأن الأمن السيبراني يعزز فعالية الرقابة الداخلية؛ وهو ما ينسجم مع مضمون الحوكمة من حيث الالتزام والرقابة والجودة. وفي المقابل، تختلف هذه النتيجة جزئياً مع دراسة الزيود (2021) التي لم تجد أثراً لحياضية التدقيق الداخلي في الحد من المخاطر السيبرانية، إلا أن هذا الاختلاف يظل جزئياً؛ لأن الدراسة الحالية لم تتناول الحياضية منفردة، بل تناولت حوكمة الشركات كبعد أشمل يضم الشفافية، والاستقلالية، وتحسين الأداء، والرقابة على الجودة، وهي عناصر ظهرت جميعها بمستوى موافقة مرتفع لدى أفراد العينة. وعليه، فإن النتيجة الحالية تبدو منسجمة في مجملها مع الاتجاه الغالب في الأدبيات السابقة الذي يؤكد أن تفعيل الحوكمة داخل بيئة المراجعة الداخلية يعزز قدرة المؤسسات على الحد من المخاطر السيبرانية ورفع مستوى الرقابة والالتزام المؤسسي.

3. (دور لإضافة القيمة للمراجعة في الحد من مخاطر الأمن السيبراني)

الجدول رقم (18) المتوسط الحسابي والانحراف المعياري لفقرات إضافة قيمة للمراجعة

العبارة	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1 تقديم تقييم مستقل وموضوعي لفعالية إجراءات الرقابة	4.27	0.868	مرتفع جداً
2 تطوير مبادئ إدارة الشركة بطريقة شاملة وشفافة	4.07	0.785	مرتفع
3 القدرة على تحقيق قيم إضافية للمساهمين	4.00	0.910	مرتفع
4 توفير معلومات موثوقة وشفافة حول مخاطر الشركة	4.10	0.759	مرتفع
5 إرساء قواعد الشفافية لحماية مصالح جميع الأطراف المعنية	3.80	0.805	مرتفع
6 تنفيذ سياسات لمنع وتقييد الممارسات التي تعرقل الحوكمة	3.93	0.944	مرتفع
7 مناقشة المشاكل الناتجة عن وجودها في الشركة بشكل فوري وفعال	3.97	0.999	مرتفع
8 ضمان الحماية الكاملة للأصول والتشريعات	3.73	0.944	مرتفع
9 ضمان الالتزام بالقوانين	4.13	0.819	مرتفع
المتوسط الحسابي العام	4.00	0.657	مرتفع
المتوسط الحسابي الكلي	4.01	0.605	مرتفع

يتضح من الجدول السابق أن الفقرة التي تنص على أن: (تقديم تقييم مستقل وموضوعي لفعالية إجراءات الرقابة) جاءت في المرتبة الأولى بمتوسط حسابي (4.27)، وانحراف معياري (0.868) بمستوى موافقة مرتفع جداً، في حين جاءت الفقرة التي تنص على: (ضمانة الحماية الكاملة للأصول والتشريعات) في المرتبة الأخيرة، بمتوسط حسابي (3.73) وانحراف معياري (0.944) بمستوى موافقة مرتفع، ونلاحظ أن إجابات أفراد عينة الدراسة حول هذا البُعد جاءت بمستوى موافقة مرتفعة لكل الفقرات وانحرافات صغيرة، مما يشير إلى تشتت قليل في إجابات مفردات العينة، وأخيراً بلغ المتوسط الحسابي العام لمتغير دور لإضافة القيمة للمراجعة في الحد من مخاطر الأمن السيبراني (4.00)، وبانحراف معياري (0.657)، مما يؤكد أن أغلب إجابات أفراد العينة جاءت بدرجة موافقة مرتفعة، ويدل على أنه يوجد دور لإضافة القيمة للمراجعة كبُعد

من أبعاد للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني من وجهة نظر موظفي شركات الاتصالات حسب المقياس المعتمد في الدراسة.

ونلاحظ أن المتوسط الحسابي لدور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني ككل بلغ (4.01)، وانحراف معياري (0.605) ويعبر عن درجة موافقة مرتفعة، ويدل على أنه يوجد دور للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني ككل من وجهة نظر موظفي شركات الاتصالات حسب المقياس المعتمد في الدراسة.

تتفق هذه النتيجة مع عدد من الدراسات السابقة التي أكدت أن المراجعة الداخلية الحديثة لا يقتصر دورها على الفحص والرقابة التقليدية، بل يمتد إلى إضافة قيمة للمؤسسة من خلال التقييم الموضوعي، وتقديم التوصيات، ودعم الشفافية، وتعزيز القدرة على مواجهة المخاطر. فقد توصلت دراسة الشيخ (2020) إلى وجود علاقة ذات دلالة إحصائية بين بعد إضافة القيمة وتحسين الأداء، وأوصت بتنفيذ الأنشطة الحديثة للمراجعة الداخلية، ومنها إضافة القيمة الاقتصادية والدور التوكيدي والخدمات الاستشارية، لما لها من دور في مجابهة المخاطر والسلامة المؤسسية. كما تتسجم النتيجة الحالية مع دراسة عثمان (2022) التي أوضحت أن وظيفة المراجعة الداخلية تؤدي دوراً رئيسياً وفعالاً في مراجعة الأمن السيبراني من خلال توفير دليل مستقل وموضوعي على الالتزام بالسياسات، وتكوين رؤية لتحسين حوكمة أمن المعلومات وجهود إدارة المخاطر. كذلك تتفق مع دراسة أبو الخير (2023) التي بينت أن جودة المراجعة الداخلية تساعد المؤسسات المالية على اتخاذ إجراءات وقائية أكثر وضوحاً في مواجهة المخاطر السيبرانية، بما يدعم الاستقرار المؤسسي. وعلى المستوى الأجنبي، تتوافق هذه النتيجة مع دراسة Jones & Smith (2019) التي أكدت أن جودة المراجعة الداخلية واستخدام الأدوات الحديثة يساهمان في الكشف المبكر عن التهديدات الأمنية والحد من آثارها، ومع دراسة Hayek & Smith (2020) التي أوضحت أن المراجعة الداخلية الجيدة تؤدي دوراً أساسياً في تقييم أنظمة الأمن السيبراني واكتشاف الثغرات وتقليل احتمالات التعرض للهجمات. كما يمكن الاستئناس جزئياً بدراسة صالح علي صالح (2022) التي أكدت أهمية بناء مؤشرات وإجراءات لقياس فعالية توكيد المراجعة الداخلية على الأمن السيبراني، وهو ما يدعم فكرة أن القيمة المضافة للمراجعة لا تتحقق فقط من خلال الرقابة، بل أيضاً من خلال التوكيد والتطوير المستمر. وبذلك، فإن ارتفاع

المتوسط الحسابي لهذا البُعد في الدراسة الحالية يعكس انسجامًا واضحًا مع الاتجاه الغالب في الأدبيات السابقة، الذي يرى أن إضافة القيمة للمراجعة الداخلية تمثل آلية حديثة وفعالة في دعم المؤسسة للحد من مخاطر الأمن السيبراني.

ثالثاً: اختبار فرضيات الدراسة

من المهم قبل الخوض في اختبار فرضيات الدراسة تحديد القواعد التي تم إتباعها والمتمثلة في الآتي:

1. مستوى المعنوية (الدلالة) لهذه الدراسة يساوي (0.05)، ودرجة الثقة المتبعة في هذه الدراسة (95%).

2. تم الاختبار من خلال المقارنة بين مستوى المعنوية لهذه الدراسة والذي يساوي (0.05)، وقيمة مستوى المعنوية (الدلالة) المشاهد، وبناءً على ذلك يتم رفض الفرضية الصفرية وقبول الفرضية البديلة في حال أن كانت قيمة مستوى المعنوية المشاهد أقل من مستوى المعنوية لهذه الدراسة (0.05) والعكس صحيح.

