المجلة الأردنية في إدارة الأعمال، المجلّد **21**، العدد **1**، **2025**
DOI: https://doi.org/10.35516/jjba.v21i1.270

The Mediating Role of Security Controls between Information-technology Risks and the Security of Accounting Information Systems: A Field Study in Telecommunication Companies Operating in the Republic of Yemen

Sultan Ali Ahmed Al-Sorihi [1], ***Mohammed A. Alrubaidi*** [2], ***Nabil Hassan Abdo Al-Hemyari*** [3]

ABSTRACT

This study aims to test Security Controls (SCs) as a mediator between information-technology risks (ITR) and the security of AISs in telecommunication companies operating in Yemen (TCOY). To achieve this objective, a questionnaire was used to collect data according to the comprehensive method, where (356) questionnaire forms were distributed and the validated questionnaire forms for analysis were (218). To analyze the data, (SmartPLS) was used in assessing the measurement model and the structural model, as well as in the evaluation of path coefficients and testing the hypotheses of the study. It has been concluded that ITRs negatively affect the security of AISs before the mediation of SCs (47.6%). The results indicate that the mediation of SCs between ITRs and security of AISs is a partial mediation. Also, ITRs have an indirect negative impact on the security of AISs after the mediation of SCs (25.3%), as part of the impact is transferred through SCs from ITRs to the security of AISs (indirect impact). The study concluded with a set of recommendations, most notably: paying more attention to the confidentiality, integrity and availability of information, keeping abreast of technological developments, implementing SCs and updating them constantly, supporting the information security by the higher management, improving security-response activities, accelerating the implementation of robust authentication, giving great attention to access control, and effectively monitoring security policy-implementation. This is to raise the level of security of AISs and reduce the negative impact of ITRs.

Keywords: Information technology risks, Security controls, Security of accounting information systems.

1 Associate Professor of Accounting and Auditing, University of Science and Technology, Yemen. Sultan.farag@yahoo.com
2 Professor of Accounting and Auditing, University of Science and Technology, Yemen. dr.marubaidi@hotmail.com
3 Assistant Professor of Accounting and Auditing, University of Science and Technology, Yemen. nabelal2000@yahoo.com

Received on 3/8/2022 and Accepted for Publication on 12/9/2023.

الدور الوسيط للضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية: دراسة ميدانية في شركات الاتصالات العاملة في الجمهورية اليمنية

سلطان علي أحمد السريحي[1]، محمد علي الربيدي[2]، نبيل حسان عبده الحميري[3]

ملخص

هدفت هذه الدراسة إلى اختبار الضوابط الأمنية كمتغير وسيط بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في الجمهورية اليمنية. ولتحقيق هذا الهدف، تم الاعتماد على طريقة المسح الشامل باستخدام الاستبانة أداة لجمع البيانات، وقد تم توزيع (356) استبانة، ولكن الصالح منها للتحليل كان (218) استبانة. ولتحليل البيانات، تم استخدام (SmartPLS) في تقييم النموذج القياسي؛ لمعرفة صلاحية أداة التحليل، واستخدام النموذج البنائي وفق معامل المسار؛ لاختبار فرضيات الدراسة، وقد تم التوصل إلى أن مخاطر تكنولوجيا المعلومات تؤثر سلباً في أمن نظم المعلومات المحاسبية بنسبة 47.6% قبل توسط الضوابط الأمنية، وتشير النتائج إلى أن وساطة الضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية هي وساطة جزئية، وأن مخاطر تكنولوجيا المعلومات تؤثر سلباً في أمن نظم المعلومات المحاسبية بعد وساطة الضوابط الأمنية بنسبة 25.3%، حيث ينتقل جزء من الأثر عبر الضوابط الأمنية؛ للحد من مخاطر تكنولوجيا المعلومات إلى أمن نظم المعلومات المحاسبية (الأثر غير المباشر). ومن أهم التوصيات في ضوء نتائج هذه الدراسة: تنفيذ الضوابط الأمنية (التقنية والإدارية) على حد سواء وتحديثها باستمرار، والاهتمام بسرية المعلومات وسلامتها وتوافرها، ومواكبة التطورات التكنولوجية، والرقابة الفاعلة على تطبيق السياسة الأمنية؛ لرفع مستوى أمن المعلومات، وخفض الأثر السلبي لمخاطر تكنولوجيا المعلومات.

الكلمات الدالة: مخاطر تكنولوجيا المعلومات، الضوابط الأمنية، أمن نظم المعلومات المحاسبية.

1. المقدمة

تعد قضية ضعف أمن نظم المعلومات وقصورها قضية شائكة ومستمرة لديناميكية التكنولوجيا المتطورة؛ فقد رصدت العديد من الدراسات والتقارير الاختراقات الأمنية التي عانت منها أنظمة الشركات. وقد أكد استطلاع (CSBS, 2016: 34, 36) أن ثلثي الشركات الكبيرة ونصف الشركات المتوسطة في عام 2015م عانت من اختراقات أمنية إلكترونية. وتوصلت دراسة (AICPA, 2013: 2, 4) إلى أن متوسط الهجمات الناجحة بلغ (102) من الهجمات في الأسبوع عام 2012م. وذكرت دراسة (Malik, 2023) أن متوسط تكلفة خرق البيانات يتراوح من 120 ألف دولار إلى 1.24 مليون دولار. وأشار تقرير (Deloitte Co, 2016: 3) إلى أن أكثر من نصف الشركات الأيرلندية عانت من اختراقات أمنية خلال عام 2015م.

لقد أصبحت الهجمات السيبرانية متطورة بمستوى يتفوق على قدرات وسائل الحماية التقليدية (العلوان، 2022). ومؤخراً تعرضت الولايات المتحدة الأمريكية لهجوم سيبراني واسع النطاق شمل وزارة الأمن الداخلي، ووزارة الخزانة، ووزارة التجارة، وإدارة الأمن النووي، وشركة FireEye، وشركة Microsoft، حيث تمكن المهاجمون من زراعة ملفات خبيثة في تحديث برنامج Orion الذي طورته شركة SolarWinds، وقام العملاء بتنزيل هذه التحديثات وبذلك منحوا المهاجمين وصولاً غير محدود إلى

1 أستاذ المحاسبة والتدقيق المشارك، جامعة العلوم والتكنولوجيا، اليمن.
2 أستاذ المحاسبة والتدقيق، جامعة العلوم والتكنولوجيا، اليمن.
3 أستاذ المحاسبة والتدقيق المساعد، جامعة العلوم والتكنولوجيا، اليمن.
تاريخ استلام البحث 2022/8/3 وتاريخ قبوله 2023/9/12.

أجهزتهم، وتشير التحقيقات إلى أن تقييم حجم الأضرار قد يستغرق شهوراً (Microsoft, 2020).

وقد ناقشت الدراسات والمنظمات المهنية الآثار السلبية الناجمة عن الاختراقات الأمنية؛ فقد أشارت دراسة (AICPA, 2013: 2, 4) إلى سائر الإيرادات المتعلقة بالتجارة الإلكترونية، التي قدرت بـ (3.4) مليار دولار أمريكي في عام 2011م الناجمة عن الاحتيال. وخلصت دراسة (CSBS, 2016: 37, 41) إلى أن متوسط كلفة الاختراقات في الشركات البريطانية الكبيرة بلغ (36,500) جنيه إسترليني في عام 2015م، وقد أثرت هذه الاختراقات بشكل كبير على الأنشطة التجارية، وأدت إلى توقف الأعمال التجارية، وسببت خسائر مالية كبيرة.

وأشارت التقارير (ACSC, 2015: 7) إلى تعرض القطاعات الاقتصادية لمخاطر مختلفة كبدتها خسائر مالية كبيرة، وذكر استطلاع (Ponemon, 2015: 1, 16, 23) أن عدد الهجمات التي تعرضت لها الشركات في (7) دول بلغ (1,928) هجمة، وجاء متوسط الكلفة السنوية (7.7$) مليون دولار، ونتج عن الهجمات تعطل الأعمال، وفقدان المعلومات السرية، وفقدان الإيرادات، وتوصلت دراسة (Ponemon GA, 2015: 1) في (11) دولة منها السعودية والإمارات، إلى أن متوسط الكلفة الإجمالية لاختراق البيانات بلغ (3.79$) مليون دولار، وجاء في تقرير (Kemper, 2018) أن كلفة الأمن السيبراني ارتفعت في عام 2017م بنسبة 23% عن العام السابق، وأن متوسط الكلفة الناجمة عن الأضرار قدّر بمليون دولار أمريكي.

وعرّف المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology (NIST)، ولجنة أنظمة الأمن القومي Committee on National Security Systems (CNSS)، والقانون الأمريكي أمن المعلومات (InfoSec) بأنه "حماية المعلومات ونظم المعلومات من الوصول غير المصرح به أو الاستخدام أو الكشف أو التوقف أو التعديل أو الإتلاف؛ من أجل ضمان السرية والسلامة والتوافر" (NISTIR 7621 r1, 2016: 2; CNSSI N 4009, 2015: 94).

ونظراً لأهمية أمن المعلومات في منظمات الأعمال، فقد أصدرت المنظمات المهنية ذات العلاقة أطراً ومعايير تهدف إلى حماية المعلومات من المخاطر، مثل إطار الأهداف الرقابية المتعلقة بالمعلومات والتكنولوجيا ذات الصلة Control Objectives for Information and Related Technology (COBIT) (ISACA, 2019)، ومن تلك المنظمات المنظمة الدولية للمعايير International Organization for Standardization (ISO) بالتعاون مع اللجنة الكهروتقنية الدولية (ISO, International Electrotechnical Commission (IEC) (2019، والاتحاد الدولي للاتصالات International Telecommunication Union (ITU) (ITU, 2020).

وتهدف هذه الدراسة إلى اختبار دور الضوابط الأمنية [المتغير الوسيط] في العلاقة بين مخاطر تكنولوجيا المعلومات [المتغير المستقل] وأمن نظم المعلومات المحاسبية [المتغير التابع] في شركات الاتصالات العاملة في اليمن.

2. مشكلة الدراسة

في عام 2018م، وصل ترتيب اليمن عالمياً في مجال الأمن السيبراني إلى (172) من أصل (175) ورقمها القياسي (0.019) (International Telecommunication Union (ITU), 2019: 68)، وقد أعطت أكاديمية الحوكمة الإلكترونية e-Governance Academy (eGA) اليمن درجة متدنية في مجال الأمن الإلكتروني، حيث كان ترتيبها (148) من أصل (161)، وكان مؤشر الأمن السيبراني (7.79) (NCSI, 2020)، وبالتالي يتضح أن هناك قصوراً كبيراً في الجوانب التشريعية والتنظيمية المتعلقة بأمن المعلومات في اليمن، وهذا ما أكدته تقارير الاتحاد الدولي للاتصالات (ITU) وأكاديمية الحوكمة الإلكترونية (EGA). وقد رصد الخبراء في شركة Kaspersky المختصة بأمن المعلومات تنصت وكالة الأمن القومي National Security Agency (NSA) على الحواسيب الشخصية المصابة ببرامج التجسس في (30) دولة، من بينها اليمن.

وتناولت بعض الدراسات مخاطر أمن نظم المعلومات المحاسبية في المنشآت اليمنية، حيث أشارت نتائج دراسة (الربيدي، 2010: 35) إلى عدم سلامة تجهيز البيانات، وعدم وجود نسخ احتياطية للبيانات في مكان آمن، وعدم وجود خطة للطوارئ، وعدم وجود رقابة آلية، وعدم القدرة على حماية خصوصية العملاء.

وأشارت نتائج الدراسة الاستطلاعية التي قام بها باحثون إلى وجود مخاطر تهدد أمن نظم المعلومات المحاسبية في شركات

الاتصالات مجتمع الدراسة، وتتمثل في التعديل غير المصرح به لحد ائتمان المشتركين، وتوقف النظام، وإجراء مكالمات مجانية، واختلاف تكاليف المكالمات في السنترال عن تكاليفها في نظام الفوترة، وعدم إجراء التسويات الدورية للجزء المستنفد من كروت الخدش والاعتراف به كإيراد، وعدم إنشاء بعض حسابات المشتركين في نظام الفوترة، والتقادم التكنولوجي للأجهزة والمعدات والبرامج، والحروب، والانعدام الكلي للطاقة العمومية.

وفيما يتعلق بالضوابط الأمنية، فإن استخدامها يساعد في منع المخاطر أو الحد من آثارها السلبية، وحماية أصول نظم المعلومات (Schuessler, 2013: 7) من الوصول غير المصرح به، وتقييد عمليات الوصول المصرح به، والتحقق من هوية المستخدمين (GAO-16-605, 2016: 6).

وقد تناول عدد من الدراسات الضوابط الأمنية المستخدمة في حماية أنظمة المعلومات من المخاطر كالتحكم بالوصول، والتحقق من الهوية، ومكافحة البرامج الضارة، وأنظمة كشف التسلل، والتشفير، والجدران النارية، والتعافي من الكوارث، والاستجابة للحوادث، والنسخ الاحتياطي، والتوعية والتدريب، والسياسات الأمنية (Schuessler, 2013: 184)، كما أشارت دراسة (Schuessler, 2009: 27) إلى أن الضوابط الأمنية يمكنها الحد من المخاطر. ووفقاً لنظرية الردع العام (Straub & Welke, 1998: 441) التي تفترض إجراءات عامة تقلل من المخاطر بشكل مباشر أو غير مباشر من خلال استخدام الضوابط، فهذا يعني أن المخاطر لها تأثير سلبي مباشر وغير مباشر في أمن المعلومات، وأن الضوابط الأمنية تحد من المخاطر. واستناداً إلى نظرية أمن المعلومات (Horne et al., 2016: 2) التي تشير إلى أن الدافع وراء كل المحاولات التي تقوم بها المنظمات لتأمين المعلومات من المخاطر هو إيجاد الموارد التي يمكن استخدامها لاحقاً في تحسين الأداء، فإن المعلومات تتعرض للمخاطر ما لم تنفذ ضوابط كافية.

وتتيح التدابير القانونية وضع آليات ملائمة للرد على اختراق أمن المعلومات من خلال التحقيق في الجرائم وملاحقة مرتكبيها. وقد أصدر البرلمان اليمني القانون ذا الرقم 40–2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية؛ من أجل تعزيز الإشراف والرقابة، وهذا يسري على التعاملات الإلكترونية. كذلك صدر القانون ذو الرقم 13–2012م بشأن حق الحصول على المعلومات، وهو يتضمن حماية نظم وشبكات المعلومات من المخاطر.

