أثـر الضوابط الأمنية في أمن نظـم المعلومات المحاسبية في قطاع الاتصالات باليمن

الاســتلام: 10/مايو/ 2023
التحكيـــم: 18/مايو/ 2023
القبـــول: 31/مايو/ 2023

نبيل حسان عبده الحميري [*,1]
محمد علي محمد الربيدي [2]

Nabil Hassan Abdo Al-Hemyari [*,1]
Mohammed Ali M. Alrubaidi [2]

[1] أستاذ المحاسبة المساعد، جامعة العلوم والتكنولوجيا، صنعاء، اليمن
[2] أستاذ المحاسبة، جامعة العلوم والتكنولوجيا، صنعاء، اليمن
*عنوان المراسلة: nabelal2000@yahoo.com

[1]Assistant Professor of Accounting, University of Science and Technology, Sana'a, Yemen
[2]Professor of Accounting, University of Science and Technology, Sana'a, Yemen

http://doi.org/10.59222/ustjmhs.1.2.1

أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن

الملخص:

هدفت الدراسة إلى اختبار أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية باتباع منهج تحليلي يعتمد على نمذجة المعادلة البنائية (SEM)، ويتمثل مجتمع الدراسة في قطاع الاتصالات باليمن، وتم استخدام الاستبانة أداة لجمع البيانات من 356 مشاركا، وقد وصل عدد الاستبانات الصالحة للتحليل 218 استبانة، وتم تحليل البيانات باستخدام طريقة المربعات الصغرى الجزئية (PLS)، وقد دعمت نتائج هذه الدراسة صحة الفرضيات المقترحة في النموذج النظري؛ حيث أكدت النتائج أن الضوابط الأمنية (التقنية، والإدارية) تؤثر بشكل إيجابي في أمن نظم المعلومات المحاسبية، وأوصت الدراسة بمزيد من الاهتمام بأمن نظم المعلومات المحاسبية، وتحديث الضوابط الأمنية باستمرار.

الكلمات المفتاحية: أمن نظم المعلومات المحاسبية، الضوابط الأمنية، قطاع الاتصالات في اليمن.

http://doi.org/10.59222/ustjmhs.1.2.1

Impact of Security Controls on Security of Accounting Information Systems at Telecommunications Sector in Yemen

Abstract:

This study aimed to investigate the impact of security controls on security of accounting information systems by following an analytical method based on the structural equation modeling (SEM). The study population was telecommunications sector in Yemen. A questionnaire was distributed to 356 participants, but only 218 forms were valid for analysis. The data were analyzed by the partial least squares (PLS). The study findings supported the hypotheses proposed in the theoretical model as it was found that security controls had a positive impact on the security of accounting information systems. The study recommends paying more attention to the security of accounting information systems and updating security controls continuously.

Keywords: security of accounting information systems, security controls, telecommunications sector in Yemen.

http://doi.org/10.59222/ustjmhs.1.2.1

المقدمة:

تحتل قضايا أمن نظم المعلومات المحاسبية ([Accounting Information Systems [AIS) مساحة واسعة من الدراسات والأبحاث؛ حيث أكدت العديد من الدراسات والتقارير (American Institute of Certified Public Accountants [AICPA], 2015; Ernst & Young, 2012; PricewaterhouseCoopers [PwC] & Infosecurity, 2014) أن أهمية أمن نظم المعلومات جاءت عالية في منظمات الأعمال، وفي مقدمة أولوياتهم تأمين البيئة الرقمية.

وقد أصدرت الهيئات المهنية أطرا ومعايير تهدف إلى تأمين البيئة الرقمية؛ حيث ذكرت دراسة PwC أن مزايا استخدام الأطر الأمنية (International Organization for Standardization [ISO], National Institute of Standards and Technology [NIST], Control Objectives for Information and Related Technologies [COBIT], etc.) تتمثل في كشف، وخفض الحوادث الأمنية، وتحديد المخاطر وترتيب أولوياتها، وتأمين البيانات الحساسة، وإدراك الثغرات الأمنية (Hulme, 2015)، وأولت التشريعات الدولية اهتماما كبيرا بحماية المعلومات، وأصدرت قوانين، مثل: قانون ساربنيز-أوكسلي، وقانون إدارة أمن المعلومات الفدرالي، وقانون مكافحة الجرائم الإلكترونية التي تساعد في حماية المعلومات من خلال تجريم ومعاقبة الوصول غير المشروع إلى أنظمة المعلومات، وتشديد العقوبة على المخالفين (مركز دعم لتقنية المعلومات، 2015).

وقد تناول بعض الباحثين قضايا أمن نظم المعلومات المحاسبية من جوانب مختلفة؛ حيث أشار الاستطلاع العالمي لأمن المعلومات ([Global Information Security Survey [GISS) إلى أن الفجوة الأمنية تتسع باستمرار بين التحسينات الحالية في أمن المعلومات والتحسينات المطلوبة؛ استنادا إلى المخاطر المتصاعدة (Ernst & Young, 2012)، وأكد تقرير Deloitte (2013) أن شركات الاتصالات لا تزال تواجه مخاطر أمنية جديدة وبشكل مرتفع، وذكر تقرير Deloitte (2014) أن استهداف شركات الاتصالات قد زاد، مثل التنصت على خطوط الهاتف، والدردشة عبر الإنترنت، والوصول إلى البيانات الشخصية، والوصول إلى خدمات مكلفة، وتوصلت دراسة استطلاعية في 2022م إلى أن متوسط تكلفة خرق البيانات بلغت 4.4 $ مليون على مستوى العالم بزيادة 13 % عن العام السابق (Lemos, 2022)، وذكر تقرير Deloitte (2006) أن ثلث الاختراقات التي عانت منها شركات الاتصالات أدت إلى حدوث خسائر مالية كبيرة، وإلحاق أضرار بالسمعة والعلامة التجارية، وتوقف النظام، وفقدان الإيرادات، وأشار تقرير Deloitte (2014) أن الهجمات التي استهدفت شركات الاتصالات أدت إلى إلحاق أضرار كبيرة بالسمعة وسرية المعلومات، وأثارت مخاوف العملاء المتعلقة بالخصوصية؛ مما أدى إلى فقدان الثقة، وقد أجمع ثلث المختصين في تكنولوجيا المعلومات على أن منع الاختراقات الأمنية تشكل الهم الأكبر للمنظمات، يليها حماية البيانات، وفق ما جاء في تقرير Kaspersky (يحيى، 2012)، وتفتقر العديد من الشركات إلى الثقة في قدرتها على مواجهة التهديدات الحالية، وفقا لاستطلاع قادة تكنولوجيا المعلومات والأمن (Mar-Elia, 2023)، وأكثر من ثلث المنظمات لا تزال تفتقر إلى الثقة في قدرة أمن المعلومات على كشف الهجمات المتطورة، ويرى 88 % من المشاركين أن أمن المعلومات لا يلبي تماما احتياجات منظماتهم، وفق ما جاء في استطلاع Ernst وYoung (Bernews, 2015).

كما أن استخدام الضوابط الأمنية في منظمات الأعمال يساعد في منع المخاطر أو الحد من آثارها السلبية (Schuessler, 2013)، ويساعد في حماية أنظمة المعلومات من الوصول غير المصرح به، وتقييد عمليات الوصول المصرح به، والتحقق من هوية المستخدمين (Government Accountability Office [GAO], 2016a)، وقد تناولت العديد من الدراسات (Ernst & Young, 2015; PwC & Infosecurity, 2015; Riad, 2009; Schuessler, 2013; Symantec Corporation, 2017) الضوابط الأمنية المستخدمة في حماية أنظمة المعلومات المحاسبية من المخاطر، كالتحكم بالوصول، والتحقق من الهوية، ومكافح البرامج الضارة، وأنظمة كشف التسلل،

http://doi.org/10.59222/ustjmhs.1.2.1

والتشفير، والجدران النارية، والسياسة الأمنية، والتوعية والتدريب، وأشارت نتائج تلك الدراسات إلى وجود اتفاق واختلاف نسبي في استخدام الضوابط الأمنية في منظمات الأعمال.

وقد تناول بعض الباحثين الأثر المباشر للضوابط الأمنية في أمن نظم المعلومات المحاسبية؛ حيث توصلت دراسة كل من Chang وWang (2011)، Seno ، Bidmeshk، وGhaffari (2015)، Al-ghananeem (2014)، Riad (2009)، ودراسة Schuessler (2009) إلى أن الضوابط الأمنية لها تأثير إيجابي مباشر في أمن نظم المعلومات المتمثل في الحفاظ على سرية المعلومات وسلامتها وتوافرها، وقد أوضحت دراسة Tsegaye وFlowerday (2014، 28) أن تطبيق مجموعة ملائمة من الضوابط الأمنية تساعد في حماية المعلومات.

ومع ذلك، قد تنشأ ثغرات أمنية جديدة مع مرور الزمن ناتجة عن عوامل تنظيمية، وبيئية، وتكنولوجية تؤدي إلى ظهور مخاطر جديدة، وتصبح الضوابط الأمنية الحالية غير كافية (Joint Task Force Transformation Initiative [JTFTI], 2012)، فقد ذكر المعهد الوطني للمعايير والتكنولوجيا (JTFTI, 2012) أن الثغرات الأمنية قد توجد في خطط الطوارئ، أو استخدام تقنيات متقادمة، أو قصور في تنفيذ آليات التحقق من الهوية، أو قصور في الجوانب التشريعية والتنظيمية، وأكدت دراسة Hayale وAbu-Khadra (2006) أن هناك جوانب قصور في أمن نظم المعلومات المحاسبية تتمثل في جوانب ضعف في الوصول المادي والمنطقي وأمن البيانات والتعافي من الكوارث، وتناولت دراسة Abdulsalam وHedabou (2022) نقاط الضعف التي قد توجد في واجهات برمجة التطبيقات، وضعف أنظمة المصادقة والتشفير، وفقدان السيطرة على الكوارث، وضعف السياسة الأمنية، وناقشت دراسة Kiseki et al. (2023) نقاط الضعف في نظام التشغيل والتطبيق وكلمات المرور، وأخطاء في الإعداد، والإعدادات الافتراضية، وعدم تحديث الضوابط الأمنية، وتستغل التهديدات نقاط الضعف في تنفيذ الهجمات التي تؤثر في موارد تكنولوجيا المعلومات.

وذكر تقرير مكتب المساءلة الحكومية GAO (2015) جوانب الضعف في الضوابط الأمنية التي شهدتها الوكالات الفدرالية المتمثل في ضعف التحكم بالوصول، وضعف إدارة إعداد البرامج والأجهزة، وضعف خطة استمرارية العمل، وأشارت دراسة Mbowe، Zlotnikova، Msanjila، وOreku (2014) إلى أن ثلثي المنظمات تقريبا لديها استراتيجيات غير كافية للضوابط، وأن أكثر من ثلثي المنظمات تعاني من ضعف في استخدام التوقيعات الرقمية والتدقيق، وتوصلت دراسة كل من Riad (2009) ، Abu-Musa (2006a) ، Tarmidi، Rashid، Deris، وRoni (2013)، وMuhrtala وOgundeji (2013) إلى عدم مواكبة أمن نظم المعلومات المحاسبية للتغيرات المتسارعة في بيئة الأعمال، وأن التطورات في تكنولوجيا المعلومات لم يرافقها تطور مماثل في الممارسات والضوابط الأمنية، وأكدت دراسة Schuessler (2009) أن الضوابط الأمنية يمكنها الحد من المخاطر وليس منع جميع المخاطر.

لذلك، يعتمد بناء برنامج أمني ناجح على إعادة وضع استراتيجية أمنية قائمة على ربط التقنيات، والعمليات، ومهارات الأفراد بشكل وثيق مع أنشطة إدارة مخاطر المنظمة (PwC, 2015)، ودعم الجهود الرامية إلى وضع مقاييس وتطبيق المعايير الدولية، ودعم الأطر القانونية والتنظيمية، والاستفادة من الممارسات المثلى (جبور، 2012)؛ حيث أشارت دراسة Abu-Musa (2006b) إلى أن وضع السياسات الأمنية وتعزيز وعي الموظفين بأمن نظم المعلومات المحاسبية يُعد من القضايا المهمة جدا في نجاح برنامج الأمن، وأكدت دراسة Choejey، Murray، وFung (2016) على أن عوامل النجاح الأكثر أهمية في تنفيذ الأمن السيبراني تتمثل في التوعية والتدريب، يليها وضع سياسات ومعايير وإجراءات الأمن، ثم موازنة الأمن، ودعم الإدارة العليا، وذكرت دراسة Riad (2009) أن من عوامل النجاح وعي وإدراك الإدارة للتغيرات الكبيرة في التكنولوجيا المتاحة والآثار الأمنية الناجمة عنها.

http://doi.org/10.59222/ustjmhs.1.2.1

وتستخدم الدراسة الحالية نظرية الردع العام، ونظرية أمن المعلومات في تفسير أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية (Horne, Ahmad, & Maynard, 2016; Straub & Welke, 1998)، وبالتالي فإن أمن نظم المعلومات المحاسبية يتحقق من خلال التصميم والتنفيذ والتطوير للضوابط الأمنية التي تعمل على الردع، والمنع، والكشف، أو الحد من الوصول غير المصرح به إلى الحواسيب، والبرامج، والمرافق (GAO, 2016b)؛ لذلك تم دراسة أمن نظم المعلومات المحاسبية لتحقيق هدف الدراسة الحالية المتمثل في قياس أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.

أمن نظم المعلومات المحاسبية:

إن أمن نظم المعلومات المحاسبية يتطور باستمرار؛ استجابة للتغيرات التكنولوجية، وقدرات المهاجمين، وقيمة الأهداف المحتملة، والآثار الناجمة عن ذلك، وعلينا أن نقبل بأننا لن نقضي على جميع المخاطر، وأنه لا شيء آمن بشكل دائم، وحتى لو استطعنا ذلك فإن الكلفة باهظة (McAfee Enterprise, 2015)، وأمن نظم المعلومات عملية متطورة لا تنتهي ولا تتوقف عند حد معين؛ حيث تتغير الدفاعات ووسائل الحماية باستمرار؛ استجابة للمخاطر الجديدة التي تتعرض لها المنظمات (Palmer, 2013).

أولا: مفهوم أمن نظم المعلومات المحاسبية:

يشير أمن المعلومات إلى مجموعة العناصر الواجب توافرها في المعلومات والأنظمة، كالسرية والسلامة والتوافر، بحيث يغطّي كل عنصر من هذه العناصر جانبا مهما من الجوانب المطلوب توافرها في تلك المعلومات، وهذه العناصر تتكامل فيما بينها، ويترتب على غياب أحد هذه العناصر قصور في أمن المعلومات؛ لذا نجد لجنة أنظمة الأمن القومي (Committee on National Security Systems [CNSS], 2015)، والمعهد الوطني للمعايير والتكنولوجيا (Kissel, 2013; Paulsen & Toth, 2016)، قد عرّفا أمن المعلومات بأنه: 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، وعرّفتها المنظمة الدولية للمعايير بأنها: الحفاظ على سرية المعلومات، وسلامتها، وتوافرها (ISO/IEC JTC 1, 2018)، وعرّفت لجنة أنظمة الأمن القومي مصطلح أمن نظم المعلومات بأنه: حماية أنظمة المعلومات ضد الوصول غير المصرح به، أو تعديل المعلومات سواء عند التخزين أو المعالجة أو النقل، أو انقطاع الخدمة عن المستخدمين المخولين (CNSS, 2015)، وعرّفت دراسة Riad (2009) أمن نظم المعلومات المحاسبية بأنها حماية جميع المكونات التي تجمع، وتخزن، وتعالج البيانات المحاسبية للمستخدم النهائي.