اختبار فرضية الدراسة الرئيسية

لاختبار فرضية البحث الرئيسية والتي تنص على: يوجد دور ذو دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

لاختبار الفرضية الرئيسية يمكن صياغتها بصورة إحصائية كالتالي:

H0: لا يوجد دور ذو دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

H1: يوجد دور ذو دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

ولاختبار الفرضية، استخدم الباحث اختبار T للعينة الواحدة (One Sample T-Test) وذلك للتحقق من صحة هذه الفرضية، والجدول التالي يبين المتوسط الحسابي والانحراف المعياري، وكذلك نتائج اختبار T (قيمة الاختبار والدلالة الإحصائية).

جدول رقم (19) اختبار T للمحور الأول

المتوسط الحسابي	الانحراف المعياري	إحصاء اختبار T	الدلالة الإحصائية	النتيجة
4.01	0.605	12.790	0.000	رفض H0

أظهرت نتائج اختبار (T) للعينة الواحدة للجدول السابق أن المتوسط الحسابي لاستجابات أفراد مفردات العينة حول المحور يساوي (4.01)، وهو ما يُصنف ضمن فئة "المرتفع" وفقاً لمقياس ليكرت الخماسي، كما أظهر التحليل وجود فرق دال إحصائياً بين المتوسط المحسوب والمتوسط المعتمد في الدراسة، حيث بلغت قيمة الدلالة الإحصائية (0.000) وهي أصغر من مستوى الدلالة المعتمد في الدراسة (0.05)، مما يدعم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على أنه: يوجد دور ذو دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

الفرضيات الفرعية:

الفرضية الفرعية الأولى: يوجد دور ذو دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

لاختبار الفرضية الفرعية الأولى يمكن صياغتها بصورة إحصائية كالتالي:

H0: لا يوجد دور ذو دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

H1: يوجد دور ذو دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

ولاختبار الفرضية، استخدم الباحث اختبار T للعينة الواحدة (One Sample T-Test) وذلك للتحقق من صحة هذه الفرضية، والجدول التالي يبين المتوسط الحسابي والانحراف المعياري، وكذلك نتائج اختبار T (قيمة الاختبار والدلالة الإحصائية).

جدول رقم (20) اختبار T للمحور الأول

المتوسط الحسابي	الانحراف المعياري	إحصاء اختبار T	الدلالة الإحصائية	النتيجة
4.11	0.705	11.749	0.000	رفض H0

أظهرت نتائج اختبار (T) للعينة الواحدة للجدول السابق أن المتوسط الحسابي لاستجابات أفراد مفردات العينة حول المحور يساوي (4.11)، وهو ما يُصنف ضمن فئة "المرتفع" وفقاً

لمقياس ليكرت الخماسي، كما أظهر التحليل وجود فرق دال إحصائيًا بين المتوسط المحسوب والمتوسط المعتمد في الدراسة، حيث بلغت قيمة الدلالة الإحصائية (0.000) وهي أصغر من مستوى الدلالة المعتمد في الدراسة (0.05)، مما يدعم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على أنه: يوجد دور ذو دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

تتفق هذه النتيجة مع ما توصلت إليه عدة دراسات سابقة أكدت أن إدارة المخاطر تمثل محورًا جوهريًا في فاعلية المراجعة الداخلية الحديثة عند التعامل مع التهديدات المختلفة، ومن بينها التهديدات السيبرانية. فقد أوضحت دراسة الوليد (2017) أن المراجعة الداخلية تسهم في تخفيض المخاطر وتساعد الإدارة في وضع الخطط والسياسات اللازمة لتحديد الاستراتيجية المناسبة لإدارة المخاطر، كما بينت دراسة صالح (2018) وجود علاقة ذات دلالة إحصائية بين الدور الحوكمي للمراجعة الداخلية وإدارة المخاطر، وأكدت أن وجود نظام مراجعة داخلية قوي يساعد المؤسسات على التنبؤ بالمخاطر قبل حدوثها واتخاذ التدابير الوقائية في الوقت المناسب. كذلك تتسجم هذه النتيجة مع دراسة بن عطايف (2021) التي توصلت إلى أن الاتجاهات الحديثة للمراجعة الداخلية تساعد في اختيار الأساليب المناسبة لمواجهة المخاطر المحتملة، ومع دراسة عثمان (2022) التي أكدت أن وظيفة المراجعة الداخلية تؤدي دورًا رئيسيًا في تقييم الاضطرابات السيبرانية وتحسين حوكمة أمن المعلومات وجهود إدارة المخاطر. كما تتوافق هذه النتيجة مع دراسة عمر (2023) التي أثبتت وجود علاقة ارتباط بين إدارة المخاطر وأمن نظم المعلومات المحاسبية، فضلًا عن توافقها مع دراسات أجنبية مثل Jones & Smith (2019) و Hayek & Smith (2020) اللتين أكدت أن جودة المراجعة الداخلية واستخدام الأدوات الحديثة والتقييم المستمر للتهديدات الأمنية تعزز قدرة المؤسسات على الكشف المبكر عن الثغرات وتقليل المخاطر السيبرانية. وبذلك، فإن النتيجة الحالية لا تعكس فقط ارتفاع متوسط استجابات أفراد العينة، بل تؤكد أيضًا انسجامها مع الاتجاه العام في الأدبيات السابقة الذي ينظر إلى إدارة المخاطر باعتبارها أحد الأبعاد الأكثر تأثيرًا في الحد من مخاطر الأمن السيبراني داخل المؤسسات.

الفرضية الفرعية الثانية: يوجد دور ذو دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

لاختبار الفرضية الفرعية الثانية يمكن صياغتها بصورة إحصائية كالتالي:

H_0 : لا يوجد دور ذو دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن

السيبراني بشركات الاتصالات قيد الدراسة.

H_1 : يوجد دور ذو دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن السيبراني

بشركات الاتصالات قيد الدراسة.

ولاختبار الفرضية، استخدم الباحث اختبار T للعينة الواحدة (One Sample T-Test)

وذلك للتحقق من صحة هذه الفرضية، والجدول التالي يبين المتوسط الحسابي والانحراف

المعياري، وكذلك نتائج اختبار T (قيمة الاختبار والدلالة الإحصائية).

جدول رقم (21) اختبار T للمحور الثاني

المتوسط الحسابي	الانحراف المعياري	إحصاء اختبار T	الدلالة الإحصائية	النتيجة
3.94	0.645	11.372	0.000	رفض H_0

أظهرت نتائج اختبار (T) للعينة الواحدة للجدول السابق أن المتوسط الحسابي لاستجابات أفراد مفردات العينة حول المحور يساوي (3.94)، وهو ما يُصنف ضمن فئة "المرتفع" وفقاً لمقياس ليكرت الخماسي، كما أظهر التحليل وجود فرق دال إحصائياً بين المتوسط المحسوب والمتوسط المعتمد في الدراسة، حيث بلغت قيمة الدلالة الإحصائية (0.000) وهي أصغر من مستوى الدلالة المعتمد في الدراسة (0.05)، مما يدعم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على أنه: يوجد دور ذو دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

تتفق هذه النتيجة مع ما توصلت إليه عدد من الدراسات السابقة التي أكدت أن البعد الحوكمي للمراجعة الداخلية يمثل عنصراً مؤثراً في الحد من المخاطر وتعزيز فعالية الرقابة داخل المؤسسة؛ فقد خلصت دراسة صالح (2018) إلى وجود علاقة ذات دلالة إحصائية بين الدور الحوكمي للمراجعة الداخلية وإدارة المخاطر، بما يعني أن تعزيز هذا الدور ينعكس إيجاباً على فعالية التعامل مع المخاطر. كما تتسجم هذه النتيجة مع دراسة عمر (2023) التي أوضحت أن حوكمة الشركات تعزز الشفافية والدقة في المعلومات، وأوصت بتعزيزها بوصفها أحد الاتجاهات الحديثة في المراجعة الداخلية، وهو ما يتوافق مع ما أظهرته الدراسة الحالية من دلالة إحصائية لوجود دور لحوكمة الشركات في الحد من مخاطر الأمن السيبراني. كذلك تتفق النتيجة مع دراسة

