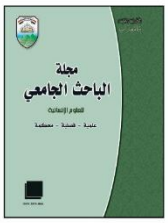
جامعة إب
مجلة الباحث الجامعي
ISSN: 2079-5068 ISSN (online): 2663-3930



أثر الإجراءات الرقابية للتكنولوجيا في أمن نظم المعلومات المحاسبية
دراسة ميدانية في البنوك العاملة في الجمهورية اليمنية

معين حسين علي السياني*، محمد حمود السمحي
قسم المحاسبة، كلية العلوم الإدارية، جامعة إب، اليمن
***Email:** mueenalsayani@gmail.com

الكلمات المفتاحية:
أمن نظم المعلومات المحاسبية، الإجراءات الرقابية للتكنولوجيا، البنوك العاملة في الجمهورية اليمنية.

الملخص:

هدفت الدراسة إلى معرفة أثر الإجراءات الرقابية المتعلقة بالتكنولوجيا في أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية، ويتمثل مجتمع الدراسة في البنوك العاملة في الجمهورية اليمنية معتمدة على منهج وصفي تحليلي كونه مناسبًا لطبيعة الدراسة بشقيها النظري والميداني، وتم استخدام الاستبانة أداة لجمع البيانات من127 مشاركا، وقد تمت استعادة (88) استبانة، وتم تحليل البيانات باستخدام برنامج التحليل الاحصائي (SPSS) باستخدام معامل ارتباط وانحدار بيرسون واختبار تي للعينة الواحدة، وتوصلت الدراسة إلى وجود أثر إيجابي للضوابط الأمنية المتعلقة في أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية، وقد أوصت الدراسة بأنهُ يجب على البنوك العاملة في الجمهورية اليمنية أن تبذل مزيدًا من الاهتمام والتعزيز في الإجراءات الرقابية لما لها من أثر في أمن نظم المعلومات المحاسبية.

أثر الإجراءات الرقابية للتكنولوجيا في أمن نظم المعلومات المحاسبية دراسة ميدانية في البنوك العاملة في الجمهورية اليمنية

The Impact of Technological Control Procedures on the Security of Accounting Information Systems: A Field Study in Banks Operating in the Republic of Yemen

Mueen Husein Ali Al-Saiani*, Mohammed H. Al-Samhi
Department of Accounting, Faculty of Administrative Sciences, Ibb University, Yemen
***Email: mueenalsayani@gmail.com**

Keywords:

Accounting Information Systems Security, Technological Control Procedures, Banks Operating In The Republic Of Yemen

Abstract:

This study aimed to investigate the impact of technological control procedures on the security of accounting information systems in banks operating in the Republic of Yemen. The study population consisted of these banks, employing a descriptive analytical approach suitable for both the theoretical and field aspects of the research. A questionnaire was used to collect data from (127) participants, with (88) responses returned. Data analysis was conducted using the statistical analysis program (SPSS), employing Pearson correlation and regression coefficients, as well as a one-sample (T-test). The findings revealed a positive impact of security controls related to the security of accounting information systems in the banks. The study recommended that banks operating in the Republic of Yemen should place greater emphasis on enhancing control procedures due to their significant effect on the security of accounting information systems.

المقدمة:

تواجه منظمات الأعمال جملة من المخاطر التي تهدد سرية وسلامة وتوافر المعلومات، بما في ذلك الهجمات الإلكترونية والمادية، والبرامج الخبيثة، وإخفاق الأجهزة، وأخطاء البرامج، والكوارث الطبيعية وغير الطبيعية (Joint Task Force Transformation Initiative, 2012)؛ إذ يمكن أن تؤدي هذه الهجمات إلى فقدان السرية أو السلامة أو التوافر (Donaldson, Siegel, Williams, & Aslam, 2015)، وهو ما أكدته بعض الدراسات التي أشارت إلى أن قيمة الجريمة الإلكترونية تُقدر بحوالي 105 مليار دولار سنويًا، متجاوزة تجارة المخدرات عالميًا (عبد الله، والناصر، 2019).