3. أسئلة الدراسة

وفق ما تمت مناقشته في مشكلة الدراسة، فإن السؤال الرئيسي يتمثل في: ما مدى أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية في شركات الاتصالات العاملة في الجمهورية اليمنية؟ ويقسم هذا السؤال الرئيسي إلى السؤالين الفرعيين الآتيين:

1) ما أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط التقنية؟
2) ما أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الإدارية؟

4. أهداف الدراسة

تعد الأهداف انعكاساً للأسئلة، ويتمثل الهدف الرئيسي في اختبار دور الضوابط الأمنية [المتغير الوسيط] بين مخاطر تكنولوجيا المعلومات [المتغير المستقل] وأمن نظم المعلومات المحاسبية [المتغير التابع] في شركات الاتصالات العاملة في الجمهورية اليمنية. ويتفرع هذا الهدف إلى هدفين فرعيين هما:

1) اختبار الضوابط التقنية [المتغير الوسيط] بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية.
2) اختبار الضوابط الإدارية [المتغير الوسيط] بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية.

5. اهمية الدراسة

تكمن هذه الأهمية من الناحية النظرية في بناء إطار نظري علمي يوضح مفهوم أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية. وتكمن هذه الأهمية من الناحية العملية في الفائدة التي سوف تتحقق للمستفيدين من هذه الدراسة.

1.5 الأهمية النظرية

- تقدم الدراسة الحالية تأصيلاً نظرياً علمياً لمفاهيم أمن نظم المعلومات المحاسبية، ومخاطر تكنولوجيا المعلومات،

والضوابط الأمنية.

- تقدم الدراسة الحالية متغيراً وسيطاً لم تسبق دراسته من قبل الدراسات السابقة (الضوابط الأمنية)؛ لقياس الأثر غير المباشر لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية.
- يساعد استخدام الضوابط الأمنية (التقنية والإدارية) في تحقيق أمن نظم المعلومات المحاسبية من خلال آليات المصادقة، والتحكم بالوصول، والتشفير، والتدابير التنظيمية والقانونية، التي تعمل جميعها على منع المخاطر أو الحد من آثارها السلبية.
- بناء نموذج معرفي جديد يستند على تأصيل علمي يعكس الترابط المنطقي بين المخاطر والأمن، وذلك من خلال الضوابط، وفقاً لنظرية الردع العام، ونظرية أمن المعلومات التي تفسر العلاقة بين هذه المتغيرات ولم يسبق تفسيرها من قبل.
- تطوير مقاييس المتغيرات المستخدمة في الدراسة الحالية بخلاف الدراسات السابقة.
- تُعد هذه الدراسة الأولى من نوعها في قطاع الاتصالات في البيئة اليمنية.

2.5 الأهمية العملية

- تُساعد دراسة أمن نظم المعلومات المحاسبية في شركات الاتصالات في كشف وخفض الحوادث الأمنية، وتحديد المخاطر، وتأمين المعلومات الحساسة.
- تُبين الدراسة الحالية دور الضوابط الأمنية في شركات الاتصالات؛ نظراً لأهميتها في حماية الموارد من الوصول غير المصرح به، وتقييد عمليات الوصول، والتحقق من هوية المستخدمين.
- سوف تستفيد من هذه الدراسة كل من: إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت في شركات الاتصالات، ووزارة الاتصالات وتقنية المعلومات، وذلك من خلال تنفيذ الضوابط الأمنية الملائمة بما في ذلك تنفيذ المصادقة القوية متعددة العوامل والتحكم بالوصول المادي والمنطقي.

6. الإطار النظري للدراسة

1.6 مفهوم وأهمية أمن نظم المعلومات المحاسبية

أصبح استخدام مصطلح أمن المعلومات شائعاً بعد ظهور تكنولوجيا المعلومات والاتصالات وأنظمة المعلومات واستخدامها في معالجة البيانات ونقلها وتخزينها، وجعل من أنظمة المعلومات الموجودة في أي منظمة ذات أهمية خاصة (العرود وشاكر، 2009)، وتعد نظم المعلومات المحاسبية أحد الفروع الرئيسية لأمن نظم المعلومات الشامل للمنظمة.

وقد عرفتها لجنة أنظمة الأمن القومي (CNSSI N 4009, 2015: 94)، والمعهد الوطني للمعايير والتكنولوجيا (NISTIR 7621 r1, 2016: 2)، بأنها "حماية المعلومات ونظم المعلومات من الوصول غير المصرح به، أو الاستخدام، أو الكشف، أو التعديل، أو الإتلاف، أو التعطل؛ من أجل ضمان السرية، والسلامة، والتوافر"، وهو أكثر التعاريف شمولية، وهذا يعني أن أمن نظم المعلومات المحاسبية يعد عملية حماية للحد من المخاطر لضمان السرية، والسلامة، والتوافر للمعلومات. في أثناء المعالجة أو التخزين أو النقل؛ من أجل ضمان استمرارية المنظمة.

وتشير نظم المعلومات المحاسبية المحوسبة Computerized Accounting Information Systems (CAISs) إلى نظم إلكترونية تعمل على معالجة البيانات، وتهيئ لاتخاذ قرارات مناسبة، والتنفيذ والمتابعة لأنشطة المنظمة، وتحقق الفاعلية والكفاءة، وتمكن من تبادل المعلومات. وقد حقق استخدام هذه الأنظمة (CAISs) في منظمات الأعمال العديد من المزايا (AICPA, 2013).

ومع تزايد اعتماد الشركات على نظم المعلومات المحاسبية المحوسبة (CAISs). تصبح قضية أمن الأنظمة مسألة ذات أهمية قصوى؛ إذ يقوم أمن المعلومات بأداء أربع وظائف مهمة، وهي: حماية قدرة المنظمة على العمل، والتشغيل الآمن للتطبيقات، وحماية البيانات، وحماية الأصول التقنية المستخدمة في المنظمة، كما يتضمن أمن نظم المعلومات المحاسبية الإجراءات اللازمة لحماية النظم المحاسبية من المخاطر الداخلية والخارجية (Bafghi, 2014: 73, 75)، وضمان استمرارية الأعمال، ومنع المخاطر أو الحد من آثارها السلبية، والتركيز على الاستثمار في كشف الهجمات والاستجابة للحوادث (Gunawan & Nengzih, 2023: 24).

وتشير نتائج استطلاع (PwC) إلى أن استخدام الأطر الأمنية يؤتي ثماره على المدى الطويل، مثل (ISO 27001) و(NIST)، حيث أفاد المشاركون أن مزايا استخدام الأطر الأمنية تتمثل في القدرة على كشف وخفض الحوادث الأمنية بنسبة 47%، والقدرة على تحديد المخاطر وترتيب أولوياتها بنسبة 49%، وتأمين البيانات الحساسة بنسبة 45%، وإدراك الثغرات في السياسة بنسبة 37% (Hulme, 2015). وأكد المدققون على ضرورة تعزيز أمن نظم المعلومات المحاسبية وفقاً لأحدث التطورات التكنولوجية (Bafghi, 2014: 73).

وتحظى القضايا الأمنية باهتمام كبير بشكل عام من قبل الأفراد والمنظمات والدول، ومنها قضايا أمن نظم المعلومات المحاسبية Accounting Information Systems (AISs)؛ فهي تحتل مساحة واسعة من الدراسات والأبحاث وعقد المؤتمرات، وقد أدى انتشار الأنظمة وشبكات المعلومات والاعتماد عليها إلى عدم قدرة أي نشاط تجاري على إهمال القضية الأمنية، وبالأخص في حالة أن المنظمات ومستخدمي الأنظمة غير مدركين للمخاطر، وأن تلك الأنظمة غير آمنة، وبموجبها ستزداد المخاطر الأمنية (Riad, 2009: 35; Quoc, Bao, Huu & Bao, 2023: 342). وقد وصلت كمية البيانات التي يتم إنشاؤها وتخزينها إلى مستويات غير مسبوقة، وتحتوي هذه البيانات على معلومات حساسة كالتفاصيل الشخصية، والمعلومات المالية، والأسرار التجارية، وأصبح ضمان أمن هذه البيانات أولوية قصوى في منظمات الأعمال (LinkedIn, 2023).

وتؤكد العديد من الدراسات والتقارير أهمية أمن المعلومات في منظمات الأعمال، حيث توصل تقرير الأمن السنوي لشركة (Cisco) إلى أن ثلثي المشاركين يقولون إن القيادة التنفيذية في منظماتهم تعتبر الأمن أولوية عالية، ويرى 58% من مديري العمليات الأمنية Security Operations (SecOps) أن القيادة التنفيذية في منظماتهم تعتبر الأمن أولوية عالية، كما يرى 67% من كبار موظفي أمن المعلومات Chief Information Security Officers (CISOs) أن القيادة التنفيذية في منظماتهم تعتبر الأمن أولوية عالية (Cisco, 2015: 48).

2.6 عناصر أمن المعلومات

منذ أواخر سبعينات القرن العشرين وأمن المعلومات محاط بالسرية Confidentiality، والسلامة Integrity، والتوافر Availability، ويطلق على تلك الخصائص مثلث أمن المعلومات، ويشير إليها الباحثون والمنظمات المهنية بعناصر الأمن.

الشكل (1)
مثلث أمن المعلومات

وأشارت دراسة (Riad, 2009: 43) إلى أن هناك عناصر أساسية لأمن المعلومات بشكل عام وأمن المعلومات المحاسبية بشكل خاص اتفق عليها معظم الأكاديميين والممارسين، وهي: السرية، والسلامة، والتوافر.

3.6 أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية

تعد مخاطر تكنولوجيا المعلومات تهديداً لنظم المعلومات المحاسبية، وهي نقاط ضعف في الضوابط الأمنية، وتسبب الأضرار والخسائر وأي نتائج سلبية محتملة نتيجة استخدام الأجهزة والبرمجيات والأنظمة والتطبيقات والشبكات (Bin et al., 2008: 477). وتستخدم المنظمات الضوابط الأمنية لزيادة فاعلية أمن نظم المعلومات، والحد من المخاطر التي تؤثر سلباً في نظم المعلومات. ويتمثل غرض الضوابط الأمنية إما في القضاء على المخاطر أو في الحد من تأثيرها؛ لحماية أصول نظم المعلومات (Schuessler, 2013: 7).

1.3.6 مخاطر تكنولوجيا المعلومات

إن المقصود بمخاطر أمن المعلومات هي تلك المخاطر التي تنشأ عن فقدان سرية، أو سلامة، أو توافر المعلومات ونظم

المعلومات، وتنعكس الآثار السلبية المحتملة على عمليات وأصول التنظيم، وتشمل هذه المخاطر: أفعالاً بشرية (داخلية وخارجية، متعمدة وغير متعمدة)، ومشاكل تكنولوجية (البرمجيات، والأجهزة، والأنظمة، والبرامج الخبيثة)، وكوارث طبيعية وغير طبيعية (NIST SP 800-30 r1, 2012: 6-8)، وإن إحدى القضايا المهمة التي تعاني منها منظمات الأعمال حالياً هي استمرار ظهور مخاطر جديدة لم تشهدها المنظمات من قبل.

وتتمثل الأضرار المترتبة على حدوث المخاطر في كشف المعلومات، أو تعديلها، أو إتلافها، أو الحرمان من الخدمة (NIST SP 800-30 r1, 2012, 8). وتتراوح الأضرار بين خسائر بسيطة وتدمير النظام بالكامل. ومن الملاحظ أن المخاطر الأمنية زادت بشكل كبير (Tarmidi et al., 2013: 109)، حيث ناقشت بعض الدراسات أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات، وأشارت أغلب هذه الدراسات إلى وجود أثر سلبي لها (Gordon et al., 2011: 35; Straub & Welke, 1998: 441; Riad, 2009: 45).

وتشير دراسة (Al-Ghananeem, 2014: 64) إلى أن المخاطر تؤثر سلباً في ضمان أمن المعلومات (الضوابط الأمنية)، وأظهرت دراسة (Straub, 1987: 280) أن الوقاية أداة فاعلة في الحد من إساءة الاستخدام، وأن المخاطر تدفع المنظمات إلى استخدام التدابير المضادة. وقد أرجعت بعض الدراسات (Abu-Musa, 2006: 187; Tarmidi et al., 2013: 109) ارتفاع المخاطر إلى قصور في الممارسات الأمنية، والضوابط الرقابية.

ونخلص إلى القول إن مخاطر تكنولوجيا المعلومات هي الأثر السلبي المحتمل في أنظمة المعلومات المحاسبية المتمثل في الوصول أو الكشف غير المصرح به للمعلومات (فقدان السرية)، وتعديل المعلومات أو إتلافها (فقدان السلامة)، وتعطل أو توقف النظام والخدمات (فقدان التوافر)، وقد تم اختيار مخاطر تكنولوجيا المعلومات متغيراً مستقلاً في هذه الدراسة؛ لأهمية منعها أو الحد منها. لذلك تمت إضافتها إلى النموذج المعرفي لهذه الدراسة.

2.3.6 الضوابط الأمنية

تعرف الضوابط الأمنية بأنها الضوابط الإدارية والتقنية اللازمة لنظم المعلومات؛ لحماية سريتها، وسلامتها، وتوافر معلوماتها (CNSSI N 4009, 2015: 110). وعرّفتها دراسة (Riad, 2009: 73) بأنها التدابير المضادة المستخدمة لحماية النظم والمعلومات المحاسبية، وضمان سريتها، وسلامتها، وتوافرها. وتستخدم المنظمات الضوابط الأمنية؛ لزيادة فاعلية أمن نظم المعلومات، والحد من المخاطر التي تؤثر سلباً في نظم المعلومات، والهدف من ذلك هو القضاء على المخاطر أو الحد من تأثيرها، وحماية أصول نظم المعلومات (Schuessler, 2013: 7).

والضوابط الأمنية الأكثر استخداماً، هي: ضوابط الوصول الإلكتروني إلى البيانات والشبكات، وتنفيذ الإجراءات والإرشادات التنظيمية والتشغيلية. وتعمل تقنيات التشفير، والتوقيع الرقمي، والبصمة الرقمية على حماية عناصر أمن المعلومات، وتعمل تقنيات الجدران النارية والشبكات الخاصة الافتراضية على حماية الشبكات في ظل ازدياد استخدام شبكة الإنترنت غير الآمن.