عثمان (2022) التي بينت أن وظيفة المراجعة الداخلية تؤدي دورًا رئيسيًا في تحسين وحوكمة أمن المعلومات وجهود إدارة المخاطر السيبرانية، كما تتسق مع دراسة الشيخ وأحمد (2023) التي أثبتت وجود تأثير ذي دلالة إحصائية لتنفيذ عناصر الرقابة الداخلية وفق إطار COSO في تقليل مخاطر المحاسبة السحابية، وأن الأمن السيبراني يعزز فعالية الرقابة الداخلية؛ وهو ما يدعم النتيجة الحالية من زاوية أن الحوكمة والرقابة المؤسسية الرشيدة تسهمان في الحد من المخاطر التقنية. وفي المقابل، تختلف هذه النتيجة جزئيًا مع دراسة الزيود (2021) التي لم تجد أثرًا لحياضية التدقيق الداخلي في الحد من المخاطر السيبرانية، إلا أن هذا الاختلاف لا ينقض النتيجة الحالية، لأن دراسة الزيود تناولت بعدًا جزئيًا محددًا هو الحيادية، بينما تناولت الدراسة الحالية حوكمة الشركات كبعد أشمل يتضمن الشفافية، والاستقلالية، وتحسين الأداء، والالتزام بالجودة؛ ومن ثم فإن النتيجة الحالية تبدو أكثر اتساقًا مع الاتجاه الغالب في الأدبيات الذي يؤكد أن تفعيل الحوكمة داخل بيئة المراجعة الداخلية يعزز قدرة المؤسسات على الحد من مخاطر الأمن السيبراني.

الفرضية الفرعية الثالثة: يوجد دور ذو دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

لاختبار الفرضية الفرعية الثالثة يمكن صياغتها بصورة إحصائية كالتالي:

H_0 : لا يوجد دور ذو دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

H_1 : يوجد دور ذو دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

ولاختبار الفرضية، استخدم الباحث اختبار T للعينة الواحدة (One Sample T-Test) وذلك للتحقق من صحة هذه الفرضية، والجدول التالي يبين المتوسط الحسابي والانحراف المعياري، وكذلك نتائج اختبار T (قيمة الاختبار والدلالة الإحصائية).

جدول رقم (22) اختبار T للمحور الثالث

المتوسط الحسابي	الانحراف المعياري	إحصاء اختبار T	الدلالة الإحصائية	النتيجة
4.00	0.657	11.660	0.000	رفض H_0

أظهرت نتائج اختبار (T) للعينة الواحدة للجدول السابق أن المتوسط الحسابي لاستجابات أفراد مفردات العينة حول المحور يساوي (4.00)، وهو ما يُصنف ضمن فئة "المرتفع" وفقًا لمقياس ليكرت الخماسي، كما أظهر التحليل وجود فرق دال إحصائيًا بين المتوسط المحسوب والمتوسط المعتمد في الدراسة، حيث بلغت قيمة الدلالة الإحصائية (0.000) وهي أصغر من مستوى الدلالة المعتمد في الدراسة (0.05)، مما يدعم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على أنه: يوجد دور ذو دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

تتفق هذه النتيجة مع الاتجاه العام في الدراسات السابقة الذي يؤكد أن إضافة القيمة للمراجعة الداخلية لا تقتصر على الدور الرقابي التقليدي، بل تمتد إلى تقديم تقييمات موضوعية، وخدمات تأكيدية واستشارية، وتوصيات عملية تساهم في الحد من المخاطر السيبرانية. ففي هذا السياق، توصلت دراسة الشيخ (2020) إلى وجود علاقة ذات دلالة إحصائية بين بعد إضافة القيمة وتحسين الأداء، وأوصت بتنفيذ الأنشطة الحديثة للمراجعة الداخلية، ومنها إضافة القيمة الاقتصادية والدور التوكيدي والخدمات الاستشارية، لما لها من دور في مجابهة المخاطر والسلامة المصرفية. كما تتسجم النتيجة الحالية مع دراسة عثمان (2022) التي بينت أن وظيفة المراجعة الداخلية تؤدي دورًا رئيسيًا في مراجعة الأمن السيبراني من خلال توفير دليل مستقل وموضوعي على الالتزام بالسياسات، وتكوين رؤية تساهم في تحسين حوكمة أمن المعلومات وجهود إدارة المخاطر. كذلك تتفق مع دراسة أبو الخير (2023) التي أكدت أن جودة المراجعة الداخلية تساعد المؤسسات المالية على اتخاذ إجراءات وقائية أكثر وضوحًا في مواجهة المخاطر السيبرانية. ويمكن أيضًا الاستئناس بنتائج دراسة صالح علي صالح (2022) التي دعمت أهمية توكيد المراجعة الداخلية على الأمن السيبراني وضرورة وضع إجراءات لقياس فعاليتها، وهو ما يرتبط مباشرة بمفهوم القيمة المضافة للمراجعة من حيث تعزيز الثقة والالتزام وتحسين فعالية الأداء الرقابي. وعلى المستوى الأجنبي، تتوافق هذه النتيجة مع دراستي Jones & Smith (2019) و Hayek & Smith (2020) اللتين أكدتا أن جودة المراجعة الداخلية، واستخدام الأدوات الحديثة، والتقييم المستمر للثغرات والسياسات الأمنية، كلها أمور تعزز قدرة المؤسسة على الكشف المبكر عن التهديدات والحد من المخاطر السيبرانية. وبناءً على ذلك، فإن قبول الفرضية الفرعية الثالثة في الدراسة الحالية يعد نتيجة منطقية ومتسقة مع الأدبيات السابقة،

ويعكس أن إضافة القيمة للمراجعة تمثل بُعدًا فاعلاً من أبعاد الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني.

ثانياً - مناقشة النتائج

أظهرت نتائج الدراسة أن أغلب أفراد العينة كانوا من الفئة العمرية الواقعة بين 25 سنة إلى أقل من 35 سنة، وأن غالبية المبحوثين يحملون درجة البكالوريوس، ويتخصصون في المحاسبة، ويشغلون وظيفة موظف، كما أن جزءاً مهماً منهم تلقى دورات تدريبية في مجال المراجعة الداخلية. ويمكن تفسير ذلك بأن بيئة شركات الاتصالات قيد الدراسة تضم كوادراً وظيفية شابة نسبياً ومؤهلة علمياً، وهو ما يعزز قابلية تبني الممارسات الحديثة في المراجعة الداخلية والتعامل مع متطلبات البيئة الرقمية. ومع ذلك، فإن محدودية الدورات التدريبية لدى بعض أفراد العينة توحى بأن تطوير الكفاءة المهنية في مجال الأمن السيبراني ما زال بحاجة إلى مزيد من الدعم المؤسسي، وهو ما ينسجم مع ما أكدته بعض الدراسات السابقة من أن ضعف الخبرة التقنية وقلة التدريب يمثلان من أهم التحديات التي تعوق فعالية المراجعة الداخلية في مواجهة المخاطر السيبرانية، كما في دراسة الشورة (2020)، ودراسة محمد (2022)، فضلاً عن تأكيد دراسة عثمان (2022) على أهمية تدريب المراجعين الداخليين على التقنيات الحديثة المرتبطة بالأمن السيبراني.

كما بينت نتائج اختبار الفرضية الرئيسية وجود دور ذي دلالة إحصائية للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة، حيث جاءت قيمة مستوى الدلالة الإحصائية أقل من (0.05)، بما يدعم قبول الفرضية الرئيسية، كما جاء مستوى التقدير العام مرتفعاً، الأمر الذي يدل على إدراك أفراد العينة لأهمية التحول في وظيفة المراجعة الداخلية من الدور التقليدي إلى دور أكثر شمولاً يركز على إدارة المخاطر، وتعزيز الحوكمة، وإضافة القيمة. وتعد هذه النتيجة منسجمة مع الاتجاه العام في الدراسات السابقة التي أكدت أن المراجعة الداخلية الحديثة أصبحت أداة فاعلة في تحسين البيئة الرقابية، ودعم الإدارة في مواجهة المخاطر المستجدة، ومن بينها المخاطر السيبرانية. وفي هذا السياق،

أكدت دراسة عثمان (2022) أن وظيفة المراجعة الداخلية تلعب دوراً رئيسياً في تقييم الاضطرابات السيبرانية وتحسين حوكمة أمن المعلومات وجهود إدارة المخاطر، كما أوضحت دراسة أبو الخير (2023) أن جودة المراجعة الداخلية تساعد المؤسسات المالية على اتخاذ إجراءات وقائية واضحة في مواجهة المخاطر السيبرانية، في حين أكدت دراستا Jones & Smith (2019) و Hayek & Smith (2020) أن جودة المراجعة الداخلية واستخدام الأدوات الحديثة يعززان قدرة المؤسسات على الكشف المبكر عن التهديدات والحد من آثارها .