وفي بيئة الأعمال اليمنية تشهد تطورات سريعة نتيجة لضغوطات البيئة الخارجية؛ وذلك يخلق مخاطر تهدد أمن نظم المعلومات في البنوك. تستغل هذه المخاطر الثغرات الأمنية في النظام أو إجراءات أمن النظام، وهو ما يجعلها عرضة للهجمات؛ فوفقًا لتقرير الرقم القياسي العالمي للأمن السيبراني، كانت اليمن تحتل مرتبة متدنية في الأمن السبراني في الأعوام 2015 و2017 و2018 و2020 (ITU, 2015; ITU, 2017; ITU, 2018; ITU, 2020).

ولمواجهة هذه التهديدات، تعتمد البنوك على وسائل متعددة لحماية معلوماتها، تتضمن هذه الوسائل وضع أنظمة حماية للمعلومات والنظام، وحماية النظم الإلكترونية بطرق ملائمة، ومتابعتها بصورة مستقلة، ووضع ترتيبات لاسترجاع المعلومات في الحالات الطارئة، فضلًا عن توفير الحماية المادية لأجهزة الحاسوب والبرامج والبيانات (حجر، 2014؛ الشرعبي، 2014؛ الربيدي، 2012).

كما تستدعي هذه الظروف تفعيل الرقابة على تقنية المعلومات لضمان أمن النظام وتلبية متطلبات حماية المعلومات من الاستخدام غير المصرح به أو التسريب أو التعديل أو التضرر أو الضياع. ويمكن تحقيق ذلك من خلال ضوابط منطقية تضمن الوصول إلى النظم والبيانات والبرامج من قبل المستخدمين المصرح لهم فقط (Sheikhpour and Modiri, 2012). بناءً على ذلك، تهدف هذه الدراسة إلى فحص أثر الإجراءات الرقابية الخاصة بالتكنولوجيا على أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية.

مشكلة الدراسة:

تشهد بيئة الأعمال اليمنية تطورات متسارعة نتيجة لضغوطات متغيرات البيئة الخارجية، والتي كان لها انعكاسات تتمثل في المخاطر التي تهدد أمن نظم المعلومات في الشركات. والمخاطر المهددة لأمن نظم المعلومات تستغل الثغرات الأمنية في النظام، أو الشبكة، أو إجراءات أمن النظام، أو تنفيذ الإجراءات التي تُستغل من قبل المهاجمين؛ فقد جاء في تقرير الرقم القياسي العالمي للأمن السيبراني مجموعة من المؤشرات المستخدمة في قياس القدرات

الوطنية في مجال الأمن في عام 2015؛ كان ترتيب اليمن (27) ورقمها القياسي (0.059)، وهي درجة متدنية جدًا (International Telecommunication Union (ITU) 2015:5)، وفي عام 2017 جاءت اليمن في الترتيب قبل الأخير (164) ورقمها القياسي (0.007) (ITU,2017:54))، وفي عام 2018 وصل ترتيب اليمن عالميا إلى(172) من أصل (175) ورقمها القياسي (0.019) .(ITU,2018:68)، فضلًا عن الدرجة المتدنية التي نالتها اليمن في ضوء مقاييس أكاديمية الحوكمة الإلكترونية في مجال الأمن الإلكتروني؛ إذ كان ترتيبها (148) من أصل (161)، وكان مؤشر الأمن السيبراني (7.79) .(ITU,2020)

وفي ضوء ما سبق تتبلور مشكلة الدراسة بالسؤال الرئيس:

ما أثر الإجراءات الرقابية المتعلقة بالتكنولوجيا في أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية؟

أهمية الدراسة:

تتمثل أهمية الدراسة الحالية في الآتي:

أولا: الأهمية العلمية:

1- تناولت الدراسة الحالية أمن نظم المعلومات المحاسبية في البنوك اليمنية نتيجة لاستخدام نظم المعلومات على نطاق واسع في التواصل وتخزين كميات كبيرة من البيانات الحساسة. وتعد سرية المعلومات وسلامتها وتوافرها في القطاع المصرفي قضية جوهرية بما في ذلك خصوصية العملاء وسمعة البنك.

2- تُبين الدراسة الحالية الإجراءات الرقابية في البنوك مجتمع الدراسة؛ لأن هذه البنوك عرضة للهجمات الإلكترونية التي تستهدف المعلومات السرية، وسلامة المعلومات والأنظمة، وتوافر المعلومات والخدمات، وبيانات العملاء الشخصية.

3- تعزز الدراسة فهمنا لكيفية تعزيز الأمن والثقة في النظم المحاسبية الإلكترونية من خلال تطبيق الإجراءات الرقابية المتعلقة بتكنولوجيا المعلومات.