ويُعد أمن نظم المعلومات المحاسبية (AIS) جزءا لا يتجزأ من أمن نظم المعلومات (Information Systems [IS]) الشامل للشركة (Riad, 2009)، وأن أمن نظم المعلومات (IS) هو جزءٌ من أمن المعلومات (InfoSec) (Cherdantseva & Hilton, 2014).

ولأغراض الدراسة الحالية فإن تعريف أمن نظم المعلومات المحاسبية يتحدد بأنه: الحفاظ على سرية المعلومات، وسلامة المعلومات والأنظمة، وتوافرها سواء أثناء المعالجة، أو التخزين، أو النقل.

ثانيا: أهمية أمن نظم المعلومات المحاسبية:

تعتمد العمليات اليومية في منظمات الأعمال على أنظمة المعلومات بشكل عام وأنظمة المعلومات المحاسبية بشكل خاص، ويُعد تحقيق الأمن والحفاظ على سرية المعلومات وسلامتها وتوافرها في أنظمة الشركات متطلبا أساسيا ومهما، لأن هذه الأنظمة معرضة للعديد من المخاطر التي تستهدف سرية المعلومات وسلامتها وتوافرها التي قد تؤدي إلى كشف المعلومات السرية أو تعديل البيانات المالية أو حجب الخدمات، وتوقف الأعمال، والإضرار بالسمعة، وفقدان إيرادات، وخسائر مالية، مما يؤدي إلى فقدان الثقة؛ لذلك تولي منظمات الأعمال اهتماما كبيرا؛ لضمان أمن تلك الأنظمة، وفي مقدمة أولوياتها تأمين البيئة الرقمية (Abu-Musa, 2006b; JTFTI, 2012; JTFTI, 2013).

http://doi.org/10.59222/ustjmhs.1.2.1

وتتمثل أهمية أمن نظم المعلومات المحاسبية في تأمين المعلومات المالية وحمايتها من المخاطر، وذلك من خلال برامج التوعية والتدريب، وتطبيق السياسة الأمنية، والتحقق من الهوية، والتحكم بالوصول، والتشفير، وقد أولت الهيئات المهنية قدرا كبيرا من الاهتمام بالمعايير والسياسات والقوانين واللوائح وتطويرها لمساعدة منظمات الأعمال في تأمين معلوماتها بشكل كاف من المخاطر (AlKalbani, Deng, Kam, & Zhang, 2017)؛ حيث أشار تقرير Cisco (2015) إلى أن ثلثي المختصين أفادوا أن القيادة التنفيذية في منظماتهم تعتبر الأمن أولوية عالية، وتوصلت دراسة Richardson (2010) إلى أن نصف المستجيبين يرون أن الإدارة العليا تعتبر الأمن أولوية عالية، وأكد تقرير PwC وInfosecurity (2014) أن أولوية أمن المعلومات عالية في الشركات، وأكد غالبية المشاركين على أهمية أمن المعلومات وأولويته وأثره الإيجابي في أنظمة الشركات.

ثالثا: أبعاد أمن نظم المعلومات المحاسبية:

يُقصد بأمن نظم المعلومات الحفاظ على سرية المعلومات وسلامتها وتوافرها أثناء المعالجة أو التخزين أو النقل (ISO/IEC JTC 1, 2018; Paulsen & Toth, 2016)، وسوف تعتمد الدراسة الحالية في قياس أمن نظم المعلومات المحاسبية على الأبعاد الثلاثة الآتية:

1. سرية المعلومات: وهي حماية المعلومات من الكشف والوصول والاستخدام غير المصرح به (ISO/IEC JTC 1, 2018; Paulsen & Toth, 2016)،
2. سلامة المعلومات: وهي حماية المعلومات من التعديل والإتلاف غير المصرح به (Paulsen & Toth, 2016)،
3. توافر المعلومات: وتعني ضمان إمكانية الوصول إلى نظام المعلومات أو المعلومات في الوقت المناسب، وإمكانية الاعتماد عليها واستخدامها (ISO/IEC JTC 1, 2018; Kissel, 2013).

الضوابط الأمنية:

تهدف الضوابط الأمنية إلى حماية أصول نظم المعلومات من الوصول غير المصرح به، وتقييد عمليات الوصول المصرح به، والحماية من التعديل غير المشروع أو التوقف (GAO, 2016a)، وتعمل الضوابط الأمنية إما بغرض القضاء على الخطر، أو من أجل الحد من المخاطر التي تؤثر سلبا في أنظمة المعلومات وخفض تكاليفها (Schuessler, 2013)، ويعتمد مستوى الحماية على حساسية وأهمية المعلومات، وتزداد تكاليف الحماية بازدياد مستوى الحماية المطبق؛ لذلك لا بد من الموازنة بين مستوى الحماية وتكاليف تطبيقها (القحطاني، 2015، 107)، ويعتمد اختيار وتطبيق الضوابط الأمنية على تقييم مخاطر نظم المعلومات؛ حيث أن تقييم المخاطر تُحدد التهديدات ونقاط الضعف في النظام، والضوابط الأمنية تحد من المخاطر المحتملة وتقلل من الخسائر (Keung, 2013).

أولا: مفهوم الضوابط الأمنية:

يُقصد بالضوابط الأمنية (Security Controls [SC]) الضوابط الإدارية والتقنية المفروضة على نظام المعلومات؛ لحماية سرية المعلومات والأنظمة، وسلامتها، وتوافرها (CNSS, 2015)، والضوابط الأمنية هي مصطلح مرادف للإجراءات الوقائية والتدابير المضادة (JTFTI, 2010)، وقد عرّفها المعهد الوطني للمعايير والتكنولوجيا (JTFTI, 2013) بأنها: التدابير المضادة المفروضة على نظام المعلومات التي تهدف إلى: (1) حماية سرية، وسلامة، وتوافر المعلومات التي يتم معالجتها، وتخزينها، ونقلها بواسطة هذه الأنظمة، (2) تلبية مجموعة من متطلبات أمنية محددة، وأيضا عرّفتها المنظمة الدولية للمعايير بأنها: إدارة المخاطر، بما في ذلك السياسات، والإجراءات، والإرشادات، والممارسات، أو الهياكل التنظيمية التي قد تكون ذات طابع تقني، أو إداري، أو قانوني (ISO/IEC JTC 1, 2009)، وعرّفتها دراسة Riad (2009) بأنها: التدابير المضادة المستخدمة لحماية سرية المعلومات المحاسبية، وسلامتها، وتوافرها.

http://doi.org/10.59222/ustjmhs.1.2.1

ولأغراض الدراسة الحالية فإن الضوابط الأمنية تُعرف بأنها: الضوابط التقنية والإدارية اللازمة؛ لحماية سرية المعلومات المحاسبية، وسلامتها، وتوافرها من المخاطر المختلفة أثناء المعالجة أو التخزين أو النقل.

ثانيا: أبعاد الضوابط الأمنية:

بناءً على ما سبق من تعريف المعهد الوطني للمعايير والتكنولوجيا (Ross et al., 2005) والمنظمة الدولية للمعايير (ISO/IEC JTC 1, 2009)، ولجنة أنظمة الأمن القومي (CNSS, 2015)، للضوابط الأمنية، يتضح أن التعريف تضمن بُعدين أساسيين لقياس الضوابط الأمنية، وهما:

1. الضوابط التقنية: وهي التدابير المتخذة لحماية نظام المعلومات من خلال الآليات المدرجة في مكونات الأجهزة والبرامج، كآليات التحقق من الهوية، والتحكم بالوصول، ومكافح البرامج الضارة، وحماية الشبكة، وأنظمة التشفير (NIST, 2006; Stoneburner, Goguen, & Feringa, 2002; Rot, 2009).
2. الضوابط الإدارية: وهي الإجراءات الإدارية المتخذة لحماية نظام المعلومات من خلال سياسة الأمن، وخطط الطوارئ، والتوعية والتدريب، وإجراءات التدقيق، والتدابير القانونية (Keung, 2013; Kim, Lee, & Ham, 2013; Stoneburner et al., 2002).

النظريات المفسرة لمتغيرات الدراسة:

هناك نظريات سلوكية راسخة ونماذج مفاهيمية أخرى تفسر أثر الضوابط الأمنية في أمن نظم المعلومات، وتقدم نظرة ثاقبة حول كيفية التعامل مع المخاطر، وتنفيذ الحماية على أساس علمي ومنهجي متين، مثل نظرية الردع العام، ونظرية أمن المعلومات، وتوضيح ذلك على النحو الآتي:

أولا: نظرية الردع العام:

تركز نظرية الردع العام (General Deterrence Theory [GDT]) على العقوبات التي تؤثر في الآخرين، وتعمل تلك العقوبات كمثبطات للأفعال غير المشروعة التي تتمثل في مبدأين رئيسين، وهما:

1- اليقين بالعقوبات (شعور الفرد بأنه لا مفر من خضوعه للعقاب إذا ارتكب الجريمة).
2- شدة العقوبات (التخويف من تبعات ارتكاب الجرائم) (Blumstein, Nagin, & Cohen, 1978; Straub & Welke, 1998).

فعندما تكون مخاطر العقاب مرتفعة (يقين بالردع)، والعقوبات على الانتهاكات شديدة (شدة الردع)، تتنبأ النظرية بردع الجناة المحتملين عن ارتكاب أفعال غير مشروعة (Straub, 1990)، وتفترض هذه النظرية إجراءات عامة تقلل من المخاطر بشكل مباشر أو غير مباشر، وذلك من خلال استخدام التدابير المضادة (الردع، والوقاية، والكشف، والمعالجة) (Straub & Welke, 1998).

وقدمت دراسة D'Arcy، Hovav، وGalletta (2009) نموذجا موسعا لنظرية الردع العام الذي يفترض أن وعي المستخدم بالتدابير المضادة (السياسات الأمنية، برامج التوعية والتدريب، مراقبة الحاسوب) لها تأثير مباشر وغير مباشر في نوايا المستخدمين المتعلقة بإساءة استخدام نظم المعلومات من خلال إدراك المستخدمين للعقوبة (اليقين، والشدة)، وتوسعت دراسة Schuessler (2009) في وجهات النظر المفاهيمية لنظرية الردع العام لتشمل المخاطر غير البشرية (الكوارث الطبيعية، والإخفاق التقني)، ويساعد هذا التوسع في التخطيط الوقائي للحد من المخاطر (TheoriZeit, 2016).

وقد تم تصنيف التدابير المضادة – وفق دورة عمل الأمن (Security Action Cycle [SAC]) في نظرية الردع العام – إلى أربع فئات (الردع، والوقاية، والكشف، والمعالجة)، وهي تساعد في إيجاد بدائل أمنية، وتقدم للممارسين منظورا نظريا لتنفيذ التدابير المضادة (Straub & Welke, 1998).

http://doi.org/10.59222/ustjmhs.1.2.1

وتعتمد الدراسة الحالية على نظرية الردع العام (GDT)؛ لتكون إطارا نظريا يمكن أن تستخدم المنظمة من خلاله الضوابط الأمنية المتاحة في الحفاظ على أمن نظم المعلومات (السرية، والسلامة، والتوافر) من المخاطر، وما يبرر استخدام نظرية الردع العام (GDT) هو إمكانية تطبيقها على أنظمة المعلومات، وقد تم تطبيقها بنجاح على أبحاث أمن نظم المعلومات من قبل Straub، وغيره من الباحثين.

ثانيا: نظرية أمن المعلومات:

تنص نظرية أمن المعلومات على أن الدافع وراء كل المحاولات التي تقوم بها المنظمة لتأمين المعلومات من المخاطر هو خلق الموارد التي يمكن استخدامها لاحقا في تحسين الأداء التنظيمي، وقد نشأت نظرية أمن المعلومات في مجال نظم المعلومات، وبنيت بالكامل من المفاهيم التي تتعلق بالمعلومات، ويُعد أمن المعلومات ظاهرة تقع ضمن نطاق نظم المعلومات (Horne et al., 2016)، وهذه النظرية تفسيرية وليست تنبؤية، فهي تقدم تفسيرات سببية محددة، ومقترحات قابلة للاختبار، وبيانات وصفية، ويمكن استخدام هذه النظرية في تفسير الدوافع وراء الجهود الرامية إلى حماية المعلومات المستخدمة من قبل الأفراد، والمجموعات، والمنظمات، وأيضا تنص 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).

ويساعد تطبيق الضوابط الأمنية في حماية سرية المعلومات، وسلامتها، وتوافرها، والتخفيف من المخاطر المختلفة (Posthumus & von Solms, 2004)، ومنع وكشف الهجمات، وتشمل الضوابط الأمنية: مكافح الفيروسات، والجدران النارية، والتحديثات الأمنية، وأنظمة التحكم في تغيير كلمة المرور، ومجموعة من التقنيات الأخرى المتوفرة لتحسين أمن المعلومات (Workman, Bommer, & Straub, 2008)، ويؤدي تطبيق ضوابط الحماية إلى تحويل المعلومات إلى موارد، وتؤدي الضوابط إلى حماية المعلومات بشكل إيجابي، ويمكن تطبيق الضوابط التقنية والإدارية؛ لحماية المعلومات المادية والرقمية (Horne et al., 2016).

الدراسات السابقة:

ناقشت بعض الدراسات أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية، مثل دراسة Riad (2009) التي تناولت العوامل المؤثرة في أمن نظم المعلومات المحاسبية، وأن بعض هذه العوامل تؤثر بشكل إيجابي في أمن المعلومات، كالضوابط الأمنية، وتوصلت دراسة فاضل (2018) إلى أن آليات الحماية تؤثر بشكل إيجابي في أمن نظم المعلومات المحاسبية، وأشارت دراسة Abu-Musa (2006b) إلى أن وضع السياسات الأمنية وتعزيز وعي الموظفين بأمن نظم المعلومات المحاسبية يُعد من القضايا المهمة جدا في نجاح برنامج الأمن، وأشارت دراسة Chang وWang (2011) إلى أن موارد نظم المعلومات (التكنولوجية، والعلائقية، والبنية التحتية) تؤثر بشكل إيجابي في أمن المعلومات، وأن البنية التحتية وموارد تكنولوجيا المعلومات ترتبط ارتباطا وثيقا بسرية المعلومات، وأن موارد تكنولوجيا المعلومات والعلاقة الخارجية الجيدة وهيكل إدارة أمن المعلومات القوي تُعد ضرورية لتوافر المعلومات التي ترتبط ارتباطا وثيقا بموثوقية النظام، وأن الموارد البشرية المتخصصة في تكنولوجيا المعلومات، والعلاقة الخارجية الجيدة ترتبط ارتباطا وثيقا بسلامة المعلومات، وتساعد التقنيات الأمنية في كشف ومنع الحوادث التي تؤثر في سلامة المعلومات.