وهناك أنظمة حماية متاحة، كالتحكم بالوصول، ومكافحة البرامج الضارة، ومكافحة الهجوم والتجسس، والاصطياد الإلكتروني، وخطط استمرارية الأعمال. ويعتمد اختيار وتطبيق الضوابط الأمنية على تقييم مخاطر نظم المعلومات؛ فعملية تقييم المخاطر تُحدد التهديدات ونقاط الضعف في النظام، والضوابط الأمنية تحد من المخاطر المحتملة وتقلل من الخسائر (Keung, 2013: 1). وينبغي تحديث الضوابط الأمنية بانتظام على أساس المخاطر المتغيرة (SANS, 2018). وقد تناولت معظم الدراسات أثر الضوابط الأمنية في أمن نظم المعلومات، وخلصت أغلبها إلى وجود أثر إيجابي، ومنها دراستا (Riad, 2009: 45; Schuessler, 2009: 63).

ونخلص إلى القول إن الضوابط الأمنية هي الضوابط التقنية والإدارية اللازمة لحماية نظم المعلومات المحاسبية وضمان سريتها، وسلامتها، وتوافرها، ضد المخاطر المختلفة في أثناء المعالجة أو التخزين أو النقل. وقد تم اختيار الضوابط الأمنية كمتغير وسيط لأهميتها في الحد من مخاطر تكنولوجيا المعلومات في أمن نظم الملومات المحاسبية. لذلك تمت إضافتها في النموذج المعرفي كمساهمة جديدة ذات أهمية كبيرة لهذه الدراسة.

3.3.6 وساطة الضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم الملومات المحاسبية

في هذه الدراسة، تم اختيار الضوابط الأمنية متغيراً وسيطاً

بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية بشكل مخالف للدراسات السابقة التي اختبرت الأثر المباشر وفق ما تم ذكره أعلاه من أن مخاطر تكنولوجيا المعلومات تؤثر سلباً بشكل مباشر في أمن نظم المعلومات المحاسبية. كذلك تؤثر الضوابط الأمنية إيجاباً بشكل مباشر في أمن نظم المعلومات المحاسبية، لذلك يعد الأثر غير المباشر لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية ذا أهمية عالية استناداً إلى نظرية الردع العام، ونظرية أمن المعلومات التي تؤكد دور وساطة الضوابط الأمنية التقنية والإدارية في حماية المعلومات وسريتها، وسلامتها، وتوافرها من مخاطر تكنولوجيا المعلومات.

وتفترض نظرية الردع العام (GDT) إجراءات عامة تقلل من تلك المخاطر بشكل غير مباشر من خلال استخدام تقنيات الردع، والوقاية، والكشف، والمعالجة (Straub & Welke, 1998: 441). وما يبرر مناقشة نظرية الردع العام إمكانية تطبيقها على نظم المعلومات، وقد تم تطبيقها بنجاح في أبحاث أمن نظم المعلومات (Schuessler, 2013).

وقدمت دراسة (D'Arcy et al., 2008: 2) نموذجاً موسعاً لنظرية الردع العام يفترض أن وعي المستخدم بالتدابير المضادة (السياسات الأمنية، وبرامج التوعية والتدريب، ومراقبة الحاسوب) له تأثير مباشر وغير مباشر في نوايا المستخدمين المتعلقة بإساءة استخدام نظم المعلومات من خلال إدراك المستخدمين للعقوبة (اليقين والشدة). وتوسعت دراسة (Schuessler, 2009: 63) في وجهات النظر المفاهيمية لنظرية الردع العام؛ لتشمل المخاطر غير البشرية (الكوارث الطبيعية، والإخفاق التقني). ويساعد هذا التوسع في التخطيط الوقائي للحد من المخاطر؛ فمثلاً يمكن استعادة البيانات المفقودة من خلال النسخ الاحتياطية بعد إخفاق الأجهزة أو حدوث كارثة طبيعية (TheoriZeit, 2016).

4.6 نظرية الردع العام

تعاني نظم المعلومات من أنواع معينة من المخاطر، وتكمن المشكلة في عدم إدراك المعنيين لمجموعة كاملة من الضوابط التي يمكن اتخاذها للحد من المخاطر. وقد يرجع ذلك إلى ضعف المعرفة؛ فالإجراءات اللاحقة للتعامل مع المخاطر أقل فاعلية مما يجب، وهذا أحد التفسيرات القابلة للتطبيق، ويدلل على ذلك ارتفاع الخسائر الناجمة عن إساءة استخدام الحاسوب (الوصول غير المصرح به، وإتلاف موارد النظام، وكشف أو نسخ غير مصرح به للبيانات، وتعديل غير مصرح به للبيانات أو البرامج) والكوارث التي قد تكون مدمرة. ويمكن الحد من المخاطر في حال إدراك النطاق الكامل للضوابط المتاحة، وتنفيذ أكثر الضوابط فاعلية. وتعد نظرية الردع العام General Deterrence Theory (GDT) نظرية سلوكية راسخة، وهي نموذج مفاهيمي، وتقدم نظرة ثاقبة حول كيفية التعامل مع المخاطر (Straub & Welke, 1998: 441).

وتركز هذه النظرية على العقوبات التي من شأنها أن تؤثر في الآخرين، وتؤدي العقوبات إلى مثبطات للأفعال غير المشروعة، وهي تتمثل في مبدأين رئيسين، هما: 1) اليقين بالعقوبات (شعور الفرد بأنه لا مفر من خضوعه للعقاب إذا ارتكب الجريمة). 2) شدة العقوبات (التخويف من تبعات ارتكاب الجرائم) (Blumstein et al., 1978; Straub & Welke, 1998: 441)؛ فعندما تكون مخاطر العقاب مرتفعة (اليقين بالردع)، والعقوبات على الانتهاكات شديدة (شدة الردع)، تتنبأ النظرية بردع الجناة المحتملين عن ارتكاب أفعال غير مشروعة (Straub, 1990: 260). وتفترض نظرية الردع العام (GDT) إجراءات عامة تقلل من المخاطر بشكل مباشر أو غير مباشر من خلال استخدام تقنيات الردع، والوقاية، والكشف، والمعالجة (Straub & Welke, 1998: 441).

وقد تم تصنيف التدابير المضادة –وفقاً لدورة عمل الأمن The Security Action Cycle (SAC) في نظرية الردع العام– إلى أربع فئات: (الردع، والوقاية، والكشف، والمعالجة)، وهي تساعد في إيجاد بدائل أمنية، وتقدم للممارسين منظوراً نظرياً لتنفيذ التدابير المضادة (Straub & Welke, 1998: 445; Schuessler, 2013: 7). وتظهر جهود الردع في تثبيط السلوك الإجرامي باستخدام: السياسات الإدارية، وتدريب الموظفين، والمهام الأمنية الواضحة (Schuessler, 2009: 10; Merriam-Webster, 2018). وتشمل الضوابط الوقائية ضوابط التحكم بالوصول المادي (مثل الحراس، والأبواب المغلقة)، والمنطقي (مثل المصادقة، والجدران النارية)، وتشمل الإجراءات العلاجية استجابة ملائمة في شكل: إنذارات، وتأنيب، وغرامات، وإيقاف

إنهاء الخدمة، بينما تشمل الإجراءات القانونية الدعاوى الجنائية أو المدنية (Straub & Welke, 1998: 445).

وتعتمد الدراسة الحالية على نظرية الردع العام ضمن الإطار النظري من أجل أن تتمكن المنظمة من خلالها من استخدام الضوابط الأمنية المتاحة (التقنية، والإدارية) في الحفاظ على أمن نظم المعلومات المحاسبية (السرية والسلامة والتوافر) من مخاطر تكنولوجيا المعلومات (من أجل منعها أو الحد من تأثيرها).

5.6 نظرية أمن المعلومات

تعد نظرية أمن المعلومات نظرية شاملة، ويتم بموجبها تنفيذ الحماية على أساس علمي ومنهجي متين، ويتمثل هدف أمن المعلومات المسلم به على نطاق واسع في حماية سرية المعلومات، وسلامتها، وتوافرها؛ بغرض ايجاد الموارد (Miloslavskaya, 2014: 2; Horne et al., 2016: 1). وتنص نظرية أمن المعلومات Theory of Information Security (TIS) على أن الدافع وراء كل المحاولات التي تقوم بها المنظمة لتأمين المعلومات من المخاطر هو الحصول على الموارد التي يمكن استخدامها لاحقاً في تحسين الأداء التنظيمي. وقد نشأت نظرية أمن المعلومات (TIS) في مجال نظم المعلومات، وبنيت بالكامل من المفاهيم التي تتعلق بالمعلومات. وأمن المعلومات هو ظاهرة تندرج ضمن نطاق نظم المعلومات (Horne et al., 2016: 2). ويمكن استخدام هذه النظرية في تفسير الدوافع وراء الجهود الرامية إلى حماية المعلومات المستخدمة من قبل الأفراد، والمجموعات، والمنظمات، وأيضاً في حماية المعلومات المشتركة بين المنظمات. وتنص هذه النظرية على أن تطبيق الضوابط يؤدي إلى تحويل المعلومات إلى موارد. ويشير مصطلح التفسير السببي إلى التحليل السببي الاحتمالي؛ بمعنى أن تطبيق الضوابط يزيد من احتمالية تحويل المعلومات إلى موارد (Horne et al., 2016: 9).

وتقدم نظرية أمن المعلومات نموذجاً من ثلاثة عناصر، هي: (الضوابط، والمخاطر، والموارد):

1) **الضوابط:** إن ضوابط أمن المعلومات هي عبارة عن مزيج ملائم من ضوابط الأمن: المادية، أو التقنية، أو التشغيلية، ويساعد تطبيق الضوابط في حماية سرية المعلومات، وسلامتها، وتوافرها، والتخفيف من المخاطر المختلفة (Posthumus & von Solms, 2004: 642)، ويساعد أيضاً في منع وكشف الهجمات، وتشمل الضوابط الأمنية: برنامج مكافحة الفيروسات، والجدران النارية، والتحديثات الأمنية، وأنظمة التحكم في تغيير كلمة المرور، ومجموعة من التقنيات الأخرى المتاحة لتحسين أمن المعلومات (Workman et al., 2008: 2800).
2) **المخاطر:** هناك العديد من المخاطر التي تواجه سرية المعلومات، وسلامتها، وتوافرها (Workman et al., 2008: 2800). وتشمل مخاطر أمن المعلومات اعتراض المعلومات وتعديلها غير المصرح به، وكشف المعلومات لأفراد غير مخولين، وإتلاف الأجهزة والبرمجيات والمعلومات (Workman et al., 2008: 2803)، وتستغل التهديدات المختلفة في نقاط الضعف، وفي النهاية يكون لها أثر سلبي على البنية التحتية (von Solms and van Niekerk, 2013: 99)، وقد يؤدي الاختراق إلى توقف العمليات، وبالتالي يظهر التآكل المحتمل للميزة التنافسية.
3) **الموارد:** تُعرف الموارد بأنها نقاط القوة التي يمكن للمنظمة استخدامها في صياغة استراتيجياتها وتنفيذها، وتُعد موارد المعلومات عنصراً حاسماً في دعم الأداء التنظيمي من خلال إيجاد الميزة التنافسية وحمايتها، لذلك فإن الحفاظ على الموارد غير الملموسة القائمة على المعلومات يُعد ضرورة ملحة للمنظمات (Horne et al., 2016: 7)، ولكي تكون العوائد المالية للمنظمة مستدامة، يجب أن تكون الموارد التي تدعمها مستدامة أيضاً (Grant, 1991: 124).

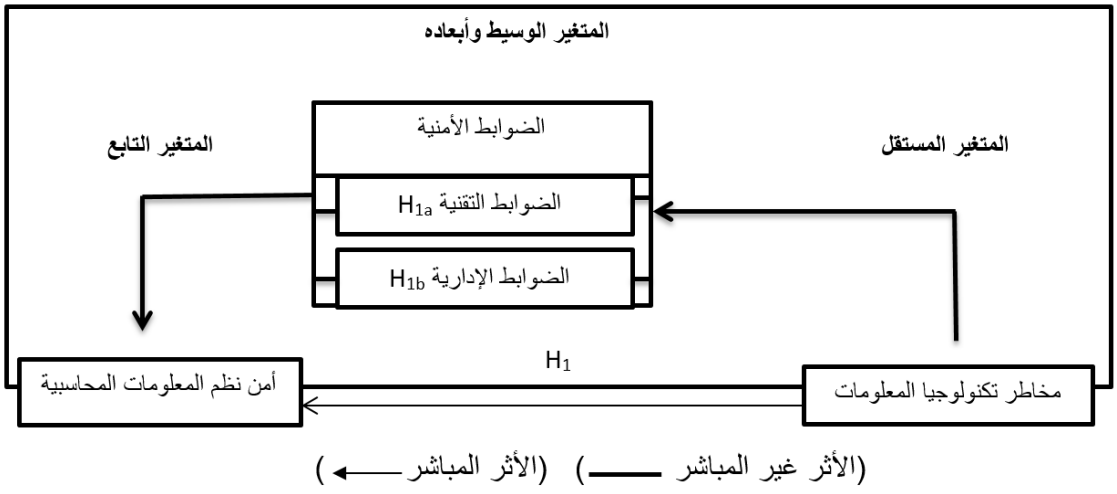
وهناك علاقة بين المعلومات والموارد، حيث يؤدي تطبيق ضوابط حماية المعلومات إلى تحويل المعلومات إلى موارد، كما أن هناك علاقة بين الضوابط والمعلومات، حيث تؤدي الضوابط إلى حماية المعلومات بشكل إيجابي. ويمكن تطبيق الضوابط التقنية، والرسمية، وغير الرسمية على المعلومات الموجودة على الوسائط المادية والرقمية. وهناك علاقة بين المخاطر والمعلومات، حيث تؤدي المخاطر إلى انتهاك سلامة المعلومات وسريتها وتوافرها بشكل سلبي. وهناك علاقة بين الضوابط والمخاطر؛ إذ إن بعض المعلومات محمية من قبل الضوابط لإنتاج موارد يمكن الاعتماد عليها. وإذا لم تتم حماية المعلومات بواسطة الضوابط، فلا يمكن اعتبارها موارد، وإن جميع المعلومات

التي يتعين استخدامها لأغراض تنظيمية يجب أن تكون محمية (Horne et al., 2016: 7-8).