وفيما يتعلق ببعد إدارة المخاطر، فقد دعمت نتائج اختبار الفرضية الفرعية الأولى هذه النتيجة بصورة واضحة، إذ بلغ المتوسط الحسابي لهذا البعد (4.11) بانحراف معياري (0.705)، كما بلغت قيمة اختبار $T = 11.749$ عند مستوى دلالة (Sig = 0.000)، وهي قيمة أقل من مستوى المعنوية المعتمد (0.05)، مما يؤكد قبول الفرضية الفرعية الأولى التي تنص على وجود دور ذي دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني. ويشير ذلك إلى أن أفراد العينة يرون أن التقييم المنهجي للمخاطر، ووضع الاستراتيجيات المناسبة للتعامل معها، وتحسين عمليات التصدي لها، كلها ممارسات تسهم بفاعلية في تخفيض التهديدات السيبرانية داخل شركات الاتصالات. وتتسجم هذه النتيجة مع دراسة الوليد (2017) التي أوضحت أن المراجعة الداخلية تسهم في تخفيض المخاطر وتساعد في وضع الخطط والسياسات المناسبة لإدارتها، كما تتفق مع دراسة صالح (2018) التي أثبتت أن المراجعة الداخلية تدعم الإدارة في اتخاذ القرارات الرشيدة من خلال تقديم معلومات دقيقة وتقييمات موضوعية للمخاطر، فضلاً عن توافقها مع دراسة بن عطاف (2021) التي أكدت أن الاتجاهات الحديثة للمراجعة الداخلية تساعد إدارة المخاطر في تحديد الأساليب المناسبة لمواجهة المخاطر المحتملة. كما تدعم هذه النتيجة دراسة عمر (2023) التي أظهرت وجود علاقة ارتباط بين إدارة المخاطر وأمن نظم المعلومات المحاسبية، ودراسة الكرعوي والعيسوي (2024) التي أكدت أن التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني يسهم في خفض الآثار السلبية للمخاطر .

أما بالنسبة لبعد حوكمة الشركات، فقد أظهرت نتائج اختبار الفرضية الفرعية الثانية وجود دور ذي دلالة إحصائية لهذا البعد في الحد من مخاطر الأمن السيبراني، حيث بلغ المتوسط الحسابي (3.94) والانحراف المعياري (0.645)، كما جاءت قيمة مستوى الدلالة الإحصائية أقل من (0.05)، وهو ما يؤكد قبول الفرضية الفرعية الثانية. ويعني ذلك أن عناصر

الحوكمة، مثل الشفافية، والاستقلالية، وتحسين الأداء، والالتزام بالجودة، تمثل من وجهة نظر الباحثين أدوات أساسية في دعم المراجعة الداخلية وتقوية قدرتها على مواجهة المخاطر السيبرانية. وتتفق هذه النتيجة مع دراسة صالح (2018) التي توصلت إلى وجود علاقة ذات دلالة إحصائية بين الدور الحوكمي للمراجعة الداخلية وإدارة المخاطر، كما تتسجم مع دراسة عمر (2023) التي بينت أن حوكمة الشركات تعزز الشفافية والدقة، وأوصت بتعزيزها كأحد الاتجاهات الحديثة في المراجعة الداخلية. كذلك تتفق مع دراسة عثمان (2022) التي أشارت إلى أن المراجعة الداخلية تسهم في تحسين وحوكمة أمن المعلومات، ومع دراسة الشيخ وأحمد (2023) التي أثبتت أن تفعيل عناصر الرقابة الداخلية وفق إطار COSO يسهم في تقليل المخاطر التقنية ويعزز فعالية الأمن السيبراني. وفي المقابل، تختلف هذه النتيجة جزئياً مع دراسة الزيود (2021) التي لم تجد أثراً لحياضية التدقيق الداخلي في الحد من المخاطر السيبرانية، إلا أن هذا الاختلاف يظل محدوداً؛ لأن الدراسة الحالية تناولت حوكمة الشركات كبعد أشمل يتضمن أكثر من عنصر، وليس الحيادية فقط.

وفيما يخص بعد إضافة قيمة للمراجعة، فقد أثبتت نتائج اختبار الفرضية الفرعية الثالثة وجود دور ذي دلالة إحصائية لهذا البعد في الحد من مخاطر الأمن السيبراني، إذ بلغ المتوسط الحسابي (4.00) والانحراف المعياري (0.657)، كما بلغت قيمة اختبار $T = 11.660$ عند مستوى دلالة (Sig = 0.000)، وهي أقل من (0.05)، الأمر الذي يؤكد قبول الفرضية الفرعية الثالثة. ويعكس ذلك إدراك أفراد العينة لأهمية القيمة المضافة التي تحققها المراجعة الداخلية من خلال التقييم المستقل والموضوعي، وتقديم التوصيات، ودعم الشفافية، وتعزيز الالتزام والرقابة. وتتفق هذه النتيجة مع دراسة الشيخ (2020) التي توصلت إلى وجود علاقة ذات دلالة إحصائية بين بعد إضافة القيمة وتحسين الأداء، وأوصت بتفعيل الأنشطة الحديثة للمراجعة الداخلية، ومنها إضافة القيمة الاقتصادية والدور التوكيدي والخدمات الاستشارية. كما تتسجم مع دراسة عثمان (2022) التي أكدت أن المراجعة الداخلية توفر دليلاً مستقلاً وموضوعياً على الالتزام بسياسات الأمن السيبراني، وهو ما يمثل جوهر القيمة المضافة للمراجعة. وتؤيد هذه النتيجة أيضاً دراسة أبو الخير (2023) التي بينت أن جودة المراجعة الداخلية تسهم في اتخاذ إجراءات وقائية واضحة في مواجهة المخاطر السيبرانية، ودراسة صالح علي صالح (2022) التي دعمت أهمية توكيد المراجعة الداخلية على الأمن السيبراني ووضع إجراءات لقياس فعاليتها. كما تتفق مع بعض الأدبيات الأجنبية، ولا سيما دراستي Jones & Smith (2019) و Hayek & Smith

(2020)، اللتين أكدتا أن جودة المراجعة الداخلية والتقييم المستمر للثغرات والسياسات الأمنية يعززان قدرة المؤسسة على الحد من التهديدات السيبرانية .

وبوجه عام، تكشف مناقشة النتائج أن الدراسة الحالية جاءت متفقة في معظمها مع الاتجاه السائد في الدراسات السابقة، والذي يؤكد أن فعالية المراجعة الداخلية في البيئة الرقمية لم تعد تقاس فقط بمدى تنفيذها للإجراءات التقليدية، بل بقدرتها على إدارة المخاطر، وتفعيل الحوكمة، وإضافة القيمة في مواجهة التهديدات السيبرانية. كما توضح النتائج أن بيئة شركات الاتصالات الليبية، بحكم طبيعتها التقنية واعتمادها المرتفع على نظم المعلومات، تجعل الحاجة إلى هذه الأبعاد أكثر إلحاحًا من غيرها، وهو ما يفسر ارتفاع مستوى الموافقة على جميع أبعاد المتغير الرئيس. وعليه، فإن الدراسة الحالية تضيف دعمًا ميدانيًا لفكرة أن تبني الاتجاهات الحديثة للمراجعة الداخلية يمثل مدخلًا عمليًا مهمًا لتعزيز قدرة المؤسسات على مواجهة المخاطر السيبرانية والحد من آثارها .

المبحث الثالث:

النتائج والتوصيات

أولاً- النتائج

توصلت الدراسة اعتماداً على تحليل البيانات الأولية لها إلى جملة من النتائج أهمها ما يلي:

1. يوجد دور للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني وبمستوى مرتفع بشركات الاتصالات بمدينة طرابلس.