وذكرت دراسة Chang وLin (2007) أن سمات الثقافة التنظيمية (التعاون) لها علاقة سلبية بالسرية، وأن سمات الثقافة التنظيمية (الفاعلية والاتساق) لها تأثير كبير في السرية، وأما المرونة والعمل الإبداعي فلا ترتبط بشكل كبير بالسرية، وأن الفاعلية والاتساق لهما تأثير إيجابي وكبير في السلامة، وأما عوامل المرونة والتعاون والعمل الإبداعي فلا ترتبط بشكل كبير بالسلامة، وأن الفاعلية والاتساق لهما تأثير إيجابي ومهم في التوافر، ولكن عوامل المرونة والتعاون والعمل الإبداعي فلا ترتبط بشكل كبير بعنصر التوافر.

http://doi.org/10.59222/ustjmhs.1.2.1

وتوصلت دراسة Schuessler (2009) إلى أن التدابير المضادة ترتبط بشكل إيجابي بفاعلية أمن نظم المعلومات، وذكرت دراسة Haeussinger وKranz (2013) أن هناك علاقة إيجابية بين الوعي بقضايا أمن نظم المعلومات واستخدام التدابير الوقائية في حماية المعلومات، وأظهرت دراسة Al-ghananeem (2014) أن معايير إدارة أمن المعلومات (الضوابط) لها تأثير إيجابي في ضمان أمن المعلومات، وأكدت دراسة Al-ghananeem، Al-taee، وJida (2014) أن أهداف أمن المعلومات لها تأثير إيجابي في ضمان أمن المعلومات، وخلصت دراسة Seno et al. (2015) إلى أن أمن المعلومات لها علاقة قوية ومباشرة بتدابير أمن المعلومات، وأن عوامل السرية والسلامة والتوافر لها تأثير إيجابي ومهم في تدابير أمن المعلومات، وأن الإجراءات تعمل على منع التعديل أو الإتلاف غير المصرح به، وأن المعلومات قابلة للاستخدام في أي مكان وزمان، وأن هناك فجوة في مؤشر منع انقطاع الخدمة، وتبين عدم وجود فجوة فيما يتعلق بحماية المعلومات من الكشف.

وذكرت دراسة Martin وKhazanchi (2006) أن الآليات الأمنية تؤثر في عنصر التوافر، وتوصلت دراسة Woodhouse (2008) إلى أن عوامل التزام الإدارة، والثقافة التنظيمية، والنضج التنظيمي تؤثر بشكل إيجابي في أمن المعلومات، وذكر تقرير Office of Management and Budget [OMB], (2016) أن مكتب الإدارة والموازنة تمكن من تحليل مجالات الضعف وتحسين الدفاعات التي كان لها أثر إيجابي في المنظمات، وأشارت دراسة Choejey et al. (2016) إلى أن عوامل النجاح المهمة في تنفيذ الأمن السيبراني تتمثل في التوعية والتدريب، يليها وضع سياسة ومعايير وإجراءات الأمن، ثم موازنة الأمن، ودعم الإدارة العليا، والبنية التحتية، وتدقيق الأمن.

وقد تناولت المنظمة الدولية للمعايير ISO/IEC JTC1 (2018) عوامل النجاح المهمة في تنفيذ نظام إدارة أمن المعلومات ([Information Security Management System [ISMS)؛ وذلك من أجل تحقيق أهداف العمل، وهذه العوامل هي: 1) سياسة وأهداف أمن المعلومات متوافقة مع أهداف ومتطلبات العمل، 2) نهج وإطار لتصميم، وتنفيذ، ومراقبة، وتحسين، والحفاظ على أمن المعلومات، بما يتماشى مع الثقافة التنظيمية، 3) التزام ودعم مستمر من الإدارة العليا، 4) فهم متطلبات حماية أصول المعلومات التي تتحقق من خلال تطبيق إدارة مخاطر أمن المعلومات، 5) برنامج فاعل للتوعية والتدريب بأمن المعلومات، 6) إدارة حوادث أمن المعلومات بشكل فاعل، 7) اتباع نهج فاعل لإدارة استمرارية الأعمال، 8) تقييم الأداء في إدارة أمن المعلومات والتغذية الراجعة، وهذه العوامل تؤثر في أمن المعلومات.

مشكلة الدراسة:

تعاني منظمات الأعمال في الجمهورية اليمنية من جوانب ضعف وقصور في أمن المعلومات (الجوانب التنظيمية، والتشريعية)؛ حيث أكدت العديد من التقارير على تدني مستوى أمن المعلومات فيما يتعلق بالقوانين، واللوائح، وفريق الاستجابة لحالات الطوارئ والحوادث، والسياسات العامة، والاستراتيجيات الوطنية، والمعايير، والتوعية والتدريب ([International Telecommunication Union [ITU & ABIresearch, 2015; ITU, 2017; ITU, 2019; ITU, 2021; National Cyber Security Index [NCSI], 2020)، وفي المؤتمر الأول لأمن المعلومات بصنعاء المنعقد في يونيو 2014م، أكد نائب رئيس الوزراء وزير الاتصالات على أن اليمن لا يملك تشريعا يحفظ للناس خصوصياتهم ويحمي ممتلكاتهم، وأكد أيضا على أهمية إنشاء مركز وطني لأمن المعلومات؛ بغرض الاستجابة لحوادث أمن المعلومات، واحتواء الحوادث وتجنبها مستقبلا (سبأ نت، 2014).

وقد أشارت دراسة الربيدي (2010) إلى أن العمليات المصرفية الإلكترونية في اليمن تواجه مخاطر في الوصول المصرح به، وخصوصية العملاء، وسلامة تجهيز البيانات، وتخزين البيانات، وتوصلت دراسة فاضل (2018) إلى أن البنوك التجارية في اليمن تواجه مخاطر تهدد سرية المعلومات، وسلامة وتكامل المعلومات، وخصوصية العملاء، وتوافر الأنظمة، وقد رصد الخبراء في Kaspersky تنصت وكالة الأمن القومي ([National Security Agency [NSA على الحواسيب الشخصية المصابة ببرامج التجسس

http://doi.org/10.59222/ustjmhs.1.2.1

في (30) دولة، ومنها اليمن، واستهدفت برامج التجسس الإلكترونية قطاع الاتصالات (Reuters, 2015)، وحدوث خلل فني أثناء الصيانة في إحدى شركات الاتصالات العاملة في اليمن؛ مما أدى إلى توقف خدمة الاتصالات لساعات (عدن الغد، 2014).

وقد أثرت الحوادث الأمنية سلبا في أمن نظم المعلومات، وأدت إلى انقطاع النظام، وتوقف الأعمال، وإلحاق أضرار بسمعة الشركة، وفقدان ثقة العملاء، وفقدان إيرادات؛ حيث تشير التقديرات إلى أن خسائر قطاع الاتصالات في اليمن من مارس 2015م إلى مارس 2020م بلغ 4.1 مليار دولار، ناتجة عن تدمير البنية التحتية، وقد تسببت الحرب في التأثير على سلامة المعلومات وخدمات الاتصالات وتوافرها، وتسبب انقطاع الكابل البحري في توقف الخدمات، وحدوث شلل في المعاملات المالية (وزارة الاتصالات وتقنية المعلومات، 2020).

ولا شك أن استخدام الضوابط الأمنية في منظمات الأعمال يمنع المخاطر أو يحد من آثارها السلبية؛ حيث أوضحت دراسة الربيدي (2010) أن إدارة البنوك في اليمن تقوم بحماية معلوماتها غالبا من خلال كلمات المرور، ومكافح الفيروسات، ووجود نظم للصلاحيات، والرقابة على النسخ الاحتياطية، والرقابة على الوصول المادي، والتشفير، وقد أشارت تلك الدراسة إلى وجود قصور في الضوابط الأمنية، أهمها: عدم وجود نسخ احتياطية للبيانات في مكان آمن، وعدم وجود خطة للطوارئ، وعدم وجود رقابة آلية، وعدم مراجعة مخرجات النظام المحاسبي، وعدم وجود سياسة مكتوبة لحماية الأجهزة والبرامج والبيانات.

وأكدت دراسة فاضل (2018) أن البنوك التجارية في اليمن تُنفذ آليات الحماية بشكل كاف وفاعل، ولكنها ليست منفذة بالشكل الأمثل، وتحتاج إلى تطوير وتحديث مستمر، وتتمثل آليات الحماية المنفذة في: أمن تعديل وتطوير النظم، يليها أمن المدخلات، ثم أمن الوسائط، وأمن المخرجات، وتوصلت دراسة فاضل إلى أن آليات الحماية لها تأثير إيجابي في أمن نظم المعلومات المحاسبية.

وذكر تقرير ITU وABIresearch (2015) أن التحقيق في الجرائم السيبرانية، وملاحقة مرتكبيها، وفرض عقوبات على الجناة تحد من مخاطر تكنولوجيا المعلومات، وقد أصدر البرلمان اليمني القانون رقم (40) لسنة (2006) بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية؛ يهدف إلى تعزيز الإشراف والرقابة، ويسري على التعاملات الإلكترونية (الجريدة الرسمية، 2006)، وأيضا أصدر البرلمان اليمني القانون رقم (13) لسنة (2012) بشأن حق الحصول على المعلومات الذي يتضمن حماية نظم وشبكات المعلومات من المخاطر (رئاسة الجمهورية، 2012)، وتقدمت الحكومة بمشروع قانون لمكافحة الجرائم الإلكترونية إلى مجلس النواب؛ بهدف ضبط الجرائم الإلكترونية.

وبناء على ما سبق، يلاحظ أن هناك ضعفا في الجوانب التشريعية، كما جاء في تصريح نائب رئيس الوزراء، ووجود مخاطر تستهدف سرية المعلومات وسلامتها وتوافرها، وفق ما جاء في الدراسات السابقة، واستهداف برامج التجسس الإلكترونية قطاع الاتصالات، وفق ما جاء في تقرير Kaspersky، وتوقف خدمات الاتصالات، والتأثير السلبي على سلامة المعلومات وخدمات الاتصالات وتوافرها وفق ما جاء في تقرير وزارة الاتصالات وتقنية المعلومات.

وتُعد سرية المعلومات وسلامتها وتوافرها في قطاع الاتصالات قضية جوهرية، وأي كشف للمعلومات السرية أو تعديلها أو عدم توافرها يؤثر سلبا في أمن نظم المعلومات المحاسبية، ويؤثر أيضا في سمعة الشركة، ويثير قلق العملاء، وبالتالي فإن تنفيذ الضوابط الأمنية الملائمة، وتحديثها باستمرار يؤدي دورا كبيرا في منع المخاطر، أو الحد من آثارها السلبية، وضمان أمن نظم المعلومات المحاسبية (الحفاظ على سرية المعلومات، وسلامتها، وتوافرها) في قطاع الاتصالات في اليمن.

واستنادا إلى نظرية الردع العام (Straub & Welke, 1998) فإن استخدام التدابير المضادة تحد من إساءة استخدام نظم المعلومات؛ حيث قدمت دراسة D'Arcy et al. (2009) نموذجا موسعا للنظرية يفترض أن وعي المستخدم بالتدابير المضادة يؤثر في نوايا المستخدمين المتعلقة بإساءة استخدام نظم

http://doi.org/10.59222/ustjmhs.1.2.1

المعلومات من خلال إدراك المستخدمين للعقوبة، ووفقا لنظرية أمن المعلومات (Horne et al., 2016) التي تنص على أن تطبيق الضوابط يؤدي إلى تحويل المعلومات إلى موارد، فإن استخدامها يساعد في تفسير الدوافع وراء الجهود الرامية إلى حماية المعلومات المستخدمة من قبل الأفراد والمجموعات والمنظمات؛ لذا فقد توسعت الدراسة الحالية في وجهات النظر المفاهيمية لنظرية الردع العام؛ لتشمل الضوابط التقنية والإدارية التي تساعد في الحفاظ على أمن نظم المعلومات المحاسبية من المخاطر.

ويتحقق أمن نظم المعلومات من خلال تطبيق المعايير المهنية، والالتزام بالسياسة الأمنية، والتوعية والتدريب في مجال الأمن، ودعم الإدارة العليا، وتدقيق الأمن بشكل منتظم، ودعم الأطر القانونية والتنظيمية، والاستفادة من الممارسات المثلى في تعزيز الأمن (Choejey et al., 2016; Keung, 2013; PwC, 2015; Riad, 2009)، وقد أكد المدققون على ضرورة تعزيز أمن نظم المعلومات المحاسبية وفقا لأحدث التطورات التكنولوجية (Bafghi, 2014)، وبالتالي فإن الدراسة الحالية تسعى إلى الإسهام في قياس أثر الضوابط الأمنية (التقنية، والإدارية) في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.

أسئلة الدراسة:

بناء على مشكلة الدراسة يمكن صياغة السؤال الآتي:

السؤال الرئيس: ما درجة أثر الضوابط الأمنية (التقنية، والإدارية) في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن؟ وسيتم الإجابة عن هذا السؤال من خلال الإجابة عن الأسئلة الفرعية الآتية:

- السؤال الفرعي الأول: ما درجة أثر الضوابط التقنية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن؟
- السؤال الفرعي الثاني: ما درجة أثر الضوابط الإدارية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن؟

أهداف الدراسة:

بناء على أسئلة الدراسة تم صياغة مجموعة من الأهداف التي تسعى الدراسة الحالية إلى تحقيقها، وهي:

الهدف الرئيس: قياس أثر الضوابط الأمنية (التقنية، والإدارية) في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن، ويتفرع هذا الهدف إلى الأهداف الفرعية الآتية:

- الهدف الفرعي الأول: قياس أثر الضوابط التقنية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.
- الهدف الفرعي الثاني: قياس أثر الضوابط الإدارية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.

أهمية الدراسة:

تتمثل أهمية الدراسة الحالية في الآتي:

أولا: الأهمية النظرية:

تتمثل الأهمية النظرية في تطوير أداة الدراسة التي تفيد في قياس أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية، وتسهم الدراسة الحالية في إظهار نتائج تأثر أمن نظم المعلومات المحاسبية بواسطة مفهوم أحدث للضوابط الأمنية، وأيضا تسهم في دراسة الضوابط الأمنية بأبعاد (الضوابط التقنية،

http://doi.org/10.59222/ustjmhs.1.2.1

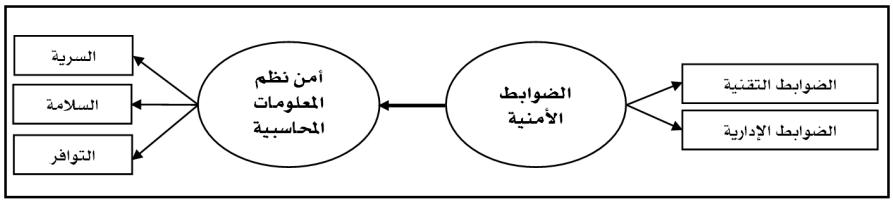
والضوابط الإدارية) مختلفة عن الأبعاد التي سبق دراستها، وكذلك استخدام نظرية الردع العام، ونظرية أمن المعلومات في تفسير العلاقة بين المتغيرات، وبناء نموذج معرفي جديد يستند على الدراسات السابقة، والنظريات العلمية المفسرة للعلاقة بين متغيرات الدراسة.

ثانيا: الأهمية العملية:

تتمثل الأهمية العملية في إمكانية استفادة مجلس الإدارة، والإدارة التنفيذية في قطاع الاتصالات مجتمع الدراسة وذلك من خلال إنشاء إدارة لأمن المعلومات تعمل على بناء وتطبيق نظام لإدارة أمن المعلومات وفق معايير دولية، وإمكانية استفادة كل من إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت في قطاع الاتصالات، وذلك من خلال تنفيذ الضوابط الأمنية الملائمة، وتلافي جوانب الضعف والقصور في الضوابط الأمنية.

النموذج المعرفي:

بناء على الخلفية النظرية والأدب السابق، تم بناء النموذج المعرفي للدراسة الحالية كما هو موضح في الشكل (1).