7. النموذج المعرفي

استناداً إلى الإطار النظري والدراسات السابقة، تسعى الدراسة الحالية إلى اختبار الضوابط الأمنية باعتبارها متغيراً وسيطاً بين مخاطر تكنولوجيا المعلومات باعتبارها متغيراً مستقلاً وأمن نظم المعلومات المحاسبية باعتباره متغيراً تابعاً، وذلك من خلال استخدام نظرية الردع العام ونظرية أمن المعلومات المفسرة للأثر والعلاقة فيما بين متغيرات الدراسة.

بناءً على ما سبق، يُمكننا بناء شكل النموذج المعرفي للدراسة الحالية الذي يوضح علاقة الأثر المنطقي بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية، علماً بأن تلك الضوابط لا تمنع المخاطر، بل تحد منها؛ لذلك سيكون للمخاطر أثر غير مباشر وأثر مباشر.



الشكل (2)
النموذج المعرفي للدراسة

8. التعريفات الإجرائية

1.8 أمن نظم المعلومات المحاسبية

سبقت الإشارة إلى أن **أمن نظم المعلومات** هو الحفاظ على سرية المعلومات، وسلامتها، وتوافرها. ويتضمن هذا التعريف أبعاد المتغير التابع المتمثلة في (1) **السرية:** وهي حماية المعلومات من الكشف والوصول غير المصرح به (NISTIR 7621 r1, 2016: 2; ISO/IEC 27000, 2018: 2). (2) **السلامة:** وهي حماية المعلومات من التعديل والإتلاف غير المصرح به (NISTIR 7621 r1, 2016: 2). (3) **التوافر:** ويعني ضمان إمكانية الوصول إلى نظام المعلومات، أو ضمان الوصول إلى المعلومات في الوقت المناسب، وإمكانية الاعتماد عليها واستخدامها (ISO/IEC 27000, 2018: 2).

2.8 مخاطر تكنولوجيا المعلومات

سبق تحديد مفهوم **مخاطر تكنولوجيا المعلومات** بأنها تلك المخاطر التي تنشأ عن فقدان سرية المعلومات، أو فقدان سلامتها، أو فقدان توافرها، أو فقدان نظم المعلومات. ويتضمن تعريف مخاطر تكنولوجيا المعلومات الأبعاد الآتية: (1) **المخاطر المتعلقة بالسرية،** وتعني الكشف أو الوصول غير المصرح به للمعلومات السرية من خلال التنصت وكسر كلمة المرور، والوصول غير المصرح به، والأفعال المتعمدة، والاصطياد الإلكتروني والاجتماعي (Gordon et al., 2011: 35; Watuthu, 2015: 19). (2) **المخاطر المتعلقة بالسلامة،** وتعني التعديل أو الإتلاف غير المصرح به للمعلومات أو نظم المعلومات من خلال أفعال الموظفين، وأخطاء البرمجيات،

والتقادم التكنولوجي (Ahmadzadegan et al., 2013: 633). (3) **المخاطر المتعلقة بالتوافر**، وتعني منع المستخدمين المخولين من الوصول إلى المعلومات أو نظام المعلومات عند الطلب من خلال هجمات الحرمان من الخدمة، والكوارث الطبيعية، وأعطال الأجهزة الفنية (Gordon et al., 2011: 35). وقد تمت إضافة بعد رابع هو **المخاطر المشتركة**، وتعني فقدان عنصرين أو أكثر من عناصر الأمن (السرية، والسلامة، والتوافر) في هجوم واحد، كالبرامج الضارة، والانتحال، والرسائل المزعجة، وقرصنة الهاتف.

3.8 الضوابط الأمنية

أُشير سابقاً إلى أن **الضوابط الأمنية** هي: الضوابط الإدارية، والتقنية اللازمة لحماية سرية النظام والمعلومات، وسلامتهما، وتوافرهما. ويتضمن التعريف بُعدين أساسيين، هما: (1) **الضوابط التقنية**، وهي التدابير المتخذة لحماية نظام المعلومات من خلال الآليات المدرجة في مكونات الأجهزة والبرامج، كآليات التحقق من الهوية، والتحكم بالوصول، ومكافحة البرامج الضارة، وحماية الشبكة، وأنظمة التشفير. (2) **الضوابط الإدارية**، وهي الإجراءات الإدارية المتخذة لحماية نظام المعلومات من خلال: سياسة الأمن، وخطط الطوارئ، والتوعية والتدريب، وإجراءات التدقيق، والتدابير القانونية (Keung, 2013).

9. تطوير فرضيات الدراسة

تم تطوير فرضيات الدراسة الحالية بناءً على نتائج الدراسات السابقة، ونظرية الردع العام، ونظرية أمن المعلومات، واستناداً إلى اتجاه علاقة الأثر المنطقي بين متغيرات الدراسة التي تسعى إلى اختبار الأثر غير المباشر من خلال الضوابط الأمنية في شركات الاتصالات العاملة في اليمن. ومما سبق نجد أن الدراسات السابقة لم تتناول الضوابط الأمنية كمتغير وسيط، ووفقاً لنظرية الردع العام، ونظرية أمن المعلومات، يتضح أن للضوابط الأمنية دوراً وسيطاً في منع المخاطر أو الحد من آثارها السلبية، والحفاظ على سرية المعلومات وسلامتها وتوافرها، وبالتالي يمكن تطوير الفرضية الرئيسية للدراسة الحالية على النحو الآتي:

الفرضية الرئيسية: هناك أثر سلبي **لمخاطر تكنولوجيا المعلومات** في **أمن نظم المعلومات المحاسبية** من خلال **الضوابط الأمنية** في شركات الاتصالات العاملة في الجمهورية اليمنية.

ويوضح النموذج المعرفي للدراسة الأثر غير المباشر للمتغير المستقل، وهو (مخاطر تكنولوجيا المعلومات) في المتغير التابع، وهو: (أمن نظم المعلومات المحاسبية) من خلال المتغير الوسيط، وهو (الضوابط الأمنية). وتتفرع من هذه الفرضية فرضيتان على النحو الآتي:

1.9 تطوير الفرضية الفرعية الأولى

وقد تم تطويرها بناءً على نتائج الدراسات السابقة المتعلقة بِـ: **(مخاطر تكنولوجيا المعلومات، وأمن نظم المعلومات المحاسبية، والضوابط التقنية)**، ووفقاً لنظرية الردع العام (Schuessler, 2009: 63)، حيث تم التوسع في وجهات النظر المفاهيمية لهذه النظرية، لتشمل مصادر التهديدات الأخرى مثل التهديدات غير البشرية (الكوارث الطبيعية، والإخفاق التقني)، ويساعد هذا التوسع في التخطيط الوقائي للحد من المخاطر.

ومما سبق، نجد أن الدراسات السابقة لم تتناول بُعد الضوابط التقنية على أنه متغير وسيط بين المخاطر وأمن المعلومات. واستناداً إلى نظرية الردع العام، يتبين أن الضوابط التقنية لها دور وسيط بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات، وبالتالي يمكن تطوير الفرضية الفرعية الأولى للدراسة الحالية على النحو الآتي:

الفرضية الفرعية الأولى: هناك أثر سلبي **لمخاطر تكنولوجيا المعلومات** في **أمن نظم المعلومات المحاسبية** من خلال **الضوابط التقنية**.

2.9 تطوير الفرضية الفرعية الثانية

وقد تم تطويرها بناءً على نتائج الدراسات السابقة المتعلقة بِـ: **(مخاطر تكنولوجيا المعلومات، وأمن نظم المعلومات المحاسبية، والضوابط الإدارية)**، كما تم تطويرها أيضاً استناداً إلى نظرية الردع العام التي يفترض نموذجها الموسع أن وعي المستخدم بالتدابير المضادة يؤثر بشكل مباشر على إدراك المستخدم للعقوبة التي لها تأثير مباشر على نوايا إساءة استخدام نظم المعلومات، كما يفترض النموذج الموسع لتلك النظرية أن التدابير المضادة تؤثر بشكل غير مباشر على نوايا إساءة استخدام نظم المعلومات، وذلك من خلال إدراك المستخدم للعقوبة (D'Arcy et al., 2008: 2).

ومما سبق، يتضح أن الدراسات السابقة لم تتناول بُعد الضوابط الإدارية على أنه متغير وسيط بين المخاطر وأمن المعلومات. ووفقاً لنظرية الردع العام، يتبين أن الضوابط الإدارية لها دور وسيط بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات، وبالتالي يمكن تطوير الفرضية الفرعية الثانية للدراسة الحالية على النحو الآتي:

الفرضية الفرعية الثانية: هناك أثر سلبي **لمخاطر تكنولوجيا المعلومات** في **أمن نظم المعلومات المحاسبية** من خلال **الضوابط الإدارية.**

10. منهجية الدراسة

اعتمدت الدراسة الحالية المنهج الكمي بالأسلوب الاستدلالي في اختبار فرضيات الدراسة (اختبار الضوابط الأمنية، وهي متغير وسيط بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية). والتركيز الرئيس للدراسة الحالية هو على تحديد وتحليل وتفسير مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية، وعلى تحديد نمط الوساطة: (كلية، جزئية، لا توجد) للضوابط الأمنية.

1.10 مجتمع الدراسة وعينتها

استهدفت الدراسة الحالية جميع شركات الاتصالات العاملة في اليمن (وفقاً لأسلوب الحصر الشامل)؛ نظراً لصغر حجم المجتمع، وعددها سبع شركات: (المؤسسة، يمن نت، تيليمن، إم تي إن، سبأفون، يمن موبايل، واي). ويتكون مجتمع الدراسة من (356) عنصراً في أربع إدارات، وهي: إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت. وتم جمع المعلومات عن مجتمع الدراسة من خلال النزول الميداني، والرجوع إلى المختصين في إدارة الموارد البشرية، ومواقع Web الخاصة بشركات الاتصالات ووزارة الاتصالات، وكتاب الإحصاء السنوي الصادر عن الجهاز المركزي للإحصاء. وبحسب الحصر الشامل، فإن العينة المستهدفة تساوي مجتمع الدراسة في المراكز الرئيسية لشركات الاتصالات الموجودة في العاصمة صنعاء، وتم جمع البيانات من العينة من خلال أسلوبين، هما: 1) الأسلوب التقليدي، ومن خلاله تم النزول الميداني إلى الشركات لتوزيع الاستبانة واستردادها. 2) الأسلوب الإلكتروني.

2.10 تطوير أداة الدراسة

اعتمدت الدراسة الحالية الاستبانة أداة لجمع البيانات، وتم تطوير أداة الدراسة Instrument Development من خلال استخدام نهج نظري يقوم على تطوير فقرات الضوابط الأمنية التي حددها كلٌ من: (Hayale & Abu-Khadra, 2006; Riad, 2009; Schuessler, 2009)، وتطوير قائمة المخاطر التي حددها (Loch et al., 1992; Whitman, 2004; Abu-Musa, 2006; Schuessler, 2009; Riad, 2009; Hayale & Abu-Khadra, 2008؛ زويلف، 2009)، وتطوير فقرات أمن المعلومات التي حددها كلٌ من: (Chang & Wang, 2011; Al-Ghananeem et al., 2014; Seno et al., 2015)، وذلك بعد تحديد فقرات الاستبانة الذي تم بناءً على الدراسات السابقة والنظريات العلمية والدراسة الاستطلاعية، وقد تم تطوير أداة الدراسة من خلال تقييم فقرات الاستبانة، واستخدام فقرات مختصرة وموجزة، وفحص الاستبانة من قبل الخبراء المختصين، وإجراء دراسة استطلاعية؛ للتحقق من ثبات فقرات الاستبانة، واختبار صدق أداة الدراسة وثباتها.

3.10 مقاييس المتغيرات

تم قياس المتغير التابع (أمن نظم المعلومات المحاسبية)، وقياس المتغير المستقل (مخاطر تكنولوجيا المعلومات)، وقياس المتغير الوسيط (الضوابط الأمنية) من خلال المؤشرات التي تعكس واقع تلك المتغيرات في شركات الاتصالات، حيث تم تطوير الفقرات المتعلقة بقياس المتغيرات الواردة في الدراسات السابقة من خلال إعادة صياغتها أو تعديلها. وقد تم استخدام (84) فقرة في هذه الدراسة مقسمة بالتساوي بين المتغيرات الثلاثة، وقد استخدمت الدراسة الحالية مقياس ليكرت السباعي، حيث تشير (7) إلى "موافق بشدة" وهي تعني أن مستوى المتغير التابع أو المستقل أو الوسيط في شركات الاتصالات مرتفع جداً، وتشير (6) إلى "مرتفع"، وتشير (5) إلى "مرتفع إلى حدٍ ما"، وتشير (4) إلى "متوسط"، وتشير (3) إلى "منخفض إلى حدٍ ما"، وتشير (2) إلى "منخفض"، وتشير (1) إلى "غير موافق بشدة"

وهي تعني أن مستوى المتغير التابع أو المستقل أو الوسيط في شركات الاتصالات منخفض جداً (Tarmidi, 2013; Schuessler, 2009).

4.10 نسبة الاستجابة

تم توزيع الاستبانات على إدارات: تكنولوجيا المعلومات، والتدقيق الفني، والرقابة والتحكم، وتشغيل الشبكة والإنترنت وفق منتسبيها المعنيين في المراكز الرئيسية لشركات الاتصالات، وعددها (356) استبانة. وقد تم استرداد (226) استبانة، وبلغ عدد الاستبانات غير المستردة (130) استبانة، وتم استبعاد (8) استبانات لأن نسبة البيانات غير المكتملة فيها تصل إلى أكثر من 50%. وبذلك يصل عدد الاستبانات القابلة للتحليل إلى (218) استبانة ونسبة الاستجابة إلى 61%، وهي نسبة مناسبة.