وذلك من خلال:

أ. يوجد دور ذو دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني بشركات

الاتصالات قيد الدراسة.

ب. يوجد دور ذو دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة..

ت. يوجد دور ذو دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني بشركات الاتصالات قيد الدراسة.

ثانياً: التوصيات

في ضوء النتائج التي توصلت إليها الدراسة، توصي الباحثة بما يلي:

1. نظرًا لأن أغلب العاملين بشركات الاتصالات قيد الدراسة من الفئة العمرية الشابة، ويحملون مؤهل البكالوريوس، ولديهم خبرة متوسطة، مع حصولهم على عدد محدود من الدورات التدريبية في المراجعة الداخلية، فإن الدراسة توصي بزيادة الاهتمام بالبرامج التدريبية المتخصصة في المراجعة الداخلية والأمن السيبراني، بما يسهم في تطوير كفاءة العاملين ورفع جاهزيتهم لمواكبة التهديدات السيبرانية الحديثة .
2. في ضوء ما أظهرته النتائج من وجود دور مرتفع للاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني، توصي الدراسة بضرورة تبني شركات الاتصالات لهذه الاتجاهات بصورة أكثر تنظيمًا ووضوحًا، والعمل على إدماجها ضمن سياساتها الرقابية والإدارية بما يعزز قدرتها على مواجهة المخاطر السيبرانية .
3. واستنادًا إلى النتيجة التي أكدت وجود دور ذي دلالة إحصائية لإدارة المخاطر في الحد من مخاطر الأمن السيبراني، توصي الدراسة بضرورة تطوير آليات فعالة لإدارة المخاطر داخل شركات الاتصالات، تقوم على التحديد المبكر للمخاطر السيبرانية، وتحليلها، وتقييمها، ووضع الخطط المناسبة للتعامل معها بصورة مستمرة .
4. وبناءً على ما توصلت إليه الدراسة من وجود دور ذي دلالة إحصائية لحوكمة الشركات في الحد من مخاطر الأمن السيبراني، توصي الدراسة بتعزيز مبادئ الحوكمة داخل شركات الاتصالات، من خلال دعم الشفافية، وتحديد المسؤوليات، وتقوية الرقابة الداخلية، وتفعيل دور لجان المراجعة بما يسهم في تحسين القدرة على الحد من المخاطر السيبرانية .
5. وفي ضوء النتيجة التي أثبتت وجود دور ذي دلالة إحصائية لإضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني، توصي الدراسة بتمكين إدارات المراجعة الداخلية من أداء دورها التقييمي والاستشاري بصورة أكثر فاعلية، والاستفادة من تقاريرها وتوصياتها في تحسين نظم الرقابة الداخلية وتطوير الإجراءات الوقائية المتعلقة بالأمن السيبراني.

مقترحات دراسات مستقبلية:

1. أثر التدريب المتخصص للمراجعين الداخليين في رفع كفاءة الحد من مخاطر الأمن السيبراني .
2. دور المراجعة الداخلية القائمة على إدارة المخاطر في تعزيز أمن المعلومات بالمؤسسات اللببية .
3. أثر استقلالية المراجعة الداخلية في تحسين الاستجابة للمخاطر السيبرانية .
4. دور إضافة القيمة في المراجعة الداخلية في دعم الأمن السيبراني بشركات الاتصالات .
5. العلاقة بين حوكمة الشركات وفعالية المراجعة الداخلية في الحد من مخاطر الأمن السيبراني.

قائمة المصادر والمراجع

أولاً: الكتب العربية

1. الخطيب، سمير. (2005). قياس أثر المخاطر في البنوك. الإسكندرية: منشأة المعارف للنشر والتوزيع .
 2. نصار، حمدي جابر. (2007). إدارة المخاطر في ظل تكنولوجيا المعلومات .د.م: دن .
 3. علي، عبد الوهاب نصر. (2009). المراجعة وحوكمة الشركات ومسؤوليات مراقب الحسابات في مواجهة الأزمة المالية العالمية. في: موسوعة المراجعة الخارجية الحديثة وفقاً لمعايير المراجعة العربية والدولية والأمريكية. الإسكندرية: الدار الجامعية .
 4. عريقات، حربي محمد، وعقل، سعيد جمعة. (2010). التأمين وإدارة الخطر: النظرية والتطبيق (ط2). الأردن: دار الأوائل للنشر إيكن، ماري. (2018). التأثير السيبراني: كيف يغير الإنترنت سلوك البشر. بيروت، لبنان: الدار العربية للعلوم ناشرون .
 5. الجمال، جيهان عبد المعز. (2014). المراجعة الداخلية وحوكمة الشركات. بيروت: دار الكتاب الجامعي .
 6. نور الدين، أحمد قايد. (2015). التدقيق المحاسبي وفقاً للمعايير الدولية (ط1). الأردن: دار الجنان للنشر والتوزيع .
 7. عبد الصادق، عادل. (2016). الإرهاب الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق. القاهرة: المكتبة الأكاديمية البعلبكي، منير. (2017). المورد عربي: قاموس إنكليزي. بيروت، لبنان: دار العلم للملايين .
 8. الوردات، خلف عبد الله. (2017). دليل التدقيق الداخلي وفق المعايير الدولية الصادرة عن IIA (ط1). الأردن: مؤسسة الوراق للنشر والتوزيع.
 9. السالم، رائد أحمد. (2020). تحليل المخاطر وإدارة الأزمات. مصر: دار الفجر للنشر .
 10. دروزة، عبد الرحمن. (2021). إدارة المخاطر السيبرانية. الأردن: دار وائل للنشر .
- ثانياً: الرسائل العلمية (ماجستير ودكتوراه)
1. بوقرة، رابح، وغانم، هاجر. (2012). الحوكمة: المفهوم والأهمية. رسالة ماجستير في المحاسبة، كلية العلوم الاقتصادية والتجارية، جامعة محمد خيضر، بسكرة، الجزائر .

2. سالم، إياد حسن. (2012). واقع التدقيق الداخلي في بلديات قطاع غزة: دراسة ميدانية . رسالة ماجستير غير منشورة، كلية التجارة، الجامعة الإسلامية، غزة، فلسطين .
3. النجار، دعاء محمد حامد. (2013). إطار مقترح لتحقيق التكامل بين المراجعة الداخلية على أساس الخطر وأدوات إدارة التكلفة لدعم عملية اتخاذ القرارات الاستراتيجية .رسالة دكتوراه، كلية التجارة، جامعة طنطا، مصر .
4. الشوا، ورود ناهض. (2014). دور المدقق الداخلي في إدارة المخاطر في بيئة العمل من وجهة نظر موظفي مجمع الإيرادات في وزارة المالية بقطاع غزة .رسالة ماجستير غير منشورة، كلية التجارة، الجامعة الإسلامية، غزة، فلسطين .
5. محمد، الوليد الطيب إبراهيم. (2017). الاتجاهات الحديثة للمراجعة الداخلية ودورها في زيادة كفاءة نظام الرقابة الداخلية: دراسة ميدانية على مصرف الادخار والتنمية الاجتماعية . رسالة ماجستير منشورة، جامعة النيلين، السودان .
6. داما، صالح عبد الله أمين. (2018). الاتجاهات الحديثة للمراجعة الداخلية ودورها في إدارة المخاطر: دراسة ميدانية على بنك فيصل الإسلامي السوداني .رسالة ماجستير منشورة، جامعة النيلين، الخرطوم، السودان .
7. إفريج، حنين محرز رمضان. (2019). أثر نظام المعلومات المحاسبية في الحد من مخاطر السيولة في المصارف السعودية .رسالة ماجستير، كلية الاقتصاد، جامعة الزرقاء، الأردن .
8. محمد علي، نون جهاد عطية الله. (2019). الاتجاهات الحديثة للمراجعة الداخلية ودورها في دعم الميزة التنافسية: دراسة ميدانية على عينة من المصارف السودانية .رسالة ماجستير منشورة، جامعة السودان للعلوم والتكنولوجيا، السودان
9. الشورة، إيمان محمد. (2020). الأمن السيبراني في البنوك الإسلامية الأردنية .كلية الأعمال، الجامعة الأردنية، عمان، الأردن .
10. الشيخ، مصطفى محمد أحمد. (2020). الأنشطة الحديثة للمراجعة الداخلية ودورها في تحسين كفاءة الأداء المالي وترشيد القرارات .دراسة دكتوراه منشورة، جامعة النيلين، السودان .
11. الزيود، محمود سليمان سعود. (2021). أثر التدقيق الداخلي في الحد من مخاطر السيبرانية في البنوك التجارية الأردنية .رسالة ماجستير غير منشورة، جامعة آل البيت، المفرق، الأردن .