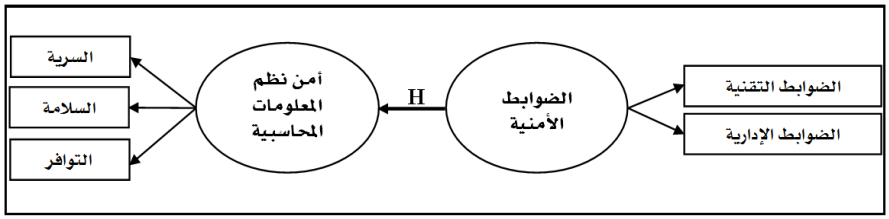


شكل (1): النموذج المعرفي للدراسة

فرضيات الدراسة:

استنادا إلى ما سبق من نظريات علمية (D'Arcy et al., 2009; Horne et al., 2016; Straub & Welke, 1998)، ودراسات سابقة (Al-ghananeem, 2014; Chang & Wang, 2011; Haeussinger & Kranz, 2013; Riad, 2009; Schuessler, 2009; Seno et al., 2015)، فإن أغلبها يشير إلى أن الضوابط الأمنية تؤثر بشكل إيجابي في أمن المعلومات، وبالتالي فقد تم تطوير الفرضية الرئيسية للدراسة الحالية على النحو الآتي:

H: تؤثر الضوابط الأمنية بشكل إيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن، والشكل (2) يوضح مسار هذه الفرضية.



شكل (2): مسار الفرضية الرئيسية

ويبين الشكل (2) الأثر المباشر للضوابط الأمنية في أمن نظم المعلومات المحاسبية؛ حيث يمثل الخط الواصل بين المتغيرين الفرضية الرئيسية، ويتفرع من هذه الفرضية الفرضيات الفرعية الآتية:

http://doi.org/10.59222/ustjmhs.1.2.1

أثر الضوابط التقنية في أمن نظم المعلومات المحاسبية:

بناء على ما سبق من نظريات علمية (D'Arcy et al., 2009; Horne et al., 2016; Straub & Welke, 1998)، **ودراسات سابقة** (Azees, Vijayakumar, & Deborah, 2016; Chang & Wang, 2011; Kankanhalli, Teo, Tan, & Wei, 2003; Schuessler, 2009)، **فإن أغلبها يؤكد على أن مؤشرات الضوابط التقنية تؤثر بشكل إيجابي في أمن المعلومات، وتلك الدراسات ركزت على مؤشرات الضوابط التقنية، ولم تتناول بُعد الضوابط التقنية بشكل مباشر، وبالتالي فقد تم تطوير الفرضية الفرعية الأولى للدراسة الحالية على النحو الآتي:**

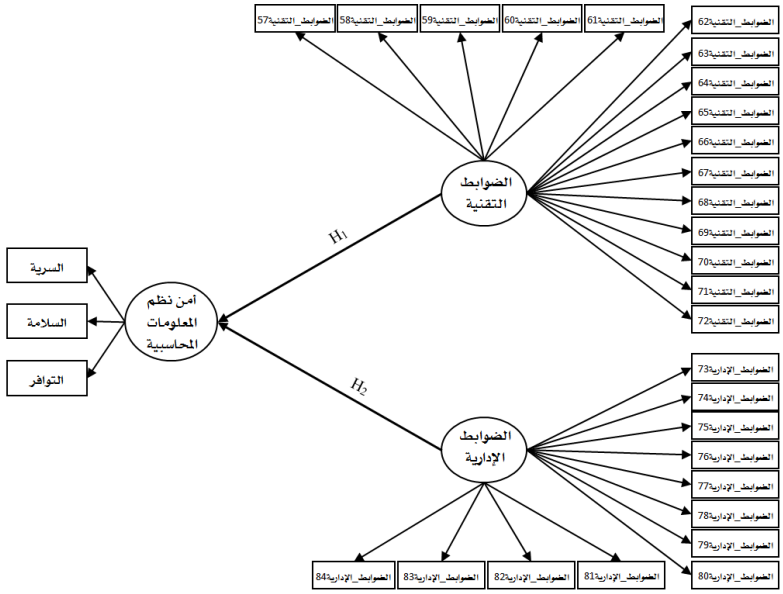
H_1: **تؤثر الضوابط التقنية بشكل إيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.**

أثر الضوابط الإدارية في أمن نظم المعلومات المحاسبية:

بناء على ما سبق من نظريات علمية (D'Arcy et al., 2009; Horne et al., 2016; Straub & Welke, 1998)، **ودراسات سابقة** (Al-ghananeem, 2014; Azees et al., 2016; Chang & Lin, 2007; Dinev & Hu, 2007; Haeussinger & Kranz, 2013; Kankanhalli et al., 2003; Schuessler, 2009)، **فإنها تؤكد في الغالب على أن مؤشرات الضوابط الإدارية تؤثر بشكل إيجابي في أمن المعلومات، وتلك الدراسات ركزت على مؤشرات الضوابط الإدارية، ولم تتناول بُعد الضوابط الإدارية بشكل مباشر، وبالتالي فقد تم تطوير الفرضية الفرعية الثانية للدراسة الحالية على النحو الآتي:**

H_2: **تؤثر الضوابط الإدارية بشكل إيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.**

ويوضح الشكل (3) مسار الفرضية الفرعية الأولى والفرضية الفرعية الثانية للفرضية الرئيسية.



شكل (3): مسار الفرضيات الفرعية

منهج الدراسة:

اعتمدت الدراسة الحالية على المنهج التحليلي، وتم استخدام أساليب الإحصاء الاستدلالي في تحقيق هدف الدراسة المتمثل في قياس أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية.

http://doi.org/10.59222/ustjmhs.1.2.1

مجتمع الدراسة وعينتها:

استهدفت الدراسة الحالية قطاع الاتصالات في اليمن الذي شمل المؤسسة العامة للاتصالات، وشركات الاتصالات الست: (سبأفون، تيليمن، يمن نت، إم تي إن، يمن موبايل، واي)، وهي تمثل مجتمع الدراسة، ونظرا لصعوبة مسح فروع هذه الشركات والمؤسسة العامة للاتصالات، وكون الكوادر الفنية ذات المهارات العالية تتواجد في المراكز الرئيسية، فقد تم الاكتفاء بالمراكز الرئيسية لشركات الاتصالات والمؤسسة العامة للاتصالات كعينة للدراسة دون فروعها.

ومن أجل الحصول على المعلومات اللازمة من مصدرها الملائم والأكثر قدرة على توفيرها لهذه الدراسة تم تحديد المدراء، ورؤساء الأقسام، والمشرفين، والمختصين المعنيين بأمن المعلومات في إدارة تكنولوجيا المعلومات، وإدارة الرقابة والتحكم، وإدارة التدقيق الفني، وإدارة تشغيل الشبكة والإنترنت في المراكز الرئيسية لشركات الاتصالات والمؤسسة العامة للاتصالات المتواجدة في العاصمة صنعاء والبالغ عددهم 356 فردا يشغل هذه الجهات المستهدفة بحسب معلومات إدارة الموارد البشرية، وتم جمع المعلومات عن قطاع الاتصالات من خلال النزول الميداني وتعاون المختصين في إدارة الموارد البشرية، ويوضح الجدول الآتي المجتمع المستهدف وحجم العينة ونسبة الاستجابة.

جدول (1): المجتمع المستهدف وحجم العينة ونسبة الاستجابة

م	الشركات والمؤسسة	الاستبانات		الاستبيانات الصالحة للتحليل في كل من إدارة				إجمالي الاستجابة	نسبة الاستجابة
		الموزعة	المستردة	الصالحة للتحليل	تكنولوجيا المعلومات	التدقيق الفني	الرقابة والتحكم	تشغيل الشبكة والإنترنت	
1	A	92	81	79	28	3	7	41	% 86
2	B	50	25	24	9	2	3	10	% 48
3	C	66	54	52	24	4	5	19	% 79
4	D	30	22	22	12	2	2	6	% 73
5	E	52	16	16	5	1	0	10	% 31
6	F	45	20	17	8	0	4	5	% 38
7	G	21	8	8	4	0	0	4	% 38
	الإجمالي	356	226	218	90	12	21	95	% 61
	النسبة	% 100	% 63	% 61	25.28%	% 3.37	% 5.90	26.69%	

ملاحظة: تم ترميز مجتمع الدراسة بناء على طلب بعض المستجيبين.

وقد تم توزيع 356 استبانة على جميع عناصر المجتمع من خلال النزول الميداني والموارد البشرية ومتعاونين، وتم استرداد 226 استبانة بنسبة 63 %، وقد كانت الاستبانات الصالحة للتحليل 218 استبانة بنسبة 61 % من الاستبانات الموزعة؛ وأما الاستبانات التي لم تسترد فعددها 130 استبانة بنسبة 37 % من الاستبانات الموزعة، ويرجع ارتفاع نسبة عدم الاستجابة إلى قلق بعض الموظفين من تقديم المعلومات اللازمة للدراسة؛ كون هذه المعلومات باعتقادهم سرية، وتقديمها قد يؤثر سلبا على الشركة.

وحدة التحليل:

تتمثل وحدة التحليل في المنظمة (المؤسسة العامة للاتصالات، وشركات الاتصالات)؛ كون أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية في الدراسة الحالية تقاس على مستوى المنظمة.

http://doi.org/10.59222/ustjmhs.1.2.1

أداة الدراسة:

تم تطوير أداة الدراسة الحالية المستخدمة في جمع البيانات عن أمن نظم المعلومات المحاسبية بالاعتماد على دراسة Chang وWang (2011)، ودراسة Al-ghananeem et al. (2014)، ودراسة Seno et al. (2015) كمصادر أصلية، وتم قياس أمن نظم المعلومات المحاسبية من خلال بُعد السرية الذي تضمن 9 فقرات، وبُعد السلامة الذي تضمن 9 فقرات، وبُعد التوافر الذي تضمن 10 فقرات. واعتمدت الدراسة الحالية في بناء الضوابط الأمنية أيضا على دراسة Loch، Carr، وWarkentin (1992)، ودراسة Whitman (2004)، ودراسة Hayale وAbu-Khadra (2006)، ودراسة Schuessler (2009)، ودراسة Riad (2009) كمصادر أصلية، وتم قياس الضوابط الأمنية من خلال بُعد الضوابط التقنية الذي تضمن 16 فقرة، وبُعد الضوابط الإدارية الذي تضمن 12 فقرة.

وقد تضمنت الاستبانة محورين رئيسين، وهما:

1. **المحور الأول: جمع بيانات عن مستوى أمن نظم المعلومات المحاسبية (المتغير التابع) في قطاع الاتصالات، كما هو موضح في الجدول (2).**

جدول (2): أبعاد وفقرات أمن نظم المعلومات المحاسبية

الأبعاد	عدد الفقرات	م	الفقرات تقيس الفقرات الآتية مستوى أمن نظم المعلومات المحاسبية في قطاع الاتصالات
السرية	9	1	المعلومات الحساسة في الشركة محمية من الكشف.
		2	خصوصية المعلومات الشخصية للعملاء محمية من الكشف.
		3	المعلومات المنقولة عبر الشبكة محمية من الاعتراض.
		4	حسابات المستخدمين على صفحات الويب الخاصة بالشركة محمية من الكشف.
		5	يتم الوصول إلى المعلومات من قبل موظفي الشركة بحسب صلاحيتهم.
		6	تفرض الشركة رقابة صارمة على الوصول المادي إلى الخوادم ووسائط التخزين.
		7	معلومات الشركة محمية من الوصول غير المصرح به.
		8	إعدادات نظام الشركة محمية من الوصول غير المصرح به.
		9	يتم مشاركة معلومات الشركة بين الأطراف المصرح لها.
السلامة	9	10	محتوى معلومات الشركة المخزنة دقيقة.
		11	محتوى معلومات الشركة المنقولة مطابقة للمعلومات الأصلية.
		12	معلومات الشركة محمية ضد التعديل غير المصرح به.
		13	إعدادات نظام الشركة محمية ضد التعديل غير المصرح به.
		14	يوفر نظام الشركة إمكانية التعرف على أي تعديلات حدثت للمعلومات.
		15	نظام الشركة يحمي المستخدمين من هجمات انتحال الهوية.
		16	يوفر نظام الشركة إمكانية التعرف على أي إتلاف حدث للمعلومات.
		17	معلومات الشركة محمية من الإتلاف غير المصرح به.
		18	أجهزة النظام ووسائط التخزين بالشركة محمية من الإتلاف.

http://doi.org/10.59222/ustjmhs.1.2.1

جدول (2): يتبع

الأبعاد	عدد الفقرات	م	الفقرات تقيس الفقرات الآتية مستوى أمن نظم المعلومات المحاسبية في قطاع الاتصالات
التوافر	10	19	تطبيقات نظم معلومات الشركة متاحة للمستخدمين المخولين.
		20	الموقع الخاص بالشركة متاح للمستخدمين دون انقطاع.
		21	الخدمات التي تقدمها أنظمة الشركة متاحة للمستخدمين طوال الوقت دون أي انقطاع.
		22	خوادم الشركة متاحة للمستخدمين المخولين باستمرار.
		23	النظام يُمكن المخولين من الوصول إلى المعلومات عند الطلب.
		24	توفر الشركة طاقة احتياطية للاستخدام عند انقطاع التيار.
		25	توفر الشركة موقع بديل لتشغيل نظم المعلومات في حال حدوث كوارث.
		26	سرعة الاستجابة لحوادث الأمن واستئناف العمليات.
		27	إمكانية استرداد بيانات وأنظمة الشركة بسرعة.
		28	نظام الشركة قادر على تلبية احتياجات جميع المستخدمين.

واستخدمت الدراسة الحالية مقياس ليكرت السباعي لأمن نظم المعلومات المحاسبية وفقا لدراسة Chang وWang (2011)، ودراسة Kankanhalli، Teo، Tan وWei (2003)؛ حيث تشير (7) إلى "موافق بشدة"، وهي تعني أن أمن نظم المعلومات المحاسبية في قطاع الاتصالات مرتفع جدا، ويشير (1) إلى "غير موافق بشدة"، وهي تعني أن أمن نظم المعلومات المحاسبية في قطاع الاتصالات منخفض جدا.

2. المحور الثاني: جمع بيانات عن مدى استخدام الضوابط الأمنية (المتغير المستقل) في قطاع الاتصالات، كما هو موضح في الجدول (3).

جدول (3): أبعاد وفقرات الضوابط الأمنية

الأبعاد	عدد الفقرات	م	الفقرات تستخدم شركات الاتصالات في حماية أنظمة المعلومات المحاسبية الضوابط الأمنية الآتية:
الضوابط التقنية	16	57	كلمة المرور.
		58	البطاقة الذكية.
		59	القياس الحيوي مثل بصمات الأصابع، أو الوجه، أو العين، أو الصوت.
		60	المصادقة القوية متعددة العوامل (تجمع بين عاملين أو أكثر مثل كلمة المرور، والبطاقة الذكية، والقياس الحيوي).
		61	ضوابط التحكم بالوصول المنطقي إلى موارد النظام مثل قواعد البيانات، أو الشبكات، أو التطبيقات.
		62	ضوابط التحكم بالوصول المادي مثل كاميرات المراقبة، وقارئ البطاقة، وأنظمة الإنذار، وإقفال الأبواب، والخزائن.
		63	مكافح الفيروسات، والديدان، وأحصنة طروادة.
		64	مكافح برامج التجسس.
		65	مكافح الاصطياد الإلكتروني.
		66	مكافح الرسائل المزعجة.
		67	الجدران النارية أو جدران الحماية.
		68	الشبكات الخاصة الافتراضية (توفر اتصال آمن للبيانات التي تنتقل عبر الشبكات).
		69	أنظمة منع التسلل (منع اختراقات النظام أو الشبكة).
		70	تشفير البيانات الحساسة.
		71	التوقيع الرقمي (المصادقة على صحة مضمون الرسالة).
		72	الشهادات الرقمية (التحقق من هوية المُرسل والمصادقة عليها).

http://doi.org/10.59222/ustjmhs.1.2.1

جدول (3): يتبع

الأبعاد	عدد الفقرات	م	الفقرات تستخدم شركات الاتصالات في حماية أنظمة المعلومات المحاسبية الضوابط الأمنية الآتية:
الضوابط الإدارية	12	73	خطة التعافي من الكوارث (إجراءات الوقاية من الكوارث والاستعداد لها).
		74	خطة الاستجابة لحوادث الأمن (إجراءات التصدي للهجمات).
		75	النسخ الاحتياطي للبيانات والأنظمة بشكل دوري.
		76	إجراءات التدقيق الداخلي (اختبار الضوابط الأمنية).
		77	إجراءات التدقيق الخارجي (اختبار الضوابط الأمنية).
		78	تطبيق سياسة أمن المعلومات.
		79	مراجعة وتحديث سياسة أمن المعلومات.
		80	تنفيذ برامج التوعية والتدريب في مجال الأمن بشكل دوري.
		81	تحسين برامج التوعية والتدريب في مجال الأمن.
		82	إبلاغ سلطات إنفاذ القانون بالحوادث الأمنية بعد وقوعها.
		83	إبلاغ فريق الاستجابة لطوارئ الحاسوب بالحوادث الأمنية.
		84	الامتثال للقوانين واللوائح المتعلقة بحماية البيانات.