ثانيًا: الأهمية العملية:

1. أنها تقدم مجموعة من الإجراءات الرقابية لأمن نظم المعلومات المحاسبية، على أمل أن تصبح البنوك اليمنية قادرة على مواكبة التطورات والمتغيرات التكنولوجية المتسارعة في ظل بيئة ديناميكية متغيرة.
2. تُساعد دراسة أمن نظم المعلومات المحاسبية في البنوك اليمنية مجتمع الدراسة في تحديد مستوى الأمن، وكشف الحوادث الأمنية وخفضها، وتحديد المخاطر وترتيب أولوياتها، وتأمين المعلومات الحساسة.
3. تسهم الدراسة الحالية إسهامًا عمليًا في تلافي جوانب الضعف والقصور أو الثغرات الأمنية في الأنظمة والبرامج والشبكات والإجراءات الرقابية، وبما يعزز أمن نظم المعلومات المحاسبية في البنوك اليمنية مجتمع الدراسة.

4. تسهم الدراسة الحالية في تحديد الضوابط والإجراءات الرقابية المتعلقة بتكنولوجيا المعلومات اللازمة لأمن نظم المعلومات المحاسبية الإلكترونية في البنوك العاملة في الجمهورية اليمنية مجتمع الدراسة، ودرجة كل إجراء، وأثره في أمن المعلومات.

5. الإسهام برفد المكتبة اليمنية في موضوع الدراسة وكذلك المهتمين، فضلًا عن أنها تُشكل إضافة للمكتبة العربية في مجال أمن المعلومات.

هدف الدراسة:

تهدف الدراسة إلى معرفة أثر الإجراءات الرقابية المتعلقة بالتكنولوجيا في أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية.

الدراسات السابقة:

ناقشت دراسة (الربيدي؛ والحميري، 2023) أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية باتباع منهج تحليلي يعتمد على نمذجة المعادلة البنائية (SEM)، وتوصلت الدراسة إلى 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.

بينما دراسة (الحميري، 2021) تناولت الضوابط الأمنية بوصفها متغيرًا وسيطا بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية في شركات الاتصالات العامة في اليمن؛ وتوصلت الدراسة إلى أن مخاطر تكنولوجيا المعلومات لها تأثير سلبي مباشر في أمن نظم المعلومات المحاسبية في شركات الاتصالات العامة في اليمن، وأن مخاطر تكنولوجيا المعلومات تؤثر سلبا في الضوابط الأمنية، وأن الضوابط الأمنية لها تأثير إيجابي في أمن نظُم المعلومات المحاسبية؛ وأن مستوى أمن نظم المعلومات المحاسبية مرتفع، ودرجة مخاطر تكنولوجيا المعلومات متوسطة، ومستوى استخدام الضوابط الأمنية مرتفع.

وجاءت دراسة (الربيدي؛ والحميري، 2021) لقياس أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات بالاعتماد على نمذجة المعادلة البنائية (SEM) بمنهج تحليلي، ويتمثل مجتمع الدراسة في شركات الاتصالات العاملة في اليمن البالغ عددها 7 شركات؛ وتوصلت الدراسة إلى أن مخاطر تكنولوجيا المعلومات تؤثر سلبا في أمن نظم المعلومات وأوصت بضرورة تعزيز أمن نظم المعلومات للحفاظ على سرية المعلومات وسلامتها وتوافرها من المخاطر، ومواكبة أمن المعلومات للتطورات المتسارعة في تكنولوجيا المعلومات والاتصالات.

وتناولت دراسة (شحادة؛ وبدر، 2020): تقييم واقع أمن وسرية المعلومات الإلكترونية في بنك فلسطين "دراسة حالة" من خلال التعرف إلى مدى توافر مقومات حماية البنية التحتية لأمن المعلومات. وقد توصلت الدراسة إلى أنه يتوافر

لدى بنك فلسطين مقومات بنية تحتية مقبولة بمحاورها الثلاثة (المادية، البرمجية، والأفراد).