12. عبد المغيث، سناء كامل علي محمد. (2022). محددات جودة المراجعة الداخلية ودورها في تقييم إدارة المخاطر بالوحدات الحكومية بالسودان: دراسة ميدانية على وزارة المالية والتخطيط الاقتصادي. رسالة دكتوراه منشورة، جامعة السودان للعلوم والتكنولوجيا، السودان .
13. زراق، عبير. (2024). دور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي: دراسة ميدانية على الجهاز المركزي للرقابة المالية، فرع حلب، الجمهورية العربية السورية .د.ن .
14. موسى، رامي صلاح أبو زيد. (2025). دور جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني. رسالة ماجستير منشورة، كلية التجارة، جامعة طنطا، متاحة عبر دار المنظومة .

ثالثاً: المجلات والدوريات والمؤتمرات

1. أحمد، خالد محمد عثمان. (2023). أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي: دراسة تطبيقية . مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، العدد الرابع .
2. أميرهم، جيهان عادل. (2022). أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على قرارات المستثمرين: دراسة ميدانية مجلة البحوث المالية والتجارية، كلية التجارة، جامعة بورسعيد، العدد الثالث، يوليو .
3. باعجاجة، سالم سعيد. (2013). مدى إضافة المراجعة الداخلية قيمة للمنشأة: دراسة ميدانية على قطاع صناعة الكهرباء .المجلة العلمية للبحوث والدراسات التجارية، جامعة حلوان، كلية التجارة، العدد (3).
4. بانقا، علم الدين. (2019). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دولة مجلس التعاون الخليجي سلسلة دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد (63).
5. البغادي، مروة فتحي السيد. (2021). اقتصاديات الأمن السيبراني في القطاع المصرفي . مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة .

6. بدوى، هبة الله عبد السلام. (2021). أثر جودة مستوى التوكيد على برنامج إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين. *مجلة الإسكندرية للبحوث التجارية*، كلية التجارة، جامعة الإسكندرية، المجلد 5، العدد 3.
7. بن عطف، ولاء فريد حسين. (2021). دور الاتجاهات الحديثة في المراجعة الداخلية وأساليب إدارة المخاطر في البنوك الإسلامية. *المجلة العربية للنشر*، العدد 37.
8. الجرعاني، أبرار بنت عبد الغني بن جبر. (2015). دور المراجعة الداخلية في تفعيل الدور الرقابي في البنوك السعودية: دراسة ميدانية. *مجلة البحوث التجارية*، كلية التجارة، جامعة عين شمس، المجلد 19، العدد 3.
9. حسين، أسعد مبارك، وآخرون. (2016). دور المراجعة الداخلية في تقييم الأداء المالي بالجامعات الحكومية بولاية البحر الأحمر. *مجلة العلوم الاقتصادية*، عمادة البحث العلمي، جامعة السودان للعلوم والتكنولوجيا، الخرطوم، المجلد 17، العدد 1.
10. الخرينج، نواف متعب بنية متعب، والبسطويسى، مروة أحمد عبد الرحمن، ومحمد، ياسر إبراهيم. (2022). دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، المجلد 13.
11. خليل، محمد أحمد إبراهيم. (2011). تطوير دور المراجعة الداخلية كنشاط مضيف للقيمة للحد من آثار المخاطر والأزمات المالية على منظمات الأعمال المصرية في ضوء حوكمة الشركات: دراسة نظرية ميدانية. *مجلة الدراسات والبحوث التجارية*، كلية التجارة، جامعة بنها، المجلد 2، العدد 1.
12. أبو راوي، أسامة علي ميلاد. (2011). دور المراجعة الداخلية في تدعيم حوكمة الشركات. *المجلة العلمية للبحوث والدراسات التجارية*، كلية التجارة، جامعة عين شمس، المجلد 2، العدد 4.
13. راغب، رجب التركاوي. (2019). أثر الخصائص النوعية للمعلومات المحاسبية على فاعلية إدارة مخاطر السيولة المصرفية: دراسة ميدانية على المصارف التجارية الليبية. *مجلة البحوث المالية والاقتصادية*، جامعة بنغازي.

14. زراق، عبير. (2024). دور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي: دراسة ميدانية على الجهاز المركزي للرقابة المالية، فرع حلب، الجمهورية العربية السورية. د.ن .
15. أبو زيد، خالد عبد الشافي، وأبو زقية، عبد الناصر محمد. (2024). دور المراجعة الداخلية في إدارة المخاطر بالمصارف التجارية العاملة في ليبيا. *مجلة دراسات الأعمال والاقتصاد*، المجلد 11، العدد 1 .
16. السمحان، منى. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود *مجلة كلية التربية، جامعة المنصورة*، العدد. (111)
17. سمرة، ياسر محمد السيد. (2011). إطار مقترح لرفع مستوى أداء المراجعة الداخلية لمراجعة إدارة مخاطر الأعمال في الشركات المصرية. *المجلة المصرية للدراسات التجارية*، كلية التجارة، جامعة المنصورة، العدد 3 .
18. سيد، ميرفت محمد أحمد. (2012). تقويم أداء وظيفة المراجعة الداخلية بالوحدات الحكومية في جمهورية مصر العربية: دراسة ميدانية. *المجلة العلمية للبحوث والدراسات التجارية*، كلية التجارة، جامعة حلوان، المجلد 2، العدد 4 .
19. شاهنده عادل غريب محمود. (2013). تفعيل مدخل المراجعة المبنية على المخاطر كأداة لتحقيق موضوعية الحكم المهني لمراقب الحسابات عن التقديرات المحاسبية. *مجلة الفكر المحاسبي*، كلية التجارة، جامعة عين شمس، العدد 4 .
20. شحاتة، السيد شحات. (2020). إطار مقترح لإسناد وظيفة المراجعة الداخلية بدورها الاستشاري والتوكيدي في مجال إدارة المخاطر في الوحدات الصغيرة ومتوسطة الحجم . *المجلة العلمية للتجارة والتمويل*، كلية التجارة، جامعة طنطا .
21. شحاتة، السيد شحاتة. (2022). نحو دور فاعل للمراجع في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، كلية التجارة، مدينة السادات، المجلد 13، العدد الثاني، مارس .
22. الشيخ، وأحمد. (2023). أثر إطار عمل (COSO) للرقابة الداخلية في الحد من مخاطر المحاسبة السحابية: الدور الوسيط للأمن السيبراني في البنوك التجارية الأردنية. *مجلة جدار للدراسات والبحوث*، عمان .

23. شيماء هشام عبد اللطيف خميس. (2012). نظرة تحليلية في المراجعة الداخلية المبنية على المخاطر لدعم الاستمرارية مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، العدد 1 .
24. صالح علي صالح، وعلي، محمد أحمد أحمد. (2022). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرارات الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية. في: المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، كلية التجارة، جامعة الإسكندرية .
25. صالح، نرمين محمد شاكر إبراهيم. (2022). محددات فعالية المراجع الداخلي للأمن السيبراني. في: المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، كلية التجارة، جامعة الإسكندرية .
26. عبد السيد، ناظم حسن. (2012). أثر حوكمة المصارف على جودة المعلومات المحاسبية مجلة المثنى للعلوم الإدارية والاقتصادية، كلية الإدارة والاقتصاد، جامعة المثنى، بغداد، المجلد 2، العدد 4 .
27. العتيبي، خالد. (2022). دور المراجعة الداخلية في تقليل مخاطر الاحتيال المالي في المؤسسات المالية العربية مجلة الدراسات الاقتصادية والإدارية، الجامعة العراقية، العدد 5 .
28. عثمان، محمد أحمد. (2022). محددات فعالية وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني. في: المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين، كلية التجارة، جامعة الإسكندرية .
29. عمر، النور كريم عمر. (2023). دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر أمن المعلومات المحاسبية. المجلة الدولية للنشر في الأبحاث والدراسات، الخرطوم .
30. فريد، حنان هارون. (2022). الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية: دراسة تجريبية. المجلة العلمية

للدراستات التجارية والبيئية، كلية التجارة بالإسماعيلية، جامعة قناة السويس، المجلد 13، العدد 4 .