واستخدمت الدراسة الحالية مقياس ليكرت السباعي للضوابط الأمنية وفقا لدراسة Loch et al. (1992)، ودراسة Schuessler (2009)؛ حيث تشير (7) إلى "تُستخدم على نطاق واسع"، وهي تعني أن استخدام الضوابط الأمنية في قطاع الاتصالات مرتفع جدا، ويشير (1) إلى "قليلة الاستخدام أو معدومة"، وهي تعني أن استخدام الضوابط الأمنية في قطاع الاتصالات منخفض جدا.

اختبار صدق المحتوى للأداة:

تم عرض الاستبانة على عدد من المحكمين المتخصصين أكاديميا ومهنيا وإحصائيا؛ وذلك للتأكد من أن فقرات الاستبانة كافية وشاملة لقياس مستوى أمن نظم المعلومات المحاسبية، وقياس مدى استخدام الضوابط الأمنية في قطاع الاتصالات، وقد أبدى المحكمون آراءهم، وقدموا ملحوظاتهم ومقترحاتهم حول تعديل بعض الفقرات، أو حذفها، أو إعادة صياغتها، أو إضافة فقرات جديدة؛ لتحسين الاستبانة، وتم إجراء التعديلات اللازمة بناء على ملحوظات المحكمين.

اختبار صدق وثبات اداة الدراسة:

تم اختبار صدق وثبات أداة الدراسة من خلال تقييم نموذج القياس.

الأساليب الإحصائية المستخدمة:

استخدمت الدراسة الحالية نمذجة المعادلة البنائية القائمة على المربعات الصغرى الجزئية (PLS-SEM) في تقييم نموذج القياس، وتقييم النموذج البنائي، واختبار الفرضيات.

نتائج الدراسة ومناقشتها:

تم تقييم نموذج البحث باستخدام طريقة المربعات الصغرى الجزئية (SmartPLS) الإصدار (v.3.2.8) على مرحلتين: تتمثل المرحلة الأولى في تقييم نموذج القياس (Measurement Model)، وعندما يحقق نموذج القياس المعايير المطلوبة، يتم الانتقال إلى مرحلة تقييم النموذج البنائي (Structural Model) (Hair, Risher, Sarstedt, & Ringle, 2019).

http://doi.org/10.59222/ustjmhs.1.2.1

المرحلة الأولى: تقييم نموذج القياس:

يصف نموذج القياس (النموذج الخارجي Outer model**) العلاقات بين الأبعاد وفقراتها (**Hair, Hult, Ringle, & Sarstedt, 2017**)، ويتم تقييم نموذج القياس من خلال الاختبارات الخاصة بالصدق والثبات؛ حيث يشير صدق** Validity **المقياس إلى قدرة أداة القياس على تحقيق الغرض الذي أنشئت من أجله، ويعبر صدق المقياس عن دقته، ويشير ثبات** Reliability **المقياس إلى القدرة على قياس المطلوب تحت عدة ظروف (التوصل إلى نفس النتائج عند إعادة الاختبار)، ويعبر ثبات المقياس عن اتساقه (**Hair et al., 2014**).**

أولا: تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الأولى:

تكون العلاقة السببية من المتغيرات إلى الفقرات؛ حيث يكون اتجاه السهم من البُعد إلى الفقرة، ويجب أن يكون الارتباط بين فقرات البُعد عاليا، ويمكن حذف بعض الفقرات من البُعد دون أن تؤثر على البُعد كليا (Hair et al., 2019; Hair et al., 2017**).**

الخطوة الأولى: تقييم ثبات المؤشر:

يتحقق الثبات عندما يكون التشبع الخارجي لكل فقرة أعلى من (0.708**)؛ وهذا يعني أن البُعد يفسر أكثر من** 50 % **من تباين فقراته (**Hair et al., 2019**)، ويتضح من نتائج تقييم ثبات المؤشر أن عدد الفقرات التي يجب حذفها (**12**) فقرة وفقا للأسباب الآتية: (**1**) تم حذف الفقرات التي تشبعها أقل من (**0.708**)، وقد أدى حذفها إلى زيادة الثبات المركب ومتوسط التباين المفسر، وهي: الضوابط التقنية**57**، والضوابط التقنية**58**، والضوابط التقنية**59**، والضوابط التقنية**60**، والضوابط التقنية**71**، والضوابط الإدارية**75**.** (**2**) **تم حذف الفقرات التي تقلل من صدق التمايز بين الأبعاد على الرغم من أن تشبعها أعلى من (**0.708**) وفقا لـ** Hair et al. (2017)**، وهي: السرية** 1**، والسلامة** 10**، والسلامة** 11**، والسلامة** 13**، والتوافر** 19**، والتوافر** 22**.** (**3**) **فقرة الضوابط التقنية**64 **تشبعها أقل من (**0.708**)، ومع ذلك لم تُحذف؛ لأن حذفها لا يؤدي إلى زيادة الثبات المركب أو متوسط التباين المفسر. وبعد حذف تلك الفقرات يمكن القول إن جميع الفقرات المتبقية تقيس الأبعاد بدرجة عالية من الثبات، ويوضح الجدول (**4**) التشبع الخارجي للفقرات المتبقية بعد الحذف.**

http://doi.org/10.59222/ustjmhs.1.2.1

جدول (4): تقييم نموذج القياس

المتغيرات	الأبعاد	الفقرات	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
أمن نظم المعلومات المحاسبية	السرية	السرية 2	0.765	0.918	0.933	0.637
		السرية 3	0.827			
		السرية 4	0.771			
		السرية 5	0.755			
		السرية 6	0.815			
		السرية 7	0.860			
		السرية 8	0.844			
		السرية 9	0.738			
	السلامة	السلامة 12	0.782	0.906	0.928	0.682
		السلامة 14	0.820			
		السلامة 15	0.792			
		السلامة 16	0.867			
		السلامة 17	0.867			
		السلامة 18	0.822			
	التوافر	التوافر 20	0.813	0.932	0.943	0.676
		التوافر 21	0.835			
		التوافر 23	0.821			
		التوافر 24	0.806			
		التوافر 25	0.751			
		التوافر 26	0.865			
		التوافر 27	0.830			
		التوافر 28	0.853			

http://doi.org/10.59222/ustjmhs.1.2.1

جدول (4):يتبع

المتغيرات	الأبعاد	الفقرات	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
الضوابط الأمنية	الضوابط التقنية	الضوابط_التقنية61	0.700	0.929	0.939	0.586
		الضوابط_التقنية62	0.725			
		الضوابط_التقنية63	0.700			
		الضوابط_التقنية64	0.838			
		الضوابط_التقنية65	0.820			
		الضوابط_التقنية66	0.797			
		الضوابط_التقنية67	0.819			
		الضوابط_التقنية68	0.806			
		الضوابط_التقنية69	0.774			
		الضوابط_التقنية70	0.706			
		الضوابط_التقنية72	0.717			
	الضوابط الإدارية	الضوابط_الإدارية73	0.744	0.944	0.952	0.642
		الضوابط_الإدارية74	0.755			
		الضوابط_الإدارية76	0.845			
		الضوابط_الإدارية77	0.848			
		الضوابط_الإدارية78	0.800			
		الضوابط_الإدارية79	0.825			
		الضوابط_الإدارية80	0.755			
		الضوابط_الإدارية81	0.794			
		الضوابط_الإدارية82	0.822			
		الضوابط_الإدارية83	0.774			
		الضوابط_الإدارية84	0.840			

الخطوة الثانية: تقييم ثبات الاتساق الداخلي:

تم استخدام الثبات المركب (Composite Reliability [CR]) في تقييم الاتساق الداخلي، وتتراوح قيمة الثبات المركب بين (0 و1)؛ حيث تشير القيم العالية إلى درجات عالية من الثبات، ويجب أن تكون قيمة الثبات المركب للبُعد بين (0.70 – 0.95)، فإذا كانت أكبر من (0.95) فإنها تُعد مشكلة، وتظهر أن الفقرات متشابهة، وتؤثر على مصداقية البيانات، وتؤدي إلى زيادة الخطأ، أيضا يمكن استخدام معامل ألفا كرونباخ (α) Cronbach's alpha كمقياس آخر لتقييم ثبات الاتساق الداخلي، وله نفس قيم الثبات المركب، ولكن ينتج عنه قيم أقل دقة من الثبات المركب (Hair et al., 2017).

وقد أظهرت النتائج في الجدول (4) أن قيم الثبات المركب (CR) للأبعاد تتراوح بين (0.928) و(0.952)، وقيم ألفا كرونباخ للأبعاد تتراوح بين (0.906) و (0.944)، وتشير هذه النتيجة إلى أن الاتساق الداخلي لجميع الأبعاد ذات ثبات عالٍ، وبالتالي يمكن القول إن جميع الأبعاد تقيس المتغيرين المستقل والتابع بدرجة عالية من الثبات.

الخطوة الثالثة: تقييم صدق التقارب:

يجب أن يكون متوسط التباين المفسر (Average variance extracted [AVE]) (0.50) أو أعلى لتوضح أن البُعد يفسر (50 %) أو أكثر من التباين في الفقرات التابعة له، وإذا كانت أقل من (0.50) فإن ذلك يشير إلى وجود تباين متبقٍ؛ أي توجد أخطاء في الفقرات (Hair et al., 2017).

http://doi.org/10.59222/ustjmhs.1.2.1

ويظهر في الجدول (4) أن قيم متوسط التباين المفسر (AVE) لجميع الأبعاد تتراوح بين (0.586) و(0.682)، ويلاحظ أن هذه القيم تقع ضمن النطاق الموصى به، وهذا يشير إلى أن البُعد يفسر أكثر من (50 %) من التباين في فقراته، وهذا يدل على تحقق صدق تقارب الأبعاد.

الخطوة الرابعة: تقييم صدق التمايز:

إثبات صحة التمايز يعني أن البُعد يتميز عن الأبعاد الأخرى ويعكس ظواهر لا تمثلها الأبعاد الأخرى في النموذج (Hair et al., 2017)، ويمكن تقييم صدق التمايز من خلال الطرق الآتية:

1) **طريقة التشبعات المتقاطعة:**

تُبين هذه الطريقة صدق تمايز الفقرة التي يجب أن يكون تشبعات الفقرات التابعة للبُعد أكبر من تشبعاتها المتقاطعة مع الأبعاد الأخرى (Hair et al., 2017)، وقد أظهرت النتائج في الجدول (5) أن تشبعات الفقرات التابعة لكل بُعد (القيم الغامقة) أعلى من تشبعاتها المتقاطعة مع الأبعاد الأخرى، وتشير هذه النتيجة إلى عدم تداخل فقرات القياس فيما بينها؛ أي أن فقرات كل بُعد تتميز عن فقرات الأبعاد الأخرى.

جدول (5): تقييم صدق تمايز الفقرات باستخدام طريقة التشبعات المتقاطعة

الفقرات / الأبعاد	التوافر	السرية	السلامة	الضوابط الإدارية	الضوابط التقنية
التوافر 20	**0.813**	0.523	0.643	-0.237	-0.311
التوافر 21	**0.835**	0.609	0.657	-0.316	-0.345
التوافر 23	**0.821**	0.694	0.740	-0.306	-0.339
التوافر 24	**0.806**	0.551	0.571	-0.195	-0.229
التوافر 25	**0.751**	0.424	0.496	-0.270	-0.340
التوافر 26	**0.865**	0.595	0.643	-0.325	-0.379
التوافر 27	**0.830**	0.566	0.656	-0.319	-0.354
التوافر 28	**0.853**	0.589	0.664	-0.354	-0.418
السرية 2	0.523	**0.765**	0.573	-0.323	-0.347
السرية 3	0.564	**0.827**	0.643	-0.384	-0.327
السرية 4	0.471	**0.771**	0.613	-0.424	-0.354
السرية 5	0.479	**0.755**	0.563	-0.282	-0.233
السرية 6	0.545	**0.815**	0.614	-0.294	-0.284
السرية 7	0.640	**0.860**	0.691	-0.377	-0.325
السرية 8	0.630	**0.844**	0.673	-0.352	-0.308
السرية 9	0.558	**0.738**	0.539	-0.301	-0.335
السلامة 12	0.668	0.694	**0.782**	-0.293	-0.326
السلامة 14	0.615	0.509	**0.820**	-0.161	-0.257
السلامة 15	0.694	0.646	**0.792**	-0.405	-0.387
السلامة 16	0.588	0.588	**0.867**	-0.198	-0.244
السلامة 17	0.626	0.717	**0.867**	-0.386	-0.363
السلامة 18	0.615	0.654	**0.822**	-0.190	-0.264
الضوابط_الإدارية73	0.516	0.425	0.468	**0.744**	0.573
الضوابط_الإدارية74	0.478	0.395	0.453	**0.755**	0.556
الضوابط_الإدارية76	0.501	0.465	0.477	**0.845**	0.613

http://doi.org/10.59222/ustjmhs.1.2.1

جدول (5): يتبع

الفقرات / الأبعاد	التوافر	السرية	السلامة	الضوابط الإدارية	الضوابط التقنية
الضوابط_الإدارية77	0.518	0.481	0.495	**0.848**	0.611
الضوابط_الإدارية78	0.477	0.474	0.490	**0.800**	0.626
الضوابط_الإدارية79	0.497	0.451	0.448	**0.825**	0.559
الضوابط_الإدارية80	0.449	0.295	0.388	**0.755**	0.431
الضوابط_الإدارية81	0.473	0.315	0.401	**0.794**	0.450
الضوابط_الإدارية82	0.519	0.334	0.414	**0.822**	0.492
الضوابط_الإدارية83	0.494	0.293	0.358	**0.774**	0.457
الضوابط_الإدارية84	0.526	0.459	0.440	**0.840**	0.607
الضوابط_التقنية61	0.397	0.462	0.403	0.484	**0.700**
الضوابط_التقنية62	0.387	0.446	0.391	0.496	**0.725**
الضوابط_التقنية63	0.406	0.439	0.383	0.354	**0.700**
الضوابط_التقنية64	0.412	0.442	0.311	0.504	**0.838**
الضوابط_التقنية65	0.435	0.426	0.332	0.552	**0.820**
الضوابط_التقنية66	0.422	0.400	0.345	0.506	**0.797**
الضوابط_التقنية67	0.471	0.519	0.473	0.464	**0.819**
الضوابط_التقنية68	0.488	0.467	0.422	0.558	**0.806**
الضوابط_التقنية69	0.553	0.505	0.488	0.625	**0.774**
الضوابط_التقنية70	0.419	0.427	0.492	0.537	**0.706**
الضوابط_التقنية72	0.444	0.446	0.460	0.624	**0.717**

2) طريقة نسبة أحادية وتغاير السمة:

يجب أن تكون قيمة نسبة أحادية وتغاير السمة (Heterotrait-monotrait ratio [HTMT]) **أقل من** (0.85)؛ **لتدل على عدم وجود ارتباط عال بين البُعد وبقية الأبعاد الأخرى، وأن البُعد متميز أو مختلف عن بقية الأبعاد الأخرى** (Henseler, Ringle, & Sarstedt, 2015).