5.10 الأساليب الإحصائية المستخدمة في تحليل البيانات

استخدمت الدراسة الحالية طريقة المربعات الصغرى الجزئية (PLS) الإصدار SmartPLS v.3.2.8، و SPSS v.25 في تقييم نموذج البحث Assessment of Study Model على مرحلتين: تتمثل المرحلة الأولى في تقييم النموذج القياسي Measurement Model، وعندما يحقق النموذج القياسي المعايير المطلوبة، يتم الانتقال إلى المرحلة الثانية المتمثلة في تقييم النموذج البنائي Hair Structural Model) (et al., 2019: 11. وسيتم توضيح هذه الأساليب على النحو الآتي:

أولاً: تقييم النموذج القياسي

هذا النموذج يحدد العلاقة بين المتغيرات الكامنة والفقرات، والعلاقة السببية بين المتغيرات الكامنة وفقراتها يمكن وصفها بالانعكاسية أو التكوينية، ويعتبر نموذج القياس الانعكاسي هو النموذج الملائم للدراسة الحالية، حيث إن قياس المتغيرات قد تم انعكاساً من خلال أبعادها، وقياس الأبعاد تم انعكاساً من خلال المؤشرات أو ما يسمى الفقرات (Hair et al., 2019: 11).

وتم تقييم نموذج القياس الانعكاسي من خلال استخدام المقاييس الإحصائية، كالتشبع الخارجي؛ لتقييم ثبات المؤشر، واستخدام الثبات المركب أو الكلي (CR)، وألفا كرونباخ (α)؛ لتقييم ثبات الاتساق الداخلي للأبعاد، واستخدام متوسط التباين المفسر (AVE)؛ لتقييم صدق التقارب، واستخدام طريقة التشبعات المتقاطعة، وطريقة نسبة أحادية وتغاير السمة (HTMT)؛ لتقييم صدق التمايز. ويمكن تلخيص المعايير المتعلقة بتقييم النموذج القياسي الانعكاسي كالآتي:

الجدول (1)

ملخص معايير تقييم النموذج القياسي الانعكاسي

تقييم	المعيار	المبادئ التوجيهية	المرجع
ثبات المؤشر	تشبع الفقرة	التشبع ≥ 0.708	(Chin, 1998)
الاتساق الداخلي	الثبات المركب (CR)	0.70 كحد أدنى (أو 0.60 في البحث الاستكشافي) 0.95 كحد أقصى والثبات الحقيقي للبُعد بين قيمة (CR) وقيمة (α)	(Hair et al., 2019)
	ألفا كرونباخ (α)	قيم (CR) نفسها، إلا أن (α) أقل دقة من الثبات المركب	(Hair et al., 2017)
صدق التقارب	متوسط التباين المفسر (AVE)	0.50 ≤ AVE	(Hair et al., 2019)
صدق التمايز	طريقة التشبعات المتقاطعة	تشبع الفقرة > تشبعاتها المتقاطعة مع الأبعاد الأخرى	(Chin, 1998)
	طريقة HTMT	0.85≥HTMT (أو 0.90 في البحث الاستكشافي)	(Hair et al., 2019)

ثانياً: تقييم النموذج البنائي

بعد التأكد من أن المقاييس تتسم بالصدق والثبات، يتم الانتقال إلى المرحلة الثانية المتمثلة في تقييم النموذج البنائي، ويسمى النموذج الداخلي Inner Model، ويهدف تقييم النموذج

البنائي إلى اختبار مستوى الترابط والعلاقة فيما بين المتغيرات الكامنة (Hair et al., 2017: 202).

الجدول (2)
ملخص معايير تقييم النموذج البنائي

المعيار	المبادئ التوجيهية	المرجع
معامل التحديد (R^2)	0.19 منخفض 0.33 متوسط 0.67 مرتفع	(Chin, 1998)
حجم الأثر (f^2) معيار Cohen	0.02 منخفض 0.15 متوسط 0.35 مرتفع	(Cohen, 1988)
ملاءمة التنبؤ (Q^2)	$0 < Q^2$	(Chin, 1998)
حجم الأثر (q^2)	0.02 منخفض 0.15 متوسط 0.35 مرتفع	(Hair et al., 2017) (Hair et al., 2019)
معامل المسار (β)	معامل المسار بين المتغيرين: القيم القريبة من (+1) علاقة إيجابية قوية والقيم القريبة من (−1) علاقة سلبية قوية، والقيم القريبة من (0) علاقة ضعيفة. العلاقة الجبرية يجب أن تكون متوافقة إحصائياً مع العلاقة الفرضية نظرياً. كل معامل مسار لا بد له من أن يكون ذا دلالة إحصائية ($t \geq 1.65$ و$p \leq 0.05$).	(Hair et al., 2017)

طرق اختبار المتغير الوسيط: توجد أكثر من طريقة لتحليل نموذج الوسيط (دلالة الوسيط)، وأبرزها:

طريقة Baron and Kenny (Baron and Kenny, 1986)، واختبار Sobel (Sobel, 1982)، وطريقة Bootstrapping (Preacher and Hayes, 2008). وقد اعتمدت الدراسة الحالية في اختبار المتغير الوسيط (الضوابط الأمنية) على طريقة Bootstrapping؛ لأنها تتلافى القصور في الطرق السابقة، وتُحدد تأثيرات الوساطة بشكل أدق.

11. نتائج الدراسة

1.11 تقييم النموذج

تم تقييم نموذج الدراسة الحالية وتحليل بياناتها باستخدام حزمة برامج المربعات الصغرى الجزئية SmartPLS v.3.2.8، وذلك على مرحلتين: المرحلة الأولى تقييم النموذج القياسي (النموذج الخارجي). والمرحلة الثانية تقييم النموذج البنائي (النموذج الداخلي) (Hair et al., 2019: 11). وتركز هذه الدراسة على فرضية المتغير الوسيط، وهي فرضية رئيسية لها فرضيتان فرعيتان.

1.1.11 تقييم النموذج القياسي الانعكاسي لمتغيرات الدراسة وأبعادها

تم سابقاً توضيح أن هذه الدراسة تصف العلاقة بين المتغيرات والفقرات بأنها انعكاسية، حيث تم قياس المتغيرات من خلال الأبعاد، وتم قياس الأبعاد من خلال المؤشرات (الفقرات).

وقد أشارت نتائج تقييم النموذج القياسي الانعكاسي لمتغيرات الدراسة وأبعادها إلى الآتي:

- **ثبات المؤشر (أبعاد الدراسة):** يتضح من الجدول (3) أن تشبع جميع قيم المؤشرات لأمن نظم المعلومات المحاسبية،

والضوابط الأمنية، ومخاطر تكنولوجيا المعلومات جاء أكبر من (0.708)؛ مما يشير إلى وجود ثبات عالٍ لأبعاد الدراسة وفقاً لـ (Hair et al., 2017:142).

- **ثبات الاتساق الداخلي (متغيرات الدراسة):** تشير النتائج في الجدول (3) إلى أن جميع قيم الثبات المركب (CR) وقيم ألفا كرونباخ (α) أعلى من (0.70) وأقل من (0.95)، ويشير هذا إلى أن قيم الاتساق الداخلي لجميع المتغيرات ذات ثبات عالٍ.
- **صدق التقارب (متغيرات الدراسة):** يظهر في الجدول (3) أن جميع قيم متوسط التباين المفسر (AVE) أكبر من (0.50)، وهذا يدل على وجود تقارب بين كل متغير وأبعاده.

الجدول (3)

تقييم ثبات المؤشر، والاتساق الداخلي، وصدق التقارب

(المتغيرات)	الأبعاد	التشبع	ثبات المؤشر	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
أمن نظم المعلومات المحاسبية	السرية	0.901	0.812	0.899	0.937	0.832
	السلامة	0.927	0.859			
	التوافر	0.907	0.823			
مخاطر تكنولوجيا المعلومات	مخاطر السرية	0.897	0.805	0.909	0.936	0.785
	مخاطر السلامة	0.861	0.741			
	مخاطر التوافر	0.895	0.801			
	المخاطر المشتركة	0.891	0.794			
الضوابط الأمنية	الضوابط التقنية	0.922	0.850	0.810	0.913	0.840
	الضوابط الإدارية	0.911	0.830			

– **صدق التمايز (متغيرات الدراسة):** يلاحظ من الجدول (4) أن كل قيم (HTMT) في كل متغير جاءت أقل من (0.85)، وهذا يشير إلى صدق تمايز المتغيرات، وأنه لا يوجد ارتباط عالٍ بين المتغير الواحد وبقية المتغيرات، وأن المتغير الواحد مختلف عن بقية المتغيرات الأخرى.

الجدول (4)

تقييم صدق تمايز المتغيرات باستخدام طريقة (HTMT)

المتغيرات	الضوابط الأمنية	مخاطر تكنولوجيا المعلومات	أمن نظم المعلومات المحاسبية
الضوابط الأمنية			
مخاطر تكنولوجيا المعلومات	0.516		
أمن نظم المعلومات المحاسبية	00.78	0.524	

2.1.11 تقييم النموذج البنائي للمتغيرات

أكدت نتائج تقييم النموذج القياسي الانعكاسي صدق وثبات أداة القياس. وفي هذه المرحلة، سوف يتم تقييم النموذج البنائي، الذي يتضمن فحص القدرة التنبؤية والتفسيرية لنموذج الدراسة، وتحليل اتجاه علاقة الأثر، وذلك على النحو الآتي:

معامل التحديد (R^2)

تم استخدام خوارزمية (PLS) في تقييم معامل التحديد (R^2)، حيث أظهرت النتائج في الجدول (5) أن معامل التحديد لأمن نظم المعلومات المحاسبية بلغ (0.484)، وهذا يشير إلى أن مخاطر تكنولوجيا المعلومات والضوابط الأمنية تفسر ما نسبته

48.4% من التباين في أمن نظم المعلومات المحاسبية، وهي نسبة متوسطة؛ لأنها أكبر من (0.33) وأقل من (0.67).

الجدول (5)
تقييم معامل التحديد

المتغير التابع	معامل التحديد (R^2)	النتيجة
أمن نظم المعلومات المحاسبية	0.484	متوسطة

حجم الأثر (f^2)

يبين الجدول (6) أن حجم أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية جاء بمقدار (0.499)، ويعتبر حجم الأثر هذا مرتفعاً، لأنه أكبر من (0.35)، بينما جاء حجم أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية بمقدار (0.077)، ويُعد حجم الأثر هذا منخفضاً لأنه أكبر من (0.02) وأقل من (0.15). والجدول (6) يوضح نتائج تقييم حجم الأثر.

الجدول (6)
تقييم حجم الأثر (f^2)

مسار المتغيرات	قيمة (f^2)	التقدير
الضوابط الأمنية –> أمن نظم المعلومات المحاسبية	0.499	مرتفع
مخاطر تكنولوجيا المعلومات –> أمن نظم المعلومات المحاسبية	0.077	منخفض

ملاءمة التنبؤ (Q^2)

الجدول (7) يوضح نتائج تقييم ملاءمة النموذج للتنبؤ.

الجدول (7)
تقييم ملاءمة التنبؤ (Q^2) على مستوى المتغير التابع

المتغير	The sum of the squared observations (SSO) مجموع مربع المشاهدات	The sum of the squared prediction errors (SSE) مجموع مربع أخطاء التنبؤ	Q^2 (=1-SSE/SSO) ملاءمة التنبؤ	التقدير
أمن نظم المعلومات المحاسبية	654.000	410.903	0.372	عالٍ

يتضح من الجدول (7) أن قيمة ملاءمة التنبؤ (Q^2) لأمن نظم المعلومات المحاسبية تساوي (0.372)، وهي قيمة عالية، لأنها أكبر من (0.35). وبالتالي يمكن القول إن النموذج لديه دقة تنبؤ عالية بمتغير أمن نظم المعلومات المحاسبية. وبشكل عام، يتمتع النموذج بدقة عالية وملاءمة من حيث التنبؤ.

حجم الأثر (q^2)

الجدول (8) يظهر نتائج تقييم حجم الأثر (q^2).

الجدول (8)

تقييم حجم الأثر (q^2)

المتغير	مدرج ضمن النموذج	مستبعد من النموذج	الفرق بين المدرج والمستبعد	1–المدرج	(q^2)	التقدير
الضوابط الأمنية	0.372	0.182	0.190	0.628	0.3025	متوسط
مخاطر تكنولوجيا المعلومات	0.372	0.346	0.026	0.628	0.0414	منخفض

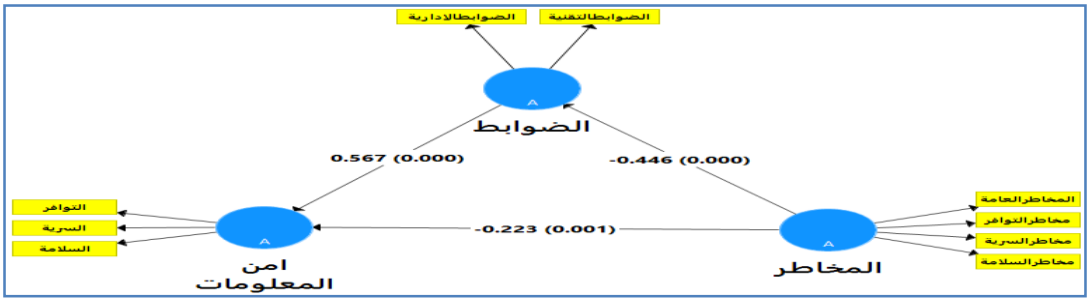
من الجدول (8)، يتضح أن قيمة حجم الأثر (q^2) لمتغير الضوابط الأمنية تساوي (0.3025)، وهي قيمة متوسطة؛ كونها أكبر من (0.15) وأقل من (0.35)، وتشير إلى أن الضوابط الأمنية لها حجم أثر متوسط في أمن نظم المعلومات المحاسبية، بينما كانت قيمة حجم الأثر (q^2) لمخاطر تكنولوجيا المعلومات تساوي (0.0414)، وهي قيمة منخفضة؛ كونها أكبر من (0.02) وأصغر من (0.15).

12. تقييم معاملات المسار – اختبار الفرضيات

1.12 اختبار الفرضية الرئيسية، وهي تنص على ما يلي:

هناك أثر سلبي لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية في شركات الاتصالات العاملة في الجمهورية اليمنية.

ويوضح الشكل (3) نتائج تقييم معاملات المسار بين المتغيرات ومستوى الدلالة.