31. فضل الله، عماد عبد الله، والعريبي، نبيل امجيجيد الشريف. (2024). الاتجاهات الحديثة للمراجعة الداخلية ودورها في دعم الميزة التنافسية بالمصارف التجارية: دراسة استطلاعية على المصارف التجارية مجلة جامعة الزيتونة الدولية، العدد 19 .

32. الكرعائي، والعيساوي. (2024). دور التدقيق الداخلي القائم على إدارة مخاطر الأمن السيبراني وانعكاسه في خفض كلفة التأمين مجلة الغري للعلوم الاقتصادية والإدارية، السودان .

33. محمد عبد الفتاح محمد عبد الفتاح. (2008). إطار مقترح لتطوير دور المراجعة الداخلية في تفعيل إدارة المخاطر المصرفية مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، العدد 2 .

34. محمد عبد الفتاح، محمد عبد الفتاح. (2012). إطار مقترح لتطوير دور المراجعة الداخلية في تفعيل إدارة المخاطر المصرفية مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، العدد 2 .

35. محمد، سالم مفتاح. (2022). التحديات التي تواجه المراجعين الداخليين في مواجهة المخاطر السيبرانية في المصارف الليبية مجلة المحاسبة والإدارة المالية، العدد 9 .

36. محمد، طارق محمد. (2015). أثر ممارسة حوكمة الشركات على شفافية القوائم المالية . مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، القاهرة، الجزء 1 .

37. هيكل، فوزي محمد. (2012). إطار مقترح لتطوير وظيفة المراجعة الداخلية بهدف ترشيد مستوى الإفصاح الاختياري في شركات المساهمة مجلة المحاسبة المصرية، العدد 3 .

38. الوكيل، حسام السعيد السيد محمد. (2011). نموذج مقترح لقياس أثر المراجعة الداخلية على إضافة قيمة للمنشأة مجلة كلية التجارة وإدارة الأعمال، جامعة حلوان .

39. وهدان، محمد علي. (2022). دور المراجعة الداخلية في تحقيق الإصلاح الحكومي: رؤية تحليلية مستقبلية. المجلة العلمية للبحوث التجارية، العدد الثالث .

40. ياسر صلاح أحمد محمد. (2016). أثر المراجعة الداخلية بحسب المخاطر في تحسين الأداء المالي في المنشآت العامة. *مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، المجلد 1، العدد 1*.

41. يعقوب، ابتهاج إسماعيل، وهاب، أسعد محمد علي، والفرطوسي، علي سموم. (2022). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية. *مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 9، العدد 1*.

رابعاً: المراجع الأجنبية (Foreign References)

1. Abdul Malik, Salau Olarinoye, Che-Ahmad, Ayoib, and Usman, Alih (2023): The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: A Conceptual Review.
2. Alina , C. M., Cerasela S.E., and Gabriela G, (2017) ,Internal audit role in cybersecurity ovidius university Annals Economic Sciences Series 17 (2).
3. Alina , C. M., Cerasela S.E., and Gabriela G, (2017) ,Internal audit role in cybersecurityovidius university Annals Economic Sciences Series 17 (2).
4. Al-Moshaigeh, A., Dickins, D. and Higgs, J. (2019) , Cybersecurity Risks and Con-trols: Is the AICPA's SOC for Cybersecurity a Solution?, The CPA Journal, Vol. 89, Issue 6.
5. Badawy, H., (2021) , The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study, Alexandria Journal of Accounting Research, 3 (5).
6. Betti N., Sarens G., and Poncin, (2021) ,Effects of digitalisation of organisations on internal audit activities and practices Managerial auditing Journal Vol 36, No 6.
7. Committee of sponsoring organizations of the treadway commission (COSO), (2019) ,Enterprise wide management (ERM) for Cybersecurity available at <http://www.coso.org/documents/COSO-Deloitte-Managing-Cyber-Risk-ina-Digital-Age.pdf>.

8. David Marqués, Sofia Félix, Georgina Morais (2023): Risk management, cybersecurity and internal audit in municipalities. 2023 18th Iberian Conference on Information Systems and Technologies (CISTI).
9. Deloitte, Development LLC, (2017), Cyber security and role of internal audit an urgent call to action, available at www2.deloitte.com.
10. Ege M., (2015) ,Does internal audit function quality deter management misconduct ? the accounting review Vol., 90 No., 2.
11. Eling M. and J.H. wirfs , (2016), Cyber Risk : too big to insure ? Risk transfer options for a mercurial risk class institute of Insurance Economics University of St. Gallen.
12. Florakis C.C. Louca, R. Michaely and M Weber, (2020) ,Cybersecurity Risk, Available at <http://ssrn.com>.
13. Frank, M., Grenier, J. and Pyzoha, J., (2019) , How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance, Journal of Information Systems, 33 (3).
14. Gay, Grant E. Auditing& assurance : services in Australia ,National Library of Australia Cataloguing – in – publication Data .2020.
15. Hartmann C.C and J. Carmen ate ,(2021) ,Academic Research on the role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches, American Accounting Association, 15.
16. homas G. Calderon Lei Gao, (2020), "Cyber Security Risks Disclosure and Implied Audit Risks: Evidence from Audit Fees", International Journal of Auditing, Vol.25, Issue 1.
17. International Accreditation Forum (IAF), (2021) , Available at: <https://iaf.nu/en/home/>.
18. International Accreditation Forum (IAF), (2021) , Available at: <https://iaf.nu/en/home>.
19. ISACA, (2019) ,auditors have a role in cyber resilience ISACA JOURNAL VOL 6 available at www.isaca.org.
20. Islam M.S, Nusrat, Farah, Thomas F. and Stafford., (2018) ,Factors associated with security / cyber security audit by internal audit function an international study Managerial auditing journal, available at :10.1108/MAJ-07/2017-1595.
21. Jim Peterson , (2022), "The Future of External Audit: Issues and Questions", International Journal of Auditing, Vol.26, Issue 1, Jan.

- 22.Kahyaoglu S.B and K. Caliyurt, (2018): Cyber security assurance process from the internal audit perspective managerial audit J. 33 (4) available at <http://doi.org/10.1108/MAJ02-2018-1804>.
- 23.Kamiya, S., Kang, J., Kim, J., and Stulz, R., (2021), Risk management, firm reputation, and the impact of successful cyberattacks on target firms, Journal of Financial Economics.
- 24.Kelton, A. and Pennington, R., (2020) , Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect?, Journal of Information Systems, 34 (3).
- 25.Kelton, A. and Pennington, R., (2020): Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect? Journal of Information Systems, 34 (3).
- 26.Li H. W.G.No and T. Wang , (2018) ,SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors International Journal of Accounting Information Systems, 30.
- 27.Lunati, Mia (2023): The Transformative Integration of Artificial Intelligence with CMMC and NIST 800-171 for Advanced Risk Management and Compliance.
- 28.Moreira, Gonalo Peres (2019): Cybersecurity and external audit: the disclosure of risk factors in annual reports.
- 29.nstitute of internal auditors (IIA), (2016) ,assessing cybersecurity Risk Roles of the three lines of Defense available at : guidance@theiia.org.
- 30.nstitute of internal auditors (IIA), (2017) ,international standards for the professional practice of internal auditing institute of internal auditors (IIA) report available at : guidance@theiia.org.
- 31.nstitute of internal auditors (IIA), (2020) ,North american pulse of internal audit available at <http://theiia.mkt5790.com/2020-pulse-of-internal-audit>.
- 32.nstitute of internal auditors (IIA), (2020) ,North american pulse of internal audit available at <http://theiia.mkt5790.com/2020> pulse-of-internal-audi.
- 33.Owolabi Sunday Alao, Adesanmi Timilehin (2021): Risk Assessment and Auditors' Responsibilities: An Assessment of COVID-19 Era. The International Journal of Business & Management.
- 34.Prigerson Carolyn, Gene Rainey, Aba Elene, 2021, Issues on Timelines And Reliability Of corporate Financial Statement And The Expertise