وقد أشارت النتائج في الجدول (6) **إلى أن جميع قيم نسبة أحادية وتغاير السمة** HTMT **تتراوح بين** (0.53) **كحد أدنى و**(0.84) **كحد أعلى، ويلاحظ أن هذه القيم أقل من** (0.85)، **وتشير هذه النتيجة إلى صدق تمايز الأبعاد، وعدم وجود ارتباط عالٍ بين البُعد وبقية الأبعاد الأخرى، وأن البُعد مختلف عن بقية الأبعاد الأخرى.**

جدول (6): **تقييم صدق تمايز الأبعاد باستخدام طريقة نسبة أحادية وتغاير السمة** (HTMT)

الأبعاد	التوافر	السرية	السلامة	الضوابط الإدارية	الضوابط التقنية
التوافر					
السرية	0.746				
السلامة	0.835	0.840			
الضوابط الادارية	0.648	0.530	0.587		
الضوابط التقنية	0.611	0.638	0.576	0.719	

http://doi.org/10.59222/ustjmhs.1.2.1

ثانيا: تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الثانية:

استخدمت الدراسة الحالية طريقة المرحلتين المنفصلة في تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الثانية؛ كونها الأنسب؛ لأن عدد الفقرات في الأبعاد غير متساوية؛ حيث يتم قياس أبعاد الدرجة الأولى في المرحلة الأولى بدون قياس أبعاد الدرجة الثانية، ومن ثم يتم استخدام المتوسطات المعيارية لأبعاد الدرجة الأولى كمؤشرات لأبعاد الدرجة الثانية في المرحلة الثانية. وقد أشارت نتائج تقييم النموذج القياسي الانعكاسي من الدرجة الثانية إلى الآتي:

1) **ثبات المؤشر (الأبعاد من الدرجة الأولى):**

يتضح من الجدول (7) أن تشبع جميع مؤشرات المتغيرات أكبر من (0.708)؛ وهذا يدل على أن أبعاد الدرجة الأولى (تظهر كمؤشرات لأبعاد الدرجة الثانية) تتمتع بثبات عالٍ.

2) **ثبات الاتساق الداخلي (الأبعاد من الدرجة الثانية):**

يتضح من الجدول (7) أن جميع قيم الثبات المركب CR وقيم ألفا كرونباخ أعلى من (0.70) وأقل من (0.95)؛ وهذا يدل على أن الاتساق الداخلي لأبعاد الدرجة الثانية تتمتع بثبات عالٍ.

3) **صدق التقارب (الأبعاد من الدرجة الثانية):**

يظهر في الجدول (7) أن جميع قيم متوسط التباين المفسر AVE أكبر من (0.50)؛ وهذا يدل على وجود تقارب بين كل بُعد من الدرجة الثانية وأبعاده من الدرجة الأولى.

جدول (7): تقييم ثبات المؤشر، والاتساق الداخلي، وصدق التقارب

الأبعاد من الدرجة الثانية (المتغيرات)	الأبعاد من الدرجة الأولى (المؤشرات)	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
أمن نظم المعلومات المحاسبية	السرية	0.901	0.899	0.937	0.832
	السلامة	0.927			
	التوافر	0.907			
الضوابط الأمنية	الضوابط التقنية	0.922	0.810	0.913	0.840
	الضوابط الإدارية	0.911			

4) **صدق التمايز (الأبعاد من الدرجة الثانية):**

يلاحظ من الجدول (8) أن قيم HTMT أقل من (0.85)، وهذا يشير إلى صدق تمايز الأبعاد من الدرجة الثانية، وأنه لا يوجد ارتباط عالٍ بين البُعد من الدرجة الثانية وبقية الأبعاد الأخرى، وأن البُعد من الدرجة الثانية مختلف عن بقيةً الأبعاد الأخرى.

جدول (8): تقييم صدق تمايز أبعاد الدرجة الثانية باستخدام طريقة (HTMT)

المتغيرات	الضوابط الأمنية	أمن نظم المعلومات المحاسبية
الضوابط الأمنية		
أمن نظم المعلومات المحاسبية	0.780	

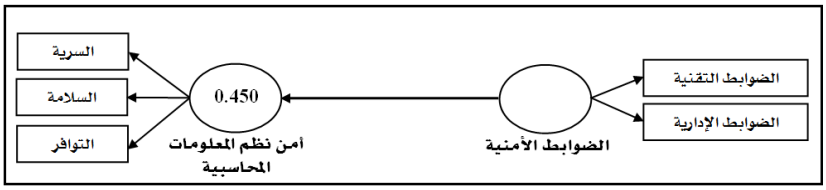
المرحلة الثانية: تقييم النموذج البنائي للمتغيرات الكلية من الدرجة الثانية:

أكدت نتائج تقييم نموذج القياس الانعكاسي أن المقاييس تتسم بالصدق والثبات، وفي هذه المرحلة سوف يتم تقييم النموذج البنائي (النموذج الداخلي Inner model) لاختبار مستوى الترابط والعلاقة فيما بين المتغيرات باستخدام نمذجة المعادلة البنائية القائمة على المربعات الصغرى الجزئية (PLS-SEM).

http://doi.org/10.59222/ustjmhs.1.2.1

أولا: معامل التحديد R^2:

يُفسر معامل التحديد التباين الكلي في المتغيرات الكامنة الداخلية (قدرة المتغيرات المستقلة على تفسير التباين في المتغير التابع)، ومعامل التحديد مقياس للقوة التفسيرية للنموذج، وتتراوح قيمة معامل التحديد R^2 بين (0 و1)؛ حيث تشير القيم العليا إلى مستويات أعلى في القوة التفسيرية، ويتم تحديد قدرة النموذج البحثي على تفسير المتغير التابع من خلال قيمة معامل التحديد R^2 التي تقدر بـ (0.67) أو (0.33) أو (0.19)؛ أي أنها قوية، أو متوسطة، أو ضعيفة على التوالي وفقا لـ Chin (1998). ويوضح الشكل (4) نتائج تقييم معامل التحديد.



شكل (4): تقييم معامل التحديد (R^2)

يظهر في الشكل (4) أن قيمة معامل تحديد R^2 أمن نظم المعلومات المحاسبية هي (0.450)؛ وهذا يشير إلى أن الضوابط الأمنية تفسر ما نسبته 45 % من التباين في أمن نظم المعلومات المحاسبية؛ وهذا يدل على أن القوة التفسيرية للنموذج متوسطة.

ثانيا: ملائمة التنبؤ (Q^2):

عندما تكون قيمة ملائمة التنبؤ Q^2 أكبر من الصفر فإن للنموذج أهمية تنبؤية، وكلما زادت القيمة زادت الأهمية، وإذا كانت مساوية للصفر فيُعد ذلك مؤشرا على أن النموذج ليس لديه دقة تنبؤية وغير ملائم من حيث التنبؤ، وكقاعدة عامة فإن قيم ملائمة التنبؤ Q^2 أعلى من (0) أو (0.25) أو (0.50)، وهذا يشير إلى أن الملائمة التنبؤية منخفضة أو متوسطة أو عالية لنموذج مسار PLS على التوالي (Hair et al., 2019, 19). والجدول (9) يُبين نتائج تقييم ملائمة النموذج للتنبؤ.

جدول (9): تقييم ملائمة التنبؤ على مستوى أبعاد أمن نظم المعلومات المحاسبية (المتغير التابع)

الأبعاد	(SSO) مجموع مربع المشاهدات	(SSE) مجموع مربع أخطاء التنبؤ	Q^2 (=1-SSE/SSO) ملائمة التنبؤ	التقدير
السرية	218	138.706	0.364	متوسطة
السلامة	218	140.526	0.355	متوسطة
التوافر	218	131.671	0.396	متوسطة

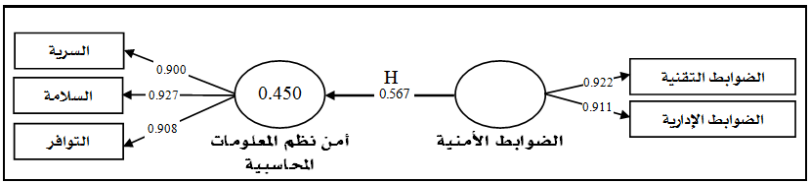
يظهر الجدول (9) نتائج تقييم ملائمة التنبؤ على مستوى أبعاد أمن نظم المعلومات المحاسبية؛ حيث تشير القيم إلى أن ملائمة النموذج للتنبؤ Q^2 متوسطة لكل من السرية والسلامة والتوافر.

ثالثا: تقييم معاملات المسار:

تقع قيم معاملات المسار ضمن نطاق (±1)، وتمثل القيم القريبة من (+1) علاقة إيجابية قوية، والقيم القريبة من (−1) علاقات سلبية قوية، وعادة ما تكون ذات دلالة إحصائية، وكلما كانت معاملات المسار المقدرة أقرب إلى (0) كانت العلاقات ضعيفة (Hair et al., 2017)؛ حيث إن التغيير في المتغير المستقل بدرجة واحدة ينشأ عنها تغيير في المتغير التابع بقدر حجم معامل المسار على فرض ثبات جميع المتغيرات الأخرى ومعاملات مساراتها (Hair et al., 2010).

http://doi.org/10.59222/ustjmhs.1.2.1

وقد تم إجراء Bootstrapping باستخدام حزمة برامج المربعات الصغرى الجزئية (PLS) لاختبار الفرضيات المقترحة بين متغيرات الدراسة الحالية، من خلال استخدام (5000) عينة فرعية (Hair et al., 2019)، وبالاعتماد على قيمة t-value التي ينبغي أن تكون أعلى من (1.96) لقبول الفرضية عند مستوى ($p < 0.05$)، وأعلى من (2.58) لقبول الفرضية عند مستوى ($p < 0.01$) (Hair et al., 2017). ويوضح الشكل (5) نتائج تقييم معاملات المسار.



شكل (5): تقييم معاملات المسار

نتائج اختبار فرضيات الدراسة:

أولا: اختبار الفرضية الرئيسية:

H: تؤثر الضوابط الأمنية بشكل إيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن، ويظهر الجدول (10) نتائج اختبار الفرضية الرئيسية.

جدول (10): اختبار الفرضية الرئيسية

المسار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
الضوابط الأمنية ← أمن نظم المعلومات المحاسبية	0.567	0.076	7.509	0.000

أظهرت النتائج في الجدول (10) أن الضوابط الأمنية تؤثر بشكل إيجابي في أمن نظم المعلومات المحاسبية؛ حيث كانت قيمة معامل المسار (β=0.567)، وقيمة (t=7.509) دالة إحصائيا عند مستوى دلالة أقل من (0.01)، وهذا يعني أن التغيير (الزيادة) في الضوابط الأمنية بدرجة واحدة ينشأ عنها زيادة في أمن نظم المعلومات المحاسبية بنسبة (56.7 %)، وبالتالي تدعم هذه النتيجة صحة الفرضية الرئيسية.

وهذه النتيجة تتفق مع نظرية أمن المعلومات (Horne et al., 2016) التي تشير إلى أن العلاقة بين الضوابط والمعلومات إيجابية، حيث تؤدي الضوابط إلى حماية المعلومات بشكل إيجابي، وتطبيق ضوابط الحماية يؤدي إلى تحويل المعلومات إلى موارد، أيضا تتفق مع نظرية الردع العام (Straub & Welke, 1998) التي تفترض إجراءات عامة تقلل من المخاطر بشكل مباشر أو غير مباشر من خلال استخدام التدابير المضادة، وكذلك تتفق مع دراسة Riad (2009) التي أشارت إلى أن الضوابط الأمنية تؤثر بشكل إيجابي في أمن المعلومات، وتتفق مع دراسة Chang وWang (2011) التي توصلت إلى أن موارد نظم المعلومات لها تأثير إيجابي ودال إحصائيا في أمن المعلومات، وأشارت دراسة Al-ghananeem (2014) إلى أن معايير إدارة أمن المعلومات تؤثر بشكل إيجابي وقوي في ضمان أمن المعلومات، وتوصلت دراسة Schuessler (2009) إلى أن الإجراءات المضادة ترتبط بشكل إيجابي بفاعلية أمن نظم المعلومات، وأكدت دراسة Seno et al. (2015) أن العلاقة بين عناصر أمن المعلومات (السرية والسلامة، والتوافر) وتدابير أمن المعلومات في الخدمات المصرفية الإلكترونية هي علاقة قوية ومباشرة.

ويُفسر هذا الاتفاق إلى حد كبير مع نتيجة الدراسة الحالية إلى إدراك منظمات الأعمال في مختلف البيئات والقطاعات بأهمية الضوابط الأمنية في تأمين أنظمة المعلومات، ويحقق تنفيذ الضوابط الأمنية الملائمة أهداف أمن نظم المعلومات المتمثل في الحفاظ على سرية المعلومات وسلامتها وتوافرها، ويؤدي

http://doi.org/10.59222/ustjmhs.1.2.1

تطبيق الضوابط الأمنية وتحديثها باستمرار إلى التصدي لأنشطة الهجوم وكشفها، والاستجابة للحوادث الأمنية، وتعزيز الموقف الدفاعي والتنافسي للشركة، وبالتالي تحسين مستوى أمن المعلومات (فكلما زاد تطبيق مجموعة ملائمة من الضوابط الأمنية زاد مستوى أمن نظم المعلومات المحاسبية).

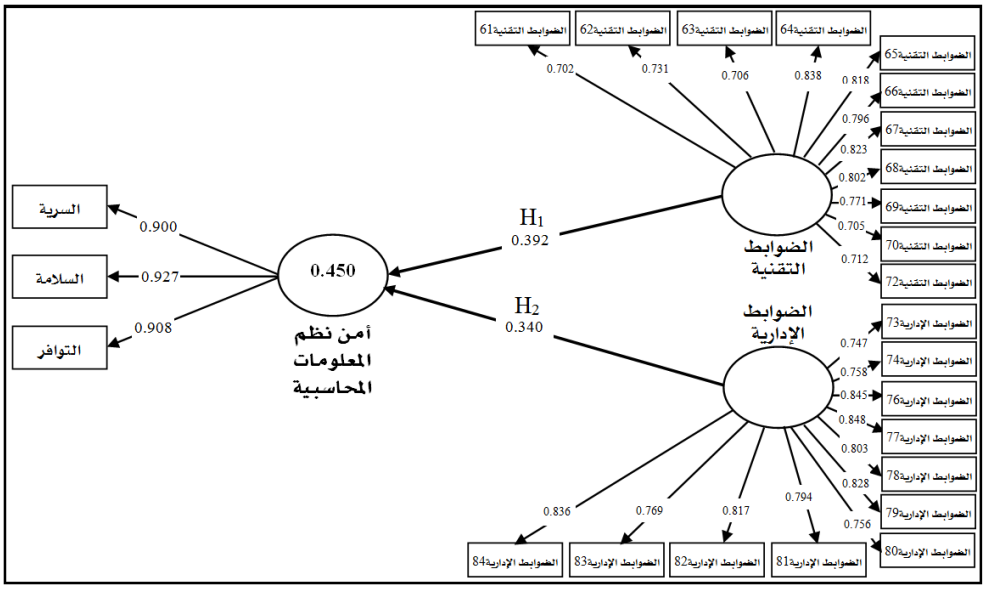
ثانيا: اختبار الفرضيات الفرعية للفرضية الرئيسية:

ويتفرع من الفرضية الرئيسية فرضيتان فرعيتان، تتمثلان بالآتي:

H_1: تؤثر الضوابط التقنية بشكل إيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.