الشكل (3)

تقييم معاملات المسار ومستوى الدلالة

يظهر الشكل (3) قيم معاملات المسار ومستوى الدلالة بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية من خلال توسط الضوابط الأمنية. ويتضح من هذا الشكل عدم ظهور معامل التحديد (R^2) لكل من الضوابط الأمنية وأمن نظم المعلومات المحاسبية. وقد تم تحديد وتوضيح معامل التحديد سابقاً، ويوضح الجدول (9) نتائج اختبار الفرضية الرئيسية.

الجدول (9)
اختبار الفرضية الرئيسية (الأثر المباشر وغير المباشر)

المسـار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
مخاطر تكنولوجيا المعلومات –> الضوابط الأمنية (a)	-0.446	0.060	7.480	0.000
الضوابط الأمنية –> أمن نظم المعلومات المحاسبية (b)	0.567	0.076	7.509	0.000
الأثر المباشر				
مخاطر تكنولوجيا المعلومات –> أمن نظم المعلومات المحاسبية (c')	**-0.223**	0.066	3.358	0.001
الأثر غير المباشر				
مخاطر تكنولوجيا المعلومات –> الضوابط الأمنية –> أمن نظم المعلومات المحاسبية (a*b)	**-0.253**	0.04	6.368	0.000

وقد تم استخدام طريقة Bootstrapping في قياس وساطة الضوابط الأمنية (التوسط أو عدم التوسط) وتحديد نوع وساطة الضوابط الأمنية (هل هو جزئي أم كلي) (Hadi et al., 2016: 66)، وذلك وفقاً للخطوات الآتية:

– قياس التوسط من خلال الأثر غير المباشر (a*b)

إذا كان الأثر غير المباشر (a*b) للمتغير المستقل في المتغير التابع دالاً إحصائياً من خلال المتغير الوسيط، فإن هناك وساطة، وإذا كان الأثر غير المباشر (a*b) غير دال إحصائياً فيشير ذلك إلى عدم الوساطة (Hair et al., 2017: 243). وكما يتضح من الجدول (9)، فإن الأثر غير المباشر (a*b) لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية دال إحصائياً من خلال الضوابط الأمنية، حيث جاءت قيمة معامل المسار (β=-0.253)، وقيمة (t=6.368)، وهي دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يدل على أن الضوابط الأمنية تتوسط العلاقة بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية، ويمر الأثر غير المباشر أو ينتقل من مخاطر تكنولوجيا المعلومات إلى أمن نظم المعلومات المحاسبية عبر الضوابط الأمنية.

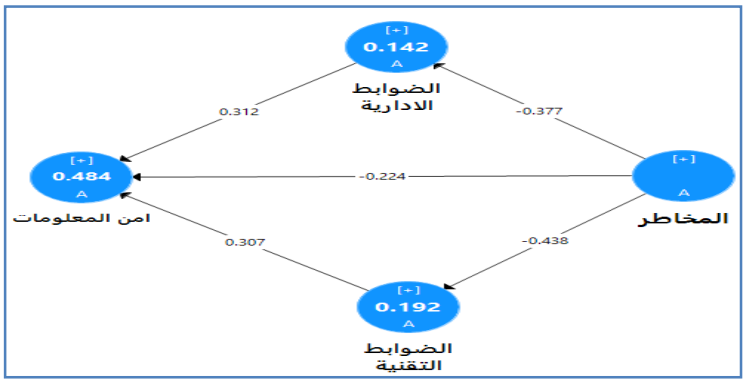
– تحديد نوع الوساطة من خلال الأثر المباشر (c')

إذا كان الأثر المباشر (c') دالاً إحصائياً للمتغير المستقل في المتغير التابع، فإن التوسط جزئي، وإذا كان الأثر المباشر (c') غير دال إحصائياً، فإن التوسط كلي (Hair et al., 2017: 243). ويتضح من الجدول (9) أن الأثر المباشر (c') دال إحصائياً لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات، حيث جاءت قيمة معامل المسار (β=-0.223)، وقيمة (t=3.358)، وهي دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يشير إلى أن وساطة الضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية هي وساطة جزئية.

2.12 تتفرع من الفرضية الرئيسية فرضيتان فرعيتان، تتمثلان في الآتي:

- هناك أثر سلبي ذو دلالة إحصائية لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط التقنية في شركات الاتصالات العاملة في اليمن.
- هماك أثر ذو دلالة إحصائية لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الإدارية في شركات الاتصالات العاملة في اليمن.

ويوضح الشكل (4) نتائج تقييم معاملات المسار.



الشكل (4)

تقييم معاملات مسار أبعاد الضوابط الأمنية

يظهر الشكل (4) قيم معاملات المسار بين المخاطر وأمن المعلومات من خلال الضوابط التقنية والضوابط الإدارية. ويتضح من هذا الشكل أن قيمة معامل التحديد (R^2) للضوابط التقنية (0.192)، وهذا يشير إلى أن المخاطر تُفسر ما نسبته 19.2% من التباين في الضوابط التقنية، وأن قيمة معامل التحديد (R^2) للضوابط الإدارية (0.142)، وهذا يشير إلى أن المخاطر تُفسر ما نسبته 14.2% من التباين في الضوابط الإدارية. ويظهر في هذا الشكل أن قيمة معامل التحديد (R^2) لأمن المعلومات جاءت (0.484)، وهذا يشير إلى أن المخاطر والضوابط التقنية والإدارية تُفسر ما نسبته 48.4% من التباين في أمن المعلومات.

ويظهر الجدول (10) نتائج اختبار الفرضيتين الفرعيتين للفرضية الرئيسية.

الجدول (10)

نتائج اختبار الفرضيات الفرعية للفرضية الرئيسية

المسار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
مخاطر تكنولوجيا المعلومات -> الضوابط الإدارية (a_1)	-0.377	0.070	5.374	0.000
مخاطر تكنولوجيا المعلومات -> الضوابط التقنية (a_2)	-0.438	0.058	7.541	0.000
الضوابط الإدارية -> أمن نظم المعلومات المحاسبية (b_1)	0.312	0.067	4.651	0.000
الضوابط التقنية -> أمن نظم المعلومات المحاسبية (b_2)	0.307	0.101	3.030	0.003
الأثر المباشر				
مخاطر تكنولوجيا المعلومات -> أمن نظم المعلومات المحاسبية (c')	**-0.224**	0.069	3.233	0.001
الأثر غير المباشر				
مخاطر تكنولوجيا المعلومات -> الضوابط الأمنية -> أمن نظم المعلومات المحاسبية (a* b)	**-0.252**	0.044	5.728	0.000
مخاطر تكنولوجيا المعلومات -> الضوابط الإدارية -> أمن نظم المعلومات المحاسبية (a_1*b_1)	-0.118	0.036	3.303	0.001
مخاطر تكنولوجيا المعلومات -> الضوابط التقنية -> أمن نظم المعلومات المحاسبية (a_2*b_2)	-0.134	0.047	2.860	0.004

أ) قياس وساطة الضوابط الإدارية وتحديد نوع الوساطة

1) يتم قياس الوساطة من خلال الأثر غير المباشر (a_1*b_1)، حيث تشير النتائج في الجدول (10) إلى أن الأثر غير المباشر (a_1*b_1) لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية دال إحصائياً من خلال الضوابط الإدارية؛ فقد جاءت قيمة معامل المسار (β=-0.118)، وقيمة (t=3.303)، وهي دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يدل على أن الضوابط الإدارية تتوسط مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية، ويمر الأثر غير المباشر أو ينتقل عبر الضوابط الإدارية من مخاطر تكنولوجيا المعلومات إلى أمن نظم المعلومات.
2) يتم تحديد نوع الوساطة من خلال الأثر المباشر (c'): إذ يتضح من الجدول (10) أن الأثر المباشر (c') لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية دال إحصائياً بعد توسط الضوابط الإدارية، حيث جاءت قيمة معامل المسار (β=-0.224)، وقيمة (t=3.233)، وهي دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يدل على أن الضوابط الإدارية تتوسط مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية توسطاً جزئياً.

ب) قياس وساطة الضوابط التقنية وتحديد نوع الوساطة

1) يتم قياس الوساطة من خلال الأثر غير المباشر (a_2*b_2)، حيث أظهرت نتائج الدراسة في الجدول (10) أن الأثر غير المباشر (a_2*b_2) لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية دال إحصائياً من خلال الضوابط التقنية؛ فقد جاءت قيمة معامل المسار (β=-0.134)، وقيمة (t=2.860) دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يدل على أن الضوابط التقنية تتوسط مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية، ويمر الأثر غير المباشر أو ينتقل عبر الضوابط التقنية من مخاطر تكنولوجيا المعلومات إلى أمن نظم المعلومات المحاسبية.
2) يتم تحديد نوع الوساطة من خلال الأثر المباشر (c'): إذ توضح النتائج في الجدول (10) أن الأثر المباشر (c') لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية دال إحصائياً بعد توسط الضوابط التقنية؛ فقد جاءت قيمة معامل المسار (β=-0.224)، وقيمة (t=3.233)، وهي دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يدل على أن الضوابط التقنية تتوسط مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية توسطاً جزئياً.

13. مناقشة النتائج

1.13 أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية

من أجل تحقيق أهداف الدراسة، تم فحص معاملات المسار في SmartPLS كما هو موضح في الجدول (10). وقد أشارت نتائج الدراسة الحالية إلى أن وساطة الضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية هي وساطة جزئية، وأن مخاطر تكنولوجيا المعلومات لها تأثير سلبي غير مباشر في أمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن. وتعزز هذه النتيجة نظرية أمن المعلومات التي تنص على أن الدافع وراء كل المحاولات التي تقوم بها المنظمة لتأمين المعلومات من المخاطر هو إيجاد الموارد التي يمكن استخدامها لاحقاً في تحسين الأداء التنظيمي. وتتعرض المعلومات للمخاطر ما لم تنفذ ضوابط كافية (Horne et al., 2016: 2). كذلك تفترض نظرية الردع العام (GDT) إجراءات عامة تقلل من مخاطر النظم بشكل مباشر أو غير مباشر من خلال استخدام التدابير المضادة (Straub & Welke, 1998: 441). وقد أشارت دراسة (Schuessler, 2009: 63) إلى أن الضوابط الأمنية يمكنها الحد من المخاطر، وليس منع جميع المخاطر. وتؤكد الحوادث الأمنية التي وقعت مؤخراً أن الضوابط الأمنية تحد من المخاطر، ولا تمنعها (Norman et al., 2017, 2)، وقد عملت على الحد من الهجمات الخبيثة التي استهدفت المؤسسات في جميع أنحاء العالم وتسببت في تعليق العمل في وزارة الداخلية الروسية، ووزارة الاتصالات الإسبانية، والخدمات الصحية البريطانية (Kaspersky, 2017: 14-18).

وبناءً على ما توصلت إليه نتائج الدراسة الحالية، واتفاقها مع نظرية أمن المعلومات، ونظرية الردع العام، والحوادث الأمنية التي وقعت في منظمات الأعمال، فهي تؤكد أن الضوابط الأمنية تحافظ على أمن نظم المعلومات من المخاطر، وأن الضوابط الأمنية يمكنها الحد من المخاطر والتخفيف من آثارها السلبية

على نظم المعلومات في الشركات، ولكن لا يمكنها منع جميع المخاطر. كذلك أشارت نتائج الدراسة الحالية إلى أن وساطة الضوابط الأمنية هي وساطة جزئية، وليست كلية، وأن المخاطر لها تأثير سلبي غير مباشر في أمن نظم المعلومات المحاسبية، حيث يمر أو ينتقل جزء من الأثر عبر الضوابط الأمنية من المخاطر إلى أمن نظم المعلومات المحاسبية. ويلاحظ أن الأثر السلبي الكلي للمخاطر في أمن نظم المعلومات قبل التوسط جاء بنسبة (47.6%)، وأن الأثر السلبي غير المباشر للمخاطر في أمن المعلومات بعد التوسط كان (25.3%)، وهذه النتيجة تؤكد أن الضوابط الأمنية تحد من المخاطر، ولا تمنع جميع المخاطر، وأن حدوث مخاطر مع وجود ضوابط أمنية في منظمات الأعمال هو بسبب استغلال الثغرات في أنظمة الحماية، كالثغرات في النظام، والشبكة، وآليات التحقق من الهوية، والتحكم بالوصول، وممارسة أساليب الخداع أو الانتحال من قبل المهاجمين بغرض الوصول إلى أنظمة المعلومات. ويترتب على الوصول إلى النظام كشف المعلومات أو تعديلها أو إتلافها، ويؤدي هذا إلى إلحاق أضرار بالمنظمة. والواقع يؤكد صحة هذا التفسير، حيث تعرضت بعض الشركات حول العالم لاختراق أنظمتها المعلوماتية على الرغم من وجود أنظمة حماية. وفي المقابل، استطاعت أنظمة الحماية في بعض الشركات صد بعض الهجمات، وتمكنت أخرى من خفض آثارها السلبية، لذلك نجد أن الضوابط الأمنية تحد من المخاطر ولكنها لا تستطيع أن تمنع جميع المخاطر، (التوسط جزئي وليس كلياً)، وهذا ما أكدته نتيجة الدراسة الحالية.

1.1.13 أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط التقنية

من أجل تحقيق الهدف الفرعي الأول للدراسة، تم فحص معاملات المسار في SmartPLS كما هو موضح في الجدول (10)، حيث توصلت الدراسة الحالية إلى أن وساطة الضوابط التقنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية هي وساطة جزئية، وأن مخاطر تكنولوجيا المعلومات لها تأثير سلبي غير مباشر في أمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن. وتعزز هذه النتيجة نظرية الردع العام (GDT) التي تم التوسع في وجهات النظر المفاهيمية لها لتشمل مصادر التهديدات الأخرى، مثل التهديدات غير البشرية (الكوارث الطبيعية، والإخفاق التقني). ويساعد هذا التوسع في التخطيط الوقائي للحد من المخاطر الأمنية (Schuessler, 2009: 62).