- Of Audit Committee Information Technology, Review Of Business Accounting & Finance (RBAF), v,1,n,5.
35. Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-Security Incidents And Audit Quality. European Accounting Review, 31(3).
 36. Sekaran, Uma, (2003), Research Methods For Business, John Wiley & Sons.
 37. Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. Journal of Management and Governance, 27(4).
 38. Sons & Sekaran, Uma, (2003), Research Methods For Business, John Wiley.
 39. The Institute of Internal Auditors (IIA) (2020). Op.Cite
 40. Tuson, O., (2021), Cyber-attacks and stock market activity, International Review of Financial Analysis.
 41. Vuko Tina, Sergeja Slapničar, Marko Čular, Matej Drašček, (2021), key drivers of cyber security audit effectiveness the neo- institutional perspective, available at <http://ssrn.com/abstract=3932177> .
 42. Vuko Tina, Sergeja Slapničar, Marko Čular, Matej Drašček, (2021): key drivers of cyber security audit effectiveness the neoinstitutional perspective, available at. <http://ssrn.com/abstract=3932177>.
 43. Yang, L., Lau, L. and Jan, H. (2020) . Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, Vol. 28 No. 1.

خامساً: مواقع الإنترنت (Websites)

1. أبو شامة، قصي (12 ديسمبر 2021) <https://isf.gov.lb>
2. <https://ab7as.net>
3. <https://fastercapital.com>
4. <https://gov.com>
5. <https://mawdoo3.com>
6. <https://www.arageek.com>
7. www.imd.org

الملاحق

ملحق (1) قائمة المحكمين

ملحق (2) استمارة الاستبيان الموزعة على الموظفين

ملحق (3) ملخص الرسالة باللغة الإنجليزية

ملحق (1) قائمة المحكمين

ت	اسم المحكم	الدرجة العلمية	الجامعة
1	د. عبد الفتاح المرخي	أستاذ مساعد	كلية الاقتصاد/الزاوية
2	د. يوسف شعبان	أستاذ مشارك	كلية الاقتصاد/الزاوية
3	د. سالم عمارة	أستاذ مشارك	الأكاديمية الليبية /الساحل الغربي
4	د. محمد الطيب الشريف	أستاذ مشارك	الاقتصاد / صبراتة
5	د. مصطفى ساسي فتوحه	أستاذ	الاقتصاد/ صبراتة
6	د. عيسى الغنودي	أستاذ مشارك	الأكاديمية الليبية / الساحل الغربي

ملحق (2) الاستبانة في صورتها النهائية



إدارة الدراسات العليا والتدريب

كلية الاقتصاد - قسم المحاسبة

أخي المستجيب،،،،، أختي المستجيبة

السلام عليكم ورحمة الله وبركاته،،،

يقوم الباحث بإجراء دراسة بعنوان: " دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية "، وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في المحاسبة. وتعد خبرتكم المهنية في مجال المراجعة وموقعكم الوظيفي المتعلق بموضوع الدراسة، فإن الباحث يأمل منكم المشاركة الفاعلة والبناءة في إتمام هذه الدراسة، وذلك من خلال الاطلاع على فقرات هذه الاستبانة والإجابة على أسئلتها بموضوعية ومهنية، علماً بأن المعلومات التي سيتحصل عليها الباحث ستعامل بسرية تامة ولن تستخدم إلا لأغراض البحث العلمي فقط.

ولكم مني فائق الاحترام والتقدير،،،

الباحث: محمد أحمد عبد الحفيظ النايض

أولاً: البيانات الأولية

1. المؤهل العلمي: أ. دبلوم متوسط () ب. دبلوم عالي () ج. بكالوريوس () د. ماجستير () هـ. دكتوراه () و. أخرى () تذكر.....
2. التخصص العلمي: أ. محاسبة () ب. إدارة أعمال () ج. اقتصاد () د. حاسوب () أخرى () تذكر.....
3. عدد سنوات الخبرة: أ. من 5 إلى أقل من 10 سنوات () ب. من 10 إلى أقل من 20 سنة () ج. من 20 سنة فأكثر () .
4. المركز الوظيفي: أ. مدير إدارة () ب. رئيس قسم () ج. موظف ()
5. عدد الدورات التدريبية التي حصلت عليها : أ. دورة واحدة () ب. دورتين () ج. ثلاث دورات فأكثر () .
6. إذا حصلت على دورات تدريبية فما هي : أ دورة في تقنية المعلومات () ب. دورة في المراجعة الداخلية () ج. أخرى () تذكر.....

ثانياً: محاور الاستبانة

الرجاء التكرم بوضع علامة (√) أمام مستوى الموافقة المناسب:

المحور الأول: التعرف على مدى تأثير إدارة المخاطر على الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية.

الرقم	العبارات	أوافق بشدة	أوافق	أوافق إلى حد ما	لا أوافق	لا بشدة
تسهم إدارة المخاطر في الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية من خلال:						
1	تقييم المخاطر وتطوير استراتيجيات لإدارتها					
2	تعزيز كفاءة أساليب الرقابة لتفادي المخاطر					
3	تطوير عمليات التصدي للمخاطر داخل الشركة					
4	قياس وتحليل المخاطر المكتشفة وفهم طبيعتها					
5	تحليل العلاقات بين المخاطر لتقييم تأثيرها على بعضها البعض					
6	إعداد تقارير شاملة عن المخاطر وتقديمها لمجلس الإدارة					
7	تحسين عملية صناعة القرار، التخطيط، والأولويات					
8	تقييم تنفيذ تقنيات معالجة الخطر					

المحور الثاني: معرفة كيف تعمل حوكمة الشركات على الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية.

الرقم	العبارات	أوافق بشدة	أوافق	أوافق إلى حد ما	لا أوافق	لا بشدة
تعمل حوكمة الشركات في الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية من خلال:						
1	توجيه أعمال الشركة ومراقبتها على أعلى مستوى					
2	الحفاظ على حقوق أصحاب المصالح والشفافية					
3	يتمتع المراجع الداخلي بالاستقلالية الكاملة في أداء واجباته داخل الشركة					
4	يتمتع المراجع بمعرفة كافية بطبيعة أعمال الشركة ونشاطاتها التشغيلية					
5	يقوم المراجع بتقييم شامل للعمليات ويقدم توصيات فعالة لتحسينها					
6	مكافحة الفساد الإداري					
7	يقدم المراجع توصيات جوهرية لتحسين العمليات وتقليل المخاطر					
8	تحسين مستوى الأداء					
9	يراقب المراجع التزام كافة إدارات الشركة بمقومات الجودة					

المحور الثالث: التعرف مدى إضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية.

الرقم	العبارات	أوافق بشدة	أوافق	أوافق إلى حد ما	لا أوافق	لا بشدة
إن إضافة قيمة للمراجعة في الحد من مخاطر الأمن السيبراني في شركات الاتصالات الليبية من خلال:						
1	تقديم تقييم مستقل وموضوعي لفعالية إجراءات الرقابة					
2	تطوير مبادئ إدارة الشركة بطريقة شاملة وشفافة					
3	القدرة على تحقيق قيم إضافية للمساهمين					
4	توفير معلومات موثوقة وشفافة حول مخاطر الشركة					
5	إرساء قواعد الشفافية لحماية مصالح جميع الأطراف المعنية					
6	تنفيذ سياسات لمنع وتقييد الممارسات التي تعرقل الحوكمة					
7	مناقشة المشاكل الناتجة عن وجودها في الشركة بشكل فوري وفعال					
8	ضمانة الحماية الكاملة للأصول والتشريعات					
9	ضمان الالتزام بالقوانين					