H_2: تؤثر الضوابط الإدارية بشكل إيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن.

ويوضح الشكل (6) تقييم معاملات المسار لكل بُعد من أبعاد المتغيرات.



شكل (6): تقييم معاملات المسار لكل بُعد من أبعاد المتغير المستقل مع المتغير التابع

يظهر في الشكل (6) خروج خطين من الضوابط التقنية والإدارية إلى أمن نظم المعلومات المحاسبية ومحدد على كل خط قيمة معامل المسار، وقيمة معامل تحديد R^2 أمن نظم المعلومات المحاسبية بمقدار (0.450)؛ وهذا يشير إلى أن الضوابط التقنية والضوابط الإدارية تُفسر ما نسبته (45 %) من التباين في أمن نظم المعلومات المحاسبية، ويبين الجدول (11) نتائج اختبار الفرضيات الفرعية للفرضية الرئيسية.

جدول (11): اختبار الفرضيات الفرعية للفرضية الرئيسية

م	المسار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
1	الضوابط التقنية ← أمن نظم المعلومات المحاسبية	0.392	0.095	4.127	0.000
2	الضوابط الإدارية ← أمن نظم المعلومات المحاسبية	0.340	0.075	4.510	0.000

http://doi.org/10.59222/ustjmhs.1.2.1

الفرضيــة الفرعيــة الأولى: أظهرت النتائج في الجدول (11) أن الضوابط التقنية تؤثر بشــكل إيجابي في أمن نظم المعلومات المحاســبية؛ حيث جاءت قيمة معامل المســار (β=0.392)، وقيمة (t=4.127) دالة إحصائيا عند مســتوى دلالة أقل من (0.01)؛ وهذا يعني أنه كلما زادت الضوابط التقنية بدرجة واحدة زاد أمن نظم المعلومات المحاسبية بنسبة (39.2 %)، وتدعم هذه النتيجة صحة الفرضية الفرعية الأولى للفرضية الرئيسية.

وتتفــق هــذه النتيجة مع نظرية الــردع العــام (Straub & Welke, 1998) التي تشــير إلى أن جهود الوقايــة أو الكشــف تســاعد في منع أو كشــف إســاءة اســتخدام أنظمة المعلومــات، وتتفق مع دراســة Kankanhalli et al. (2003) الــتي وجدت أن الجهود الوقائية (برامج أمنية) ترتبط بشــكل إيجابي بفاعليــة أمن نظم المعلومات، وأن الجهود الوقائية تؤدي إلى زيادة فاعلية أمن نظم المعلومات، وتســهم في تحســين أمن المعلومات، وتتفق مع دراســة Chang وWang (2011) التي توصلــت إلى أن العلاقة بين مــوارد تكنولوجيا المعلومات وأمن المعلومات إيجابية ودالة إحصائيا، وأيضا البنية التحتية لأمن المعلومات لها تأثير إيجابي دال إحصائيا في أمن المعلومات، وتتفق مع دراسة Azees et al. (2016) التي وجدت أن التدابير المضادة (التحقق من الهوية، ومكافح البرامج الضارة، والتوقيع الرقمي، وتقنيات التشفير، وكشف التسلل) تؤثر بشكل إيجابي في سرية وسلامة وتوافر المعلومات.

ولكن دراسة Schuessler (2009) تتفق وتختلف مع الدراسة الحالية؛ حيث أكدت أن التدابير الوقائية ترتبط بشــكل إيجابي بفاعليــة أمن نظم المعلومات، ولكن تدابير الكشــف لا ترتبــط بفاعلية أمن نظم المعلومــات، وأيضا ذكرت دراســة Ma، Johnston، وPearson (2008) أن أهــداف إدارة أمن المعلومات (الســرية) تؤثر في ممارســات إدارة أمن المعلومــات (التحكم بالوصول)، بينما الســلامة لها تأثير معتدل، والتوافر ليس له أي تأثير.

ويلاحظ أن نتيجة الدراســة الحالية تتفق إلى حد ما مع نتائج الدراســات السابقة ونظرية الردع العام؛ وقــد يرجع ذلك إلى اهتمام الشــركات بآليات التحقــق من الهوية، والتحكم بالوصــول، ومكافح البرامج الضــارة، وحماية الشــبكة، وأنظمة التشــفير؛ حيث إن جميع الشــركات في مختلف البيئــات والقطاعات تقتني وتستخدم الضوابط التقنية في حماية بياناتهم والحفاظ على سرية المعلومات وسلامتها وتوافرها، وحماية الموارد من الوصول غير المصرح به.

الفرضية الفرعية الثانية: أشارت النتائج في الجدول (11) إلى أن الضوابط الإدارية تؤثر بشكل إيجابي في أمن نظم المعلومات المحاســبية؛ حيث جاءت قيمة معامل المســار (β=0.340)، وقيمة (t=4.510) دالة إحصائيا عند مستوى دلالة أقل من (0.01)؛ وهذا يعني أنه كلما زادت الضوابط الإدارية بدرجة واحدة زاد أمن نظم المعلومات المحاســبية بنسبة (34 %)، وتدعم هذه النتيجة صحة الفرضية الفرعية الثانية للفرضية الرئيسية.

وتتفــق هذه النتيجة مع النموذج الموســع لنظرية الردع العام التي تفترض أن وعي المســتخدم بالتدابير المضادة له تأثير مباشــر وغير مباشــر في نوايا المســتخدمين المتعلقة بإســاءة اســتخدام نظــم المعلومات (D'Arcy et al., 2009)، وتتفق مع دراســة Schuessler (2009) التي أشــارت إلى أن تدابير المعالجة والــردع ترتبط بشــكل إيجــابي بفاعلية أمن نظــم المعلومات، وتتفــق مع دراســة Al-ghananeem (2014) الــتي وجدت أن سياســات الأمــن لها تأثير إيجابي في ضمــان أمن المعلومات، وتتفق مع دراســة Azees el al. (2016) التي أظهرت أن التدابير المضادة (سياسة أمن كلمة المرور) تؤثر بشكل إيجابي في ســرية وسلامة المعلومات، وتوصلت دراســة Chang وWang (2011) إلى أن العلاقة بين أمن المعلومات ومــوارد العلاقة إيجابية ودالة إحصائيا، وخلصت دراســة Chang وLin (2007) إلى أن هناك علاقة قوية بين الثقافة التنظيمية وإدارة أمن المعلومات (السرية والسلامة والتوافر).

http://doi.org/10.59222/ustjmhs.1.2.1

وتتفق وتختلف نتيجة الدراسة الحالية مع دراسة Kankanhalli et al. (2003) التي توصلت إلى أن جهود الردع (في شكل ساعات العمل المنفقة لأغراض أمن نظم المعلومات) ترتبط بشكل إيجابي بفاعلية أمن نظم المعلومات؛ أي أن جهود الردع الأكبر تسهم في تحسين فاعلية أمن نظم المعلومات، غير أن شدة الردع (في شكل عقوبات يتم فرضها على إساءة استخدام نظم المعلومات) لا تؤثر في فاعلية أمن نظم المعلومات، وأيضا تشير نتائج دراسة Ma et al. (2008) إلى أن السرية تؤثر في ممارسات إدارة أمن المعلومات (سياسة الأمن، وخطط الاستمرارية)، ولكن السلامة لها تأثير متوسط، والتوافر ليس لها أي تأثير.

ويدل هذا الاتفاق إلى حد ما مع نتيجة الدراسة الحالية على أن أولوية الضوابط الإدارية (التخطيط للطوارئ، وإجراءات التدقيق، وسياسة الأمن، والتوعية والتدريب، والتدابير القانونية) وأهميتها في مختلف البيئات والقطاعات جاءت عالية، ويساعد تطبيق الضوابط الإدارية الملائمة في التعافي من الكوارث واستعادة النظام في الموقع البديل وتخفيض الخسائر، وتقييم أمن النظام، وإجراء التحقيقات أثناء وبعد الهجوم، ورصد الهجمات بشكل مستمر، وتحسين وتعزيز أداء أمن النظام.

الاستنتاجات:

بناء على نتائج اختبار فرضيات الدراسة ومناقشتها في قطاع الاتصالات في اليمن فقد توصلت الدراسة الحالية إلى الاستنتاجات الآتية:

1) يؤدي استخدام الضوابط الأمنية الملائمة إلى رفع مستوى أمن نظم المعلومات المحاسبية، ويتضح أن قطاع الاتصالات في اليمن يستخدم الضوابط الأمنية (الضوابط التقنية، والضوابط الإدارية) في حماية سرية المعلومات وسلامتها وتوافرها.
2) يتضح أن مصدر التأثير الإيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات بالجمهورية اليمنية يعود إلى الضوابط التقنية، يليها الضوابط الإدارية.
3) يتبين أن مصدر التأثير الإيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات بالجمهورية اليمنية يعود إلى المؤشرات المرتبطة بالضوابط التقنية التي تشمل آليات التحقق من الهوية، والتحكم بالوصول، ومكافح البرامج الضارة، وحماية الشبكة، وأنظمة التشفير.
4) يتضح أن مصدر التأثير الإيجابي في أمن نظم المعلومات المحاسبية في قطاع الاتصالات بالجمهورية اليمنية يعود إلى المؤشرات المرتبطة بالضوابط الإدارية المتمثلة في التخطيط للطوارئ، وتدقيق الأمن، وسياسة أمن المعلومات، والتوعية والتدريب بأمن المعلومات، والتدابير القانونية.

التوصيات:

بناء على الاستنتاجات التي تم التوصل إليها توصي الدراسة الحالية بالآتي:

1) المزيد من الاهتمام بأمن نظم المعلومات المحاسبية؛ لأن سرية المعلومات وسلامتها وتوافرها قضية جوهرية في قطاع الاتصالات تؤثر في سمعة الشركة وتثير قلق العملاء المتعلقة بالخصوصية، وتؤثر في ثقتهم.
2) اهتمام أكثر بالضوابط الأمنية في قطاع الاتصالات، فيجب التركيز على كل من الضوابط التقنية، والضوابط الإدارية معا بدلا من التركيز على الضوابط التقنية فقط، ويجب أن تعملا معا لإيجاد بيئة آمنة، وتؤدي تلك الضوابط إلى تعزيز أمن نظم المعلومات المحاسبية.
3) التأكيد على أهمية تنفيذ الضوابط التقنية وتحديثها باستمرار، وتوظيف أحدث تقنيات الحماية (مواكبة التطورات المتسارعة في تكنولوجيا المعلومات)، وتشفير البيانات الحساسة، وتنفيذ المصادقة القوية متعددة العوامل، وإيلاء التحكم بالوصول قدرا كبيرا من الاهتمام، وتحديث مكافح البرامج الضارة باستمرار.

http://doi.org/10.59222/ustjmhs.1.2.1

4) التأكيد على أهمية تنفيذ الضوابط الإدارية وتحديثها باستمرار، وتحسين أنشطة الاستجابة للحوادث الأمنية، وتوظيف الخبراء والمختصين في مجال أمن المعلومات، وإنشاء إدارة أمن المعلومات، واعتماد موازنة أمنية كافية، ووضع ونشر السياسة الأمنية وتحديثها، وتفعيل برامج التوعية والتدريب المتعلقة بأمن المعلومات، والتخطيط للطوارئ، وتدقيق الأمن.

المقترحات:

1) بحثت الدراسة الحالية أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية، ويمكن إجراء مزيد من الأبحاث لاستكشاف العوامل الأخرى المؤثرة في أمن نظم المعلومات المحاسبية؛ لذلك نقترح دراسة أثر التوعية والتدريب في أمن نظم المعلومات المحاسبية، ودراسة أثر السياسة الأمنية في أمن نظم المعلومات المحاسبية، وإعادة تصنيف الضوابط الأمنية وفقا لتصنيف المعهد الوطني للمعايير والتكنولوجيا (NIST) ودراسة أثرها في أمن نظم المعلومات المحاسبية.
2) أجريت الدراسة الحالية في قطاع الاتصالات، وقد تكون النتائج غير قابلة للتعميم على القطاعات الأخرى؛ لذلك تقترح الدراسة الحالية توسيع نطاق البحث ليشمل أنواعا مختلفة من القطاعات، مثل: إجراء دراسات مماثلة في البنوك، والمستشفيات، والجامعات، والتأمين، والطيران.
3) تناولت الدراسة الحالية أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية، ولم تتناول الدراسة المتغيرات المعدلة والوسيطة؛ لذلك تقترح الدراسة الحالية اختبار برامج التوعية والتدريب، أو دعم الإدارة العليا كمتغيرات معدلة بين الضوابط الأمنية وأمن نظم المعلومات المحاسبية، واختبار السياسة الأمنية كمتغير وسيط بين الضوابط الأمنية وأمن نظم المعلومات المحاسبية.

الاسهام البحثي:

وضع محمد الربيدي ونبيل الحميري خطة الدراسة، وقاما ببناء الخلفية النظرية، وتحديد المنهجية، وقام نبيل الحميري بجمع البيانات، وتفسير النتائج ومناقشتها، وصياغة الاستنتاجات والتوصيات، وأخيرا، رُوجعت المسودة النهائية للدراسة من قبل محمد الربيدي.

المراجع:

جبور، منى الأشقر (2012)، *الأمن السيبراني: التحديات ومستلزمات المواجهة*، ورقة قدمت في اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، 27-28 أغسطس، بيروت، لبنان.

الجريدة الرسمية (2006)، *قانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية*، الجريدة الرسمية، العدد 24، الجمهورية اليمنية.

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*، 33، 1-45.

رئاسة الجمهورية (2012)، *قانون حق الحصول على المعلومات رقم (13) لسنة 2012م*، صنعاء، الجمهورية اليمنية.

سبأ نت (2014، يونيو 26)، *المؤتمر الأول لأمن المعلومات- صنعاء*، استرجع بتاريخ أكتوبر 12، 2019، من موقع المركز الوطني للمعلومات: https://yemen-nic.info/conferences/activ_details.php?ID=69967

عدن الغد (2014)، *خلل بشبكة (MTN) يوقف حركة الاتصالات بعدن*، استرجع بتاريخ يونيو 6، 2017، من https://adengad.net/public/posts/103375

فاضل، عبدالكريم محمد يحيى (2018)، *تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن: دراسة تطبيقية* (أطروحة دكتوراه)، جامعة دمشق، سوريا.

القحطاني، ذيب بن عايض (2015)، *أمن المعلومات*، الرياض، السعودية: مكتبة الملك فهد الوطنية.

http://doi.org/10.59222/ustjmhs.1.2.1

مركز دعم لتقنية المعلومات. (2015، مايو)، *الحماية القانونية للبيانات الشخصية*، استرجع من موقع المركز: https://sitcegypt.org/?p=4048

وزارة الاتصالات وتقنية المعلومات (2020، مارس)، *الاتصالات والبريد خمسة أعوام من الصمود*، صنعاء، الجمهورية اليمنية، استرجع بتاريخ مايو 26، 2023، من https://mtit.gov.ye/co_sub_media_image/28-Arabic_2020_R2.pdf

يحيى، عماد (2012)، *الهجمات الإلكترونية كأكبر المخاطر التي تهدد قطاع الأعمال*، استرجع بتاريخ نوفمبر 19، 2015، من https://www.tech-wd.com/wd/2012/09/08/kaspersky-global-it-security-risks-survey-report

Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. *Future Internet, 14*(1), 11. https://doi.org/10.3390/fi14010011

Abu-Musa, A. A. (2006a). Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations. *Journal of King Saud University - Computer and Information Sciences, 18*, 1-30. https://doi.org/10.1016/S1319-1578(06)80001-7

Abu-Musa, A. A. (2006b). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. *Journal of Information Systems, 20*(1), 187-203. https://doi.org/10.2308/jis.2006.20.1.187

Al-ghananeem, K. M. (2014). The impact of information security management standards to ensure information security. *International Journal of Economics and Research, 5*(1), 46-66.