ويلاحظ أن نتيجة الدراسة الحالية تتفق مع نظرية الردع العام في أن الضوابط التقنية تحافظ على أمن نظم المعلومات من المخاطر، حيث أشارت النتائج إلى أن وساطة الضوابط التقنية هي وساطة جزئية وليست كلية، وأن المخاطر لها تأثير سلبي غير مباشر في أمن نظم المعلومات المحاسبية (يمر جزء من الأثر أو ينتقل عبر الضوابط التقنية من المخاطر إلى أمن نظم المعلومات المحاسبية). ويفسر هذا أن الضوابط التقنية تحد من المخاطر، وتخفف من آثارها السلبية، وتحافظ على سرية المعلومات وسلامتها، وتوافر أنظمة المعلومات والخدمات، ولكن لا يمكنها منع جميع المخاطر.

وما يفسر وقوع حوادث أمنية على الرغم من وجود ضوابط تقنية في منظمات الأعمال هو استغلال الثغرات الأمنية؛ للوصول إلى أنظمة المعلومات، والحصول على المعلومات الحساسة، ثم فتح أبواب خلفية؛ للوصول عن بُعد إلى النظام في وقت لاحق. وفي الواقع، نجد أن بعض الشركات تم اختراق أنظمتها، والبعض الآخر تمكنت من صد بعض الهجمات، وهذا يؤكد أن الضوابط التقنية تحد من المخاطر، ولا تستطيع منع جميع المخاطر (وساطة الضوابط التقنية وساطة جزئية وليست وساطة كلية)، وهذا ما أكدته نتيجة الدراسة الحالية؛ فتطبيق الضوابط التقنية الملاءمة والكافية يخفض من حجم المخاطر بشكل كبير، ويحافظ على سرية المعلومات، وسلامتها، وتوافرها.

2.1.13 أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الإدارية

من أجل تحقيق الهدف الفرعي الثاني للدراسة، تم فحص معاملات المسار في SmartPLS كما هو موضح في الجدول (10)، حيث أشارت نتائج الدراسة الحالية إلى أن وساطة الضوابط الإدارية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية هي وساطة جزئية، وأن مخاطر تكنولوجيا المعلومات لها تأثير سلبي غير مباشر في أمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن. وتعزز هذه

النتيجة نظرية الردع العام (GDT)، حيث يفترض النموذج الموسع للنظرية أن وعي المستخدم بالتدابير المضادة يؤثر بشكل مباشر على إدراك المستخدم للعقوبة التي لها تأثير مباشر على نوايا إساءة استخدام نظم المعلومات، كما تؤثر التدابير المضادة بشكل غير مباشر على نوايا إساءة استخدام نظم المعلومات، وذلك من خلال إدراك المستخدم للعقوبة (D'Arcy et al., 2008: 2). كذلك فإن زيادة الوعي بين الموظفين بمخاطر الاصطياد الإلكتروني تقلل من تأثير الحوادث الأمنية.

وتشير نتيجة الدراسة الحالية إلى أن مخاطر تكنولوجيا المعلومات لها تأثير سلبي غير مباشر في أمن نظم المعلومات المحاسبية بعد وساطة الضوابط الإدارية، وهذا يدل على أن الضوابط الإدارية تحد من المخاطر. وتخفف من آثارها السلبية، وتحافظ على الأهداف الأمنية (السرية والسلامة والتوافر) من المخاطر، وأظهرت النتائج أن وساطة الضوابط الإدارية هي جزئية، وليست وساطة كلية (أي يمر جزء من الأثر عبر الضوابط الإدارية أو ينتقل من المخاطر إلى أمن نظم المعلومات المحاسبية)، وهذا يدل على أن الضوابط الإدارية تحد من المخاطر، ولا تمنع جميع المخاطر. وما يفسر وقوع حوادث أمنية على الرغم من وجود ضوابط إدارية في منظمات الأعمال هو استغلال الثغرات الأمنية في الضوابط الإدارية من قبل المهاجمين، وهي تُعد الأخطر على أنظمة المعلومات، حيث يستخدم المهاجمون أساليب الهندسة الاجتماعية والاصطياد الإلكتروني والحيل أو انتحال وخداع مستخدمي أنظمة المعلومات. ويعتبر العنصر البشري الحلقة الأضعف في أمن المعلومات، وكثير من الهجمات واختراق الأنظمة ناجم عن ضعف برامج التوعية والتدريب في مجال أمن المعلومات والإهمال واللامبالاة، وهذا يؤكد أن الضوابط الإدارية تحد من المخاطر وتخفف من آثارها السلبية ولا تمنعها (أي أن توسط الضوابط الإدارية هو توسط جزئي وليس توسطاً كلياً)، وهذا ما أكدته نتيجة الدراسة الحالية. وهذا يمكن منظمات الأعمال من خفض حجم هذه المخاطر إلى أدنى حد ممكن، وذلك من خلال تطبيق الضوابط الإدارية على نطاق واسع وبشكل فاعل، وإلزام المستخدمين بتطبيق السياسات الأمنية، ونشر الوعي بأمن المعلومات بين المستخدمين، واختبار فاعلية الضوابط الأمنية (التدقيق)، والامتثال للقوانين واللوائح.

14. الاستنتاجات

بناءً على نتائج التحليل الإحصائي لاختبار الفرضيات ومناقشتها، فقد خلصت الدراسة الحالية إلى العديد من الاستنتاجات، وهي على النحو الآتي:

- هناك اهتمام واسع بأمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن، وفي مقدمة اهتمامات تلك الشركات سرية المعلومات، تليها سلامة المعلومات والأنظمة، ثم توافر الأنظمة والخدمات.
- تستخدم شركات الاتصالات العاملة في اليمن الضوابط الأمنية على نطاق واسع (الضوابط التقنية، تليها الضوابط الإدارية) في حماية سرية المعلومات، وسلامتها، وتوافر أنظمة المعلومات المحاسبية من المخاطر.
- يلاحظ أن أداء الضوابط الأمنية المنخفض ناجم عن الضوابط الإدارية، تليها الضوابط التقنية.
- مصدر التأثير السلبي المباشر في أمن نظم المعلومات المحاسبية ناجم عن مخاطر السرية، تليها مخاطر التوافر؛ بمعنى أن توسع عمليات الاتصال وزيادة الترابط بين أنظمة شركات الاتصالات والمشتركين (العملاء) وتحقق نمو في إجراء المعاملات عبر الإنترنت أدى إلى زيادة المخاطر والتأثير في أمن المعلومات.
- مصدر التأثير السلبي المباشر في أمن نظم المعلومات المحاسبية يعود إلى المؤشرات المرتبطة بمخاطر السرية المتمثلة في هجمات التنصت، وكسر كلمة المرور، والوصول غير المصرح به، والأفعال المتعمدة، والاصطياد الإلكتروني والاجتماعي.
- مصدر التأثير السلبي المباشر في أمن نظم المعلومات المحاسبية يعود إلى المؤشرات المرتبطة بمخاطر التوافر المتمثلة في هجمات الحرمان من الخدمة، والكوارث الطبيعية والسياسية، وأعطال الأجهزة الفنية.
- يتضح أن مصدر التأثير الإيجابي في أمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن يعود إلى الضوابط التقنية، تليها الضوابط الإدارية.
- يتضح أن مصدر التأثير الإيجابي في أمن نظم المعلومات المحاسبية يعود إلى المؤشرات المرتبطة بالضوابط التقنية التي تشمل آليات التحقق من الهوية، والتحكم بالوصول، ومكافحة

البرامج الضارة، وحماية الشبكة، وأنظمة التشفير.

- يتضح أن مصدر التأثير الإيجابي في أمن نظم المعلومات المحاسبية يعود إلى المؤشرات المرتبطة بالضوابط الإدارية المتمثلة في التخطيط للطوارئ، وإجراءات التدقيق، وسياسة أمن المعلومات، والتوعية والتدريب على أمن المعلومات، والتدابير القانونية، كما أن نتائج الدراسة تؤكد أهمية رفع مستوى الوعي والإدراك بين مستخدمي تكنولوجيا المعلومات في مجال أمن المعلومات.
- نستنتج أن مصدر التأثير السلبي غير المباشر في أمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن ناتج عن مخاطر تكنولوجيا المعلومات، ويتضح أن وساطة الضوابط الأمنية هي وساطة جزئية، حيث ينتقل جزء من الأثر عبر الضوابط الأمنية من المخاطر إلى أمن المعلومات، ويرجع انتقال جزء من الأثر غير المباشر إلى الضوابط التقنية، تليها الضوابط الإدارية.
- نستنتج أن مصدر التأثير السلبي غير المباشر في أمن نظم المعلومات المحاسبية ناتج عن مخاطر تكنولوجيا المعلومات، ويتضح أن وساطة الضوابط التقنية هي وساطة جزئية، حيث ينتقل جزء من الأثر عبر الضوابط التقنية من المخاطر إلى أمن المعلومات، ويرجع انتقال جزء من الأثر غير المباشر إلى المؤشرات المرتبطة بالضوابط التقنية كآليات التحقق من الهوية، والتحكم بالوصول، ومكافحة البرامج الضارة، وحماية الشبكة، والتشفير.
- نستنتج أن مصدر التأثير السلبي غير المباشر في أمن نظم المعلومات المحاسبية ناتج عن مخاطر تكنولوجيا المعلومات، ويتضح أن وساطة الضوابط الإدارية هي وساطة جزئية، حيث ينتقل جزء من الأثر عبر الضوابط الإدارية من المخاطر إلى أمن المعلومات، ويرجع انتقال جزء من الأثر غير المباشر إلى المؤشرات المرتبطة بالضوابط الإدارية، كالتخطيط للطوارئ، وإجراءات التدقيق، وسياسة أمن المعلومات، والتوعية والتدريب بأمن المعلومات، والتدابير القانونية.

15. التوصيات

بناءً على الاستنتاجات التي تم التوصل إليها في شركات الاتصالات مجتمع الدراسة، يُمكن الخروج بأهم التوصيات التي تسهم في تحقيق أمن نظم المعلومات المحاسبية، حيث توصى الدراسة الحالية شركات الاتصالات العاملة في اليمن بالآتي:

- تعزيز أمن نظم المعلومات المحاسبية، ومواكبة التطورات المتسارعة للحفاظ على سرية المعلومات والأنظمة، وسلامتهما، وتوافرهما من مخاطر تكنولوجيا المعلومات، وإيلاء كل من السرية، والتوافر، والسلامة مزيداً من الاهتمام؛ لأنها الأكثر أهمية في قطاع الاتصالات.
- الاهتمام بالضوابط الأمنية وتنفيذها وتحديثها بشكل منتظم، مع التركيز على كل من الضوابط التقنية والضوابط الإدارية معاً بدلاً من التركيز على الضوابط التقنية وحدها، ويجب أن تعمل الضوابط التقنية والإدارية معاً لإيجاد بيئة آمنة.
- العمل على منع أو خفض مخاطر تكنولوجيا المعلومات إلى أدنى حد ممكن والحد من آثارها السلبية، وذلك من خلال تعزيز الضوابط الوقائية التي تمنع المخاطر، وتعزيز ضوابط الكشف في حال تجاوز الضوابط الوقائية، بالإضافة إلى تعزيز الضوابط التصحيحية في حال تجاوز ضوابط الكشف، وكذلك تعزيز الضوابط المكافئة أو البديلة (كالموقع البديل، والتعافي من الكوارث) في حال تجاوز الضوابط التصحيحية.
- يجب أن تعمل إدارات تكنولوجيا المعلومات في شركات الاتصالات على رفع أداء الضوابط الأمنية (الإدارية، والتقنية) من خلال معالجة جوانب الضعف والقصور في الضوابط الأمنية، والرقابة على تنفيذها، وتحديثها باستمرار، والامتثال للقوانين واللوائح، وذلك لخفض أثر مخاطر تكنولوجيا المعلومات (مخاطر السلامة والتوافر والسرية) في أمن نظم المعلومات المحاسبية.
- ضرورة اختبار الاختراق بشكل دوري؛ للتحقق من مدى وجود ثغرات أمنية في الأنظمة، والبرامج، والأجهزة، والشبكات، وإجراءات أمن النظام، والضوابط الداخلية، وتنفيذ الضوابط وتحديثها، وتكنولوجيا الاتصالات، بحيث تساعد هذه الاختبارات في معالجة الثغرات وجوانب القصور في الضوابط الأمنية، وخفض الأثر السلبي لمخاطر تكنولوجيا المعلومات.
- ضرورة فحص الضوابط التقنية؛ للتحقق من مدى وجود ثغرات أمنية أو قصور في تنفيذ آليات التحقق من الهوية، واستخدام تقنيات متقادمة، والتحكم بالوصول، ومكافحة البرامج الضارة، والاتصال الآمن للبيانات التي تنتقل عبر الشبكات، وأنظمة

التشفير، بحيث يساعد فحص هذه الضوابط في خفض الأثر السلبي للمخاطر المتعلقة بـ (السرية، والسلامة، والتوافر، والمخاطر المشتركة).

- ضرورة فحص الضوابط الإدارية، للتحقق من مدى وجود ثغرات أمنية في خطط الطوارئ، أو وجود قصور في نظام النسخ الاحتياطي، أو قصور في الجوانب التشريعية والتنظيمية المتعلقة بأمن المعلومات، والامتثال للقوانين واللوائح، وسد الثغرات في سياسة الأمن، واستخدام أساليب الهندسة الاجتماعية، وبرامج التوعية والتدريب على أمن المعلومات، بحيث يساعد فحص هذه الضوابط في حفض الأثر السلبي للمخاطر المتعلقة بـ (السرية، والسلامة، والتوافر، والمخاطر المشتركة).
- التأكيد على أهمية تنفيذ الضوابط التقنية، وتحديثها باستمرار، وتوظيف أحدث تقنيات الحماية لما لها من أثر إيجابي في تحقيق أمن نظم المعلومات، والتأكيد على أهمية تشفير بيانات الشركة الحساسة وخصوصية بيانات العملاء، والمصادقة على صحة مضمون الرسائل الواردة (استخدام التوقيع الرقمي)، والتحقق من هوية المُرسل والمصادقة عليها (استخدام الشهادات الرقمية).
- التأكيد على أهمية تنفيذ الضوابط الإدارية، وتحديثها باستمرار، وتوظيف الكوادر ذات المهارات العالية؛ لما له من أثر إيجابي في تحقيق أمن نظم المعلومات.
- ضرورة الاهتمام بالضوابط الأمنية (التقنية، والإدارية)، وتعزيز الدور الرقابي على مقدمي خدمات تكنولوجيا المعلومات، وتحسين أنشطة الاستجابة للحوادث الأمنية، والرد على الاختراقات الأمنية، بحيث يكون لهذه الضوابط دور إيجابي في تعزيز أمن نظم المعلومات وخفض الأثر السلبي لمخاطر تكنولوجيا المعلومات.
- تحسين الأمن الإلكتروني، واعتباره أولوية عليا، وتسريع تنفيذ المصادقة القوية متعددة العوامل (القياسات الحيوية، والبطاقات الذكية، وكلمة المرور)، وإيلاء التحكم بالوصول المادي والمنطقي قدراً كبيراً من الاهتمام. وينبغي تحديث مكافح البرامج الضارة تلقائياً وبشكل مستمر، واستخدام وتحديث الشبكات الخاصة الافتراضية والجدران النارية، واستخدام تقنيات التشفير للبيانات الحساسة، بحيث تساعد هذه التقنيات في خفض الأثر السلبي للمخاطر ورفع مستوى أمن المعلومات.
- مراقبة تطبيق سياسة الأمن، ونشر المبادئ التوجيهية فيما يتعلق بالاستخدام المقبول للنظام، والتوعية بأهمية أمن المعلومات والتدريب عليه، وتسجيل وتتبع الأنشطة غير العادية (عمليات التدقيق الداخلي والخارجي للنظام)، وتشديد العقوبات على المخالفين، بحيث تعمل هذه الإجراءات على خفض المخاطر ورفع مستوى الأمن.
- يتطلب الأمر من وزارة الاتصالات وتقنية المعلومات إنشاء مركز وطني لأمن المعلومات (فريق الاستجابة لطوارئ الحاسوب CERT) في الجمهورية اليمنية؛ وذلك بهدف الاستجابة لحوادث أمن المعلومات، والتعاون مع مراكز أمن المعلومات الدولية في احتواء الحوادث الأمنية وتجنبها في المستقبل، وتوفير بيئة معلوماتية آمنة.

يتطلب الأمر من وزارة الاتصالات وتقنية المعلومات إعداد مشروع قانون لمكافحة الجرائم الإلكترونية، وحماية البيانات الشخصية، وتقديم هذا المشروع للحكومة لمناقشته وإقراره.

المراجع

المراجع العربية

الربيدي، محمد علي، 2010، حماية المعلومات المحاسبية في ظل مخاطر التكنولوجيا للعمليات المصرفية الإلكترونية: دراسة ميدانية في البنوك العاملة في اليمن. ***مجلة كلية التجارة والاقتصاد***، المجلد 33، ص 1-45.

زويلف، أنغام محسن حسن، 2009، طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على شركات التأمين الأردنية. ***المجلة العربية للمحاسبة***، المجلد 12، العدد 1، ص 46-77.

العرود، شاهر فلاح، وشاكر، طلال حمدون، 2009، جودة تكنولوجيا المعلومات وأثرها في كفاءة التدقيق الداخلي في

الشركات الصناعية والخدمية المساهمة العامة الأردنية. ***المجلة الأردنية في إدارة الأعمال***، المجلد 5، العدد 4، ص 475-496.

العلوان، جعفر أحمد، 2022، أدوار وتحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي: دراسة حالة. ***المجلة الأردنية في إدارة الأعمال***، المجلد 18، العدد 3، ص 438-456.

المراجع العربية باللغة الإنجليزية

Al-Aroud, S.F., & Shaker, T.H. 2009. The Quality of Information Technology and Its Impact on the Efficiency of Internal Auditing in the Jordanian Public Shareholding Industrial and Service Companies. ***Jordan Journal of Business Administration***, 5 (4): 475-496.

Al-Rubaidi, M.A. 2010. Protecting Accounting Information in Light of Technology Risks for Electronic Banking Operations: A Field Study in Banks Operating in Yemen. ***Journal of the Faculty of Commerce and Economics***, 33: 1-45.

Alalwan, J.A. 2022. The Roles and Challenges of Cybersecurity Based on Artificial Intelligence: A Case Study. ***Jordan Journal of Business Administration***, 18 (3): 438-456.

Zoelf, A.M.H. 2009. The Nature of Threats to the Security of Electronic Accounting Information Systems: An Applied Study on Jordanian Insurance Companies. ***The Arab Journal of Accounting***, 12 (1): 46-77.

المراجع الأجنبية

Abu-Musa, A.A. 2006. Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry. ***Journal of Information Systems***, 20 (1): 187-203.

ACSC, Australian Cyber Security Centre. 2015. ***Threat Report: Partnering for a Cyber-secure Australia***, 1-25.

Ahmadzadegan, M.H., Elmusrati, M., & Mohammadi, H. 2013. Secure Communication and VoIP Threats in Next-generation Networks. ***International Journal of Computer and Communication Engineering***, 2 (5): 630-634.

AICPA, American Institute of Certified Public Accountants. 2013. The Top-5 Cybercrimes. In: ***Tommie Singleton***, 1-17. Durham NC.

Al-Ghananeem, K.M. 2014. The Impact of Information Security Management Standards to Ensure Information Security. ***IJER Online***, 5 (1): 46-66.

Bafghi, A.A.T. 2014. Status and Security of Accounting Information Systems in Iranian Organizations. ***International Journal of Economy, Management and Social Sciences***, 3 (12): 71-76.

Bin, X., Hui, B., & Bin, P. 2008. Research of Information-technology Security in the Financial Industry. ***Workshop on Knowledge Discovery and Data Mining***, 7 (8): 477-480.

Blumstein, A., Cohen, J., & Nagin, D. 1978. ***Introduction in Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates***. Washington, DC: National Academy of Sciences.

Chin, W.W. 1998. Issues and Opinions on Structural-equation Modeling, Editorial. ***MIS Quarterly***, 22 (1): 7-16.

Cisco. 2015. ***Annual Security Report***. San Jose, CA: Cisco Systems, Inc.

CNSSI, N. 4009. Committee on National Security Systems Instruction No. 4009. 2015. ***Committee on National Security Systems (CNSS) Glossary***.

Cohen, J. 1988. ***Statistical Power Analysis for the Behavioral Sciences*** (2nd edn.). United States of America: Lawrence Erlbaum Associates.

CSBS. 2016. ***Cyber-security Breaches Survey, Main Report***. London: Ipsos MORI Social Research Institute and Institute for Criminal Justice Studies, University of

Portsmouth.

D'Arcy, J., Hovav, A., & Galletta, D. 2009. User Awareness of Security Countermeasures and Its Impact on Information-system Misuse: A Deterrence Approach. ***Information Systems Research***, 20 (1): 79-98.

Deloitte Co. 2016. ***Cyber-opportunity Analysis Report: Positioned to Lead***. Deloitte Touche Tohmatsu, Limited (DTTL).

GAO-16-605, Government Accountability Office. 2016. ***Information Security: FDIC Implemented Controls over Financial Systems, But Further Improvements Are Needed***. Washington: GAO.

Gordon, L.A., Loeb, M.P., & Zhou, L. 2011. The Impact of Information-security Breaches: Has There Been a Downward Shift in Costs? ***Journal of Computer Security***, (19): 33-56.

Grant, R.M. 1991. The Resource-based Theory of Competitive Advantage: Implications for Strategy Formulation. ***California Management Review***, 33 (3): 114-135.

Gunawan, S., & Nengzih, N. 2023. The Influence of Accounting Information System Quality, Accounting Information Quality and Accounting Information System Security on End User Satisfaction of S4/Hana System Application Product (SAP) with Perceived Usefulness As a Moderating Variable at PT Hakaaston. ***Saudi Journal of Economics and Finance***, 7: 22-32.

Hair, J.F., Celsi, M., Money, A.H., Samouel, P., & Page, M.J. 2019. ***Essentials of Business Research Methods*** (3rd edn.). New York: Routledge.

Hair, J.F., Hult, T.M., Ringle, C.M., & Sarstedt, M. 2017. ***A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*** (2nd edn.): Thousand Oaks, CA: Sage.

Hayale, T.H., & Abu-Khadra, H.A. 2006. Evaluation of the Effectiveness of Control Systems in Computerized Accounting Information Systems: An Empirical Research Applied on the Jordanian Banking Sector. ***Journal of Accounting-Business & Management***, 13: 39-68.

Hayale, T.H., & Abu-Khadra, H.A. 2008. Investigating Perceived Security Threats of Computerized Accounting Information Systems: An Empirical Research Applied on the Jordanian Banking Sector. ***Journal of Economic and Administrative Sciences***, 24 (1): 41-67.

Horne, C.A., Ahmad, A., & Maynard, S.B. 2016. A Theory on Information Security. Paper Presented at ***the Australasian Conference on Information Systems***, Wollongong, Australia.

Hulme, G.V. 2015. ***Survey Says Enterprises Are Stepping up Their Security Game***. Retrieved from CSO online: https://www.csoonline.com/article/2988168/security-leadership/survey-says-enterprises-are-stepping-up-their-security-game.html

ISACA, Information Systems Audit and Control Association. 2019. ***About Control Objectives for Information and Related Technology (COBIT)***. Retrieved from: https://www.isaca.org/resources/cobit

ISO/IEC27000, International Organization for Standardization/ International Electrotechnical Commission. 2018. ***International Standard: Information Technology-Security Techniques-Information-Security Management Systems-Overview and Vocabulary*** (5th edn.) Switzerland: IEC.

ITU, International Telecommunication Union. 2019. ***Global Cybersecurity Index (GCI) 2018***. Switzerland, Geneva: ITU.

ITU, International Telecommunication Union. 2020. ***Study Group 17 at a Glance: ITU-T Study Group 17-Security***. Retrieved from: https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

Kaspersky. 2017. ***KSN Report: Ransomware in 2016-2017***, 1-29. Russia: Kaspersky.

Kemper, G. 2018. ***The State of Security: How to Budget for Digital Security in 2018***. Retrieved from: Tripwire: https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/how-to-budget-for-digital-security-in-2018)/

Keung, Y.H. 2013. Information-security Controls. ***Advances***

in Robotics & Automation, 3 (2). Retrieved form: https://www.omicsonline.org/open-access/information-security-controls-2168-9695.1000e118.php?aid=23716

LinkedIn. 2023. April 27. ***The Importance of Data Security in 2023***. Retrieved on August 8, 2023 from: https://www.linkedin.com/pulse/importance-data-security-2023-deltaspike

Malik, G. 2023. April 12. ***Cybersecurity in 2023: Technologies and Trends Shaping the Current State of Security***. Eccouncil Cybersecurity-exchange. Retrieved on August 7, 2023 from: https://www.eccouncil.org/cybersecurity-exchange/network-security/cybersecurity-2023-technologies-trends/

Merriam-Webster. 2018. ***Definition of Deterrence***. Retrieved from: https://www.merriam-webster.com/dictionary/deterrence

Microsoft. 2020. ***A Moment of Reckoning: The Need for A Strong and Global Cybersecurity Response***. In: Brad Smith (Ed.).

Miloslavskaya, N.G. 2014. Information Security Theory Development. Paper Presented at ***the WG 11.8 - 11th World Conference on Information Security Education***, Moscow, Russia.

NCSI. 2020. ***National Cyber-security Index, Held and Developed by e-Governance Academy Foundation***. Retrieved from: https://ncsi.ega.ee/country/ye/467/#details

NIST SP 800-30 r1, National Institute of Standards and Technology Special Publication 800-30 Revision 1. 2012. ***Guide for Conducting Risk Assessments***. U.S: NIST.

NISTIR 7621 r1, The National Institute of Standards and Technology Interagency Reports 7621 Revision 1. 2016. ***Small-business Information Security***: ***The Fundamentals***. In: Celia Paulsen & Patricia Toth, 1-50.

Norman, A.A., Hamid, S.H., Maw, M., & Tamrin, S.I. 2017. Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review. Paper presented at ***the Future Technologies Conference (FTC)***, Vancouver, Canada.

Ponemon G.A. 2015. ***Cost of Cybercrime Study: Global Analysis***. Traverse City, Michigan, USA: Ponemon Institute, LLC.

Ponemon, G.A. 2015. ***Cost of Data Breach Study: Global Analysis***. Traverse City, Michigan, USA: Ponemon Institute, LLC.

Posthumus, S., & von Solms, R. 2004. A Framework for the Governance of Information Security. ***Computers & Security***, 23 (8): 638-646.

Quoc, T.N., Bao, Q.P.T., Huu, B.N., & Bao, A.N.P. 2023, May. Motivating Accounting Information System Security Policy Compliance: Insight from the Protection Motivation Theory and the Theory of Reasoned Action. In: ***International Conference on Emerging Challenges: Strategic Adaptation in The World of Uncertainties (ICECH 2022)***, 342-359. Atlantis Press.

Riad, N.I. 2009. ***Security of Accounting Information Systems: A Cross-sector Study of UK Companies***. Doctoral Dissertation, Cardiff University.

SANS. 2018. ***CIS Critical Security Controls: Guidelines***. Retrieved from: https://www.sans.org/critical-security-controls/guidelines

Schuessler, J.H. 2009. ***General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large versus Small Businesses***. Doctoral Dissertation, University of North Texas.

Schuessler, J.H. 2013. Contemporary Threats Countermeasures. ***Journal of Information Privacy and Security***, 9 (2): 3-20.

Straub, D.W. 1987. Controlling Computer Abuse: An Empirical Study of Effective Security Countermeasures. ***Paper Presented at the International Conference on Information Systems (ICIS)***.

Straub, D.W. 1990. Effective IS Security: An Empirical Study. ***Information Systems Research***, 1 (3): 255-276.

Straub, D.W., & Welke, R.J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. ***MIS Quarterly***, 22 (4): 441-469.

Tarmidi, M., Rashid, A., Deris, M., & Roni, R. 2013.

Computerized Accounting System Threats in Malaysian Public Services. ***International Journal of Finance and Accounting***, 2 (2): 109-113.

von Solms, R., & van Niekerk, J. 2013. From Information Security to Cyber-security. ***Computers & Security***, 38: 97-102.

Watuthu, S.N. 2015. ***A Framework to Extend COBIT Security Framework to Overcome Confidentiality Threats in Electronic Commerce***. Master Thesis. Jomo Kenyatta University.

Workman, M., Bommer, W.H., & Bommer, W.H. 2008. Security Lapses and the Omission of Information-security Measures: A Threat-control Model and Empirical Test. ***Computers in Human Behavior***, 24 (6): 2799-2816.