Al-ghananeem, K. M., Al-taee, M. A., & Jida, B. K. (2014). The impact of the goals of information security standards to ensure information security. *Journal of Management Research, 6*(2), 74.-101. https://doi.org/10.5296/jmr.v6i2.5024

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security compliance in organizations: An institutional perspective. *Data and Information Management, 1*(2), 104-114. https://doi.org/10.1515/dim-2017-0006

American Institute of Certified Public Accountants. (2015). *25th anniversary edition of the North America Top Technology Initiatives Survey results*. Durham, North Carolina: AICPA.

Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems, 10*(6), 379-388. https://doi.org/10.1049/iet-its.2015.0072

Bafghi, A. A. S. T. (2014). Status and security of accounting information systems in Iranian organizations. *International Journal of Economy, Management and Social Sciences, 3*(12), 71-76.

http://doi.org/10.59222/ustjmhs.1.2.1

Bernews (2015, December 2). *EY Global Information Survey: Cyber attacks*. Retrieved February 08, 2018, from https://bernews.com/2015/12/dd-ey-global-information-security-survey/

Blumstein, A., Nagin, D., & Cohen, J. (Eds.). (1978). *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

Chang, K. C., & Wang, C. P. (2011). Information systems resources and information security. *Information Systems Frontiers, 13*(4), 579-593. https://doi.org/10.1007/s10796-010-9232-6

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. https://doi.org/10.1108/02635570710734316

Cherdantseva, Y., & Hilton, J. (2014). *Information security and information assurance: Discussion about the meaning, scope, and goals*. Pennsylvania: IGI Global. https://doi.org/10.4018/978-1-4666-4526-4.ch010

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

Choejey, P., Murray, D., & Fung, C. C. (2016). Exploring critical success factors for cybersecurity in Bhutan'S Government Organizations. In N. Meghanathan & D. C. Wyld (Eds.), *Computer Science & Information Technology (CS & IT)* (pp. 49-61). AIRCC Publishing Corporation. https://doi.org/10.5121/csit.2016.61505

Cisco. (2015). *Annual security report*. San Jose, CA: Cisco Systems, Inc.

Committee on National Security Systems. (2015). *Committee on National Security Systems (CNSS) glossary*. Ft Meade, Maryland: CNSS Secretariat (IE414), National Security Agency.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98. https://doi.org/10.1287/isre.1070.0160

Deloitte. (2006). *Protecting the digital assets: The 2006 Technology, Media & Telecommunications Security Survey*. London, United Kingdom: Deloitte Touche Tohmatsu Limited (DTTL).

Deloitte. (2013). *Blurring the lines: 2013 TMT Global Security Study*. London, United Kingdom: DTTL.

Deloitte. (2014). *Global cyber executive briefing*. London, United Kingdom: DTTL.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386-408. https://doi.org/10.17705/1jais.00133

Ernst & Young. (2012). *Fighting to close the gap: EY's 15th annual global information security survey (GISS)*. Bahamas, The Caribbean: EYGM Limited.

Ernst & Young. (2015). *Creating trust in the digital world: EY's 18th annual global information security survey (GISS)*. Bahamas, The Caribbean: EYGM Limited.

Government Accountability Office. (2015). *Information security: Cyber threats and data breaches illustrate need for stronger controls across federal agencies*. GAO-15-758T. Washington: GAO.

Government Accountability Office. (2016a). *Information security: FDIC implemented controls over financial systems, but further improvements are needed*. GAO-16-605. Washington: GAO.

Government Accountability Office. (2016b). *Information security: Agencies need to improve controls over selected high-impact systems*. GAO-16-501. Washington: GAO.

Haeussinger, F., & Kranz, J. (2013). *Information security awareness: Its antecedents and mediating effects on security compliant behavior*. Paper presented at the 34th International Conference on Security and Privacy of Information and IS, 15-18 December, Milan.

Hair, J. F., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Hoboken, NJ: Prentice Hall Higher Education.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling* (1st ed.). Thousand Oakes, CA: Sage.

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

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

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 Jordanian Banking Sector. *Journal of Accounting, Business & Management, 13*, 39-68.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based Structural Equation Modeling. *Journal of the Academy of Marketing Science, 43*, 115-135. https://doi.org/10.1007/s11747-014-0403-8

Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). *A theory on information security*. Proceedings of the 27th Australasian Conference on Information Systems (ACIS2016), 5-7 December, Faculty of Business, University of Wollongong, Wollongong, Australia.

Hulme, G. V. (2015, October 7). *Survey says enterprises are stepping up their security game*. Retrieved June 21, 2016, from https://www.csoonline.com/article/2988168/survey-says-enterprises-are-stepping-up-their-security-game.html

International Telecommunication Union & ABIresearch (2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Geneva: ITU. Retrieved May 29, 2015, from http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

International Telecommunication Union. (2017). *Global Cybersecurity Index (GCI) 2017*. Switzerland Geneva: ITU.

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

International Telecommunication Union. (2021). *Global Cybersecurity Index (GCI) 2021*. Switzerland Geneva: ITU.

ISO/IEC JTC 1. (2009). *Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000)* (1st ed.). Washington, D.C.: ISO/IEC JTC 1.

ISO/IEC JTC 1. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000)* (5th ed.). Washington, D.C.: ISO/IEC JTC 1.

Joint Task Force Transformation Initiative. (2010). *Guide for applying the risk management framework to federal information systems: A security life cycle approach*. Special publication No. 800-37 Rev. 1. Gaithersburg, Maryland: NIST.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments*. Special publication No. 800-30 Rev. 1. Gaithersburg, Maryland: NIST.

Joint Task Force Transformation Initiative. (2013). *Security and privacy controls for federal information systems and organizations*. Special publication No. 800-53 Rev. 4. Gaithersburg, Maryland: NIST.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154. https://doi.org/10.1016/S0268-4012(02)00105-6

Keung, Y. H. (2013). Information security controls. *Advances in Robotics & Automation, 3*(2), 1000e118. https://doi.org/10.4172/2168-9695.1000e118

Kim, H. B., Lee, D. S., & Ham, S. (2013). Impact of hotel information security on system reliability. *International Journal of Hospitality Management, 35*, 369-379. https://doi.org/10.1016/j.ijhm.2012.06.002

Kiseki, D. W., Havyarimana, V., Niyonsaba, T., Zabagunda, D. L., Wail, W. I., & Semong, T. (2023). The knowledge of cyber-security vulnerabilities in an Institution of Higher and University Education. A Case of ISP-Bukavu (Institut Supérieur Pédagogique de Bukavu) (TTC= Teachers' Training College). *Journal of Computer and Communications, 11*(4), 12-32. https://doi.org/10.4236/jcc.2023.114002

Kissel, R. (ed.). (2013). *Glossary of key information security terms*. NISTIR 7298 Rev. 2. Gaithersburg, Maryland: NIST.

Lemos, R. (2022, July 27). *Average data breach costs soar to $4.4M in 2022*. Retrieved May 25, 2023, from https://www.darkreading.com/risk/most-companies-pass-on-breach-costs-to-customers

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly, 16*(2), 173-186. https://doi.org/10.2307/249574

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270. https://doi.org/10.1108/09685220810893207

Mar-Elia, D. (2023, March 27). *Five most in demand identity threat detection & response capabilities*. Retrieved May 25, 2023, from https://technative.io/five-most-in-demand-identity-threat-detection-response-capabilities/

Martin, A., & Khazanchi, D. (2006). *Information availability and security policy*. Paper presented at the Proceedings of the 12th Americas Conference on Information Systems, 4-6 August, Acapulco, Mexico.

Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A conceptual framework for threat assessment based on organization's information security policy. *Journal of Information Security, 5*(4), 166-177. https://doi.org/10.4236/jis.2014.54016

McAfee Enterprise. (2015). *McAfee labs 2016 threats predictions report*. Retrieved May 5, 2017, from https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

Muhrtala, T. O., & Ogundeji, M. (2013). Computerized accounting information systems and perceived security threats in developing economies: The Nigerian case. *Universal Journal of Accounting and Finance, 1*(1), 9-18. https://doi.org/10.13189/ujaf.2013.010102

National Cyber Security Index. (2020). *148. Yemen 7.79*. Retrieved October 20, 2020, from https://ncsi.ega.ee/country/ye/467/#details

National Institute of Standards and Technology. (2006). *Minimum security requirements for federal information and information systems*. FIPS PUB 200. Gaithersburg, MD: NIST.

Office of Management and Budget. (2016). *Annual report to Congress: Federal Information Security Management ACT*. Washington, D. C.: Executive Office of the President of the United States, OMB.

Palmer, C. (2013, June 18). *Software itself is a process, not a product*. https://noncombatant.org/2013/06/18/software-itself-is-a-process-not-a-product/

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals*. NISTIR 7621 Rev. 1. Gaithersburg, Maryland: NIST.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646. https://doi.org/10.1016/j.cose.2004.10.006

PricewaterhouseCoopers & Infosecurity (2014). *Information security breaches survey: Technical report*. London: PwC.

PricewaterhouseCoopers (PwC) & Infosecurity (2015). *Information security breaches survey: Technical report*. London: PwC.

PricewaterhouseCoopers (PwC) (2015). *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015*. London: PwC.

Reuters. (2015). *Millions of computers may be compromised by US spyware: Report*. United Kingdom: Telegraph Media Group Limited.

Riad, N. I. (2009). *Security of accounting information systems: A cross-sector study of UK companies* (Doctoral dissertation). Cardiff University, Cardiff, Wales.

Richardson, R. (2010). *15th Annual 2010/2011 Computer Crime and Security Survey*. San Francisco, California: Computer Security Institute.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005). *Recommended security controls for federal information systems*. Special publication No. 800-53. Gaithersburg, Maryland: NIST.

Rot, A. (2009). *Enterprise information technology security: Risk management perspective*. In S. I. Ao, C. Douglas, W. S. Grundfest & J. Burgstone (Eds.), *Proceedings of the World Congress on Engineering and Computer Science 2009* (Vol. II, pp. 1171-1176). Newswood Limited.

Schuessler, J. H. (2009). *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses* (Doctoral dissertation). University of North Texas, Denton, Texas.

Schuessler, J. H. (2013). Contemporary threats countermeasuresi. *Journal of Information Privacy and Security, 9*(2), 3-20. https://doi.org/10.1080/15536548.2013.10845676

Seno, S. A. H., Bidmeshk, O. G., & Ghaffari, K. (2015). *Information security diagnosis in electronic banking (Case study: Tejarat Bank's Branches of Isfahan)*. Paper presented at the 9th International Conference on e-Commerce in Developing Countries: With focus on e-Business, 16 April, Isfahan, Iran.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Risk management guide for information technology systems*. Special publication No. 800-30. Gaithersburg, Maryland: NIST.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276. https://doi.org/10.1287/isre.1.3.255

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469. https://doi.org/10.2307/249551

Symantec Corporation. (2017). *Internet security threat report* (Vol. 22). Mountain View, CA: Symantec Corporation.

Tarmidi, M., Rashid, A. A., Deris, M. S. B., & Roni, R. A. (2013). Computerized accounting system threats in Malaysian public services. *International Journal of Finance and Accounting, 2*(2), 109-113. https://doi.org/10.5923/j.ijfa.20130202.10

TheoriZeit. (2016, January 9). *General deterrence theory*. Retrieved August 6, 2016, from https://is.theorizeit.org/wiki/General_deterrence_theory#cite_ref-1

Tsegaye, T., & Flowerday, S. (2014). *Controls for protecting critical information infrastructure from cyberattacks*. Paper presented at the World Congress on Internet Security, WorldCIS, 8-10 December, London, United Kingdom.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57. https://doi.org/10.1016/j.ijinfomgt.2003.12.003

Woodhouse, S. (2008). *Critical success factors for an information security management system*. Paper presented at the 5th International Conference on Information Technology and Applications. 7-8 April, Las Vegas, Nevada.

Workman, M., Bommer, W. H., & Straub, D. (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. https://doi.org/10.1016/j.chb.2008.04.005

Arabic References in Roman Scripts:

Adn Alghad (2014). *Khalal bishabaka (MTN) yuqif harakat aliatisalat bi Adan*. Astarjie bitarikh Yunyu 6, 2017, min https://adengad.net/public/posts/103375

Aljaridat Alrasmia (2006). *Qanun raqm (40) lisanat 2006 bishan 'anzimat aldafe waleamaliaat almaliat wa almasrafiat al'iiliktruniat*. Aljaridat Alrasmiat, Aladad 24, Aljumhuriat Alyamaniati.

Alqahtani, Dhib bin Ayid (2015). Amn almaelumati. Alrayad, Alsueudiati: Maktabat Almalik Fahd Alwataniati.

Alrabidi, Muhamad Ali (2010). Himayat almaelumat almuhasabiat fi zili makhatir altiknulujia lileamaliaat almasrifiat al'iiliktruniati: Dirasat maydania fi albunuk aleamilat fi Alyaman. *Majalat Kuliyat Altijarat Walaiqtisadi, 33*, 1-45.

Fadil, Abdulkarim Muhamad Yahya (2018). *Taqyim makhatir 'amn nuzum almaelumat almuhasabiat almuhawsabat ladaa albunuk altijariat fi Alyaman: Dirasat tatbiqia* (Utaruhat dukturah). Jamieat Dimashqa, Suria.

Jabuwr, Munaa Al'ashqar (2012). *Al'amn alsiybirani: Altahadiyat wamustalzamat almuajahat*. Waraqatan qudimat fi Alliqa' Alsanawii Al'awal Lilmukhtasiyn fi Amn wa Salamat Alfada' Alsiybiranii, 27-28 Aghustus, Bayrut, Lubnan.

Markaz Daem Litiqniat Almaelumati (2015, Mayu). *Alhimayat alqanuniat lilbayanat alshakhsiati*. Aistarjie min mawqie almarkazi: https://sitcegypt.org/?p=4048

Riasat Aljumhuria (2012). *Qanun haqi alhusul ealaa almaelumat raqm (13) lisanat 2012*. Sana'a, Aljumhuriat Alyamaniati.

Saba Net (2014, Yuniu 26). *Almutamar Al'awal Li'amn Almaelumati – Sana'a*. Asturjie bitarikh 12 Uktubar, 2019, min Mawqie Almarkaz Alwatanii Lilmaelumati: https://yemen-nic.info/conferences/activ_details.php?ID=69967

Wizarat Alaitisalat wa Tiqniat Almaelumat (2020, Maris). *Alaitisalat walbarid khamsat Aewam min alsumud*. Sana'a, Aljumhuriat Alyamaniat, Aisturjie bitarikh 26 Mayu, 2023, min https://mtit.gov.ye/co_sub_media_image/28-Arabic_2020_R2.pdf

Yahya, Emad (2012). *Alhajamat al'iiliktiruniat ka'akbar almakhatir alati tuhadid qitae al'aemal*. Astarjie bitarikh Nufimbir 19, 2015, min https://www.tech-wd.com/wd/2012/09/08/kaspersky-global-it-security-risks-survey-report

http://doi.org/10.59222/ustjmhs.1.2.1