اما دراسة (Shamsi S. Bawaneh:2018) فقد تناولت ثلاثة أنواع من إجراءات أمن المعلومات والرقابة للشركات خاصة البنوك التي يتوقع استخدامها ضمن نظم المعلومات المحاسبية (AIS)، وهي: الأمن والرقابة العامة للبنوك؛ والأمن والرقابة العامة لتكنولوجيا المعلومات (IT)؛ وضوابط التطبيق لمعالجة المعاملات. وخلصت إلى جملة نتائج أهمها: أن البنوك لا تكون قادرة على حماية نفسها ضد الاحتيال على الكمبيوتر، إلا بصياغة إجراءات الرقابة تتمثل في الرقابة على المدخلات، والرقابة على عمليات المعالجة، والرقابة على المخرجات، والرقابة على المكونات المادية.

أما دراسة (الحكيم، وسليم، 2010) فقد هدفت إلى معرفة مدى إمكانية القيام بتقييم بنية الرقابة الداخلية المؤتمتة من قبل مفتشي الجهاز عند قيامهم بعملية تدقيق المؤسسات الاقتصادية التي تستخدم نظم المعلومات المحاسبية الإلكترونية وفقًا لمعايير الرقابة على نظم المعلومات، وخلصت الدراسة إلى جملة نتائج أهمها:

-لا توجد فروقات ذات دلالة إحصائية تعبر عن زيادة الفعالية الرقابية على تقنية المعلومات وذلك مع زيادة استخدام الضوابط الرقابية المتعلقة وفقًا للمعايير الرقابية المتعارف عليها.

ما يميز الدراسة الحالية عن الدراسات السابقة:

تبين من استعراض الدراسات السابقة الآتي:

1- اختلاف في (عينة الدراسة، تاريخ الدراسة وإقليم الدراسة).

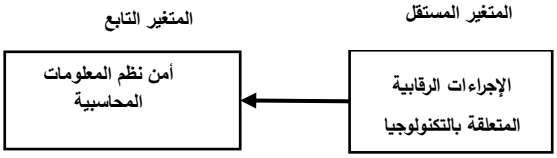
2- اتفقت الدراسة مع دراسة (الربيدي؛ والحميري،2021، 2023)، (الحميري، 2021) في المتغير التابع (أمن نظم المعلومات المحاسبية)، واختلفت في المتغير المستقل.

3- اختلفت الدراسات السابقة في المتغيرات التابعة؛ فمنها ما ترتبط بكفاءة أنظمة الرقابة الداخلية، أو على موثوقية التقارير المالية، ومنها ما ترتبط بجودة التقارير المالية، أو زيادة موثوقية المعلومات المحاسبية.

4- لا توجد دراسة واحدة تناولت المتغير المستقل وأثره في أمن نظم المعلومات (السرية، السلامة، التوافر)؛ وإنما تناولتها بشكل جزئي، وهذا ما يميز الدراسة الحالية عن الدراسات السابقة.

نموذج الدراسة

تمثل الدراسات السابقة أساسًا تم الاستناد إليه في صياغة مشكلة الدراسة، فضلًا عن الاعتماد عليها في تحديد أبعاد ومتغيرات الدراسة والمحددة بالمتغيرات المستقلة للإجراءات الرقابية المتعلقة بالتكنولوجيا، أما المتغير التابع فيتمثل في أمن نظم المعلومات المحاسبية الإلكترونية، كما هو موضح في أنموذج الدراسة الآتي:



الشكل (1): متغيرات الدراسة

تقوم الدراسة على فرضية اساسية هي:

" لا يوجد أثر ذو دلالة إحصائية للإجراءات الرقابية المتعلقة بالتكنولوجيا على أمن نظم المعلومات المحاسبية الإلكترونية في البنوك العاملة في الجمهورية اليمنية".

التعريفات الإجرائية:

1. أمن نظم المعلومات المحاسبية: هو مجموعة من الإجراءات والسياسات اللازمة لحماية أمن نظم المعلومات المحاسبية الإلكترونية من مخاطر انتهاك السرية، وضمان سلامتها، وتوافرها في أثناء المعالجة أو التخزين أو النقل.

2. الإجراءات الرقابية المتعلقة بالتكنولوجيا: هي مجموعة من الإجراءات التي تهدف إلى حماية الأجهزة والأنظمة (أنظمة التشغيل، والأجهزة الصلبة، والشبكات، والوسائط المختلفة، وقواعد البيانات) من مجموعة واسعة من المخاطر لضمان سرية المعلومات، وسلامتها، وتوافرها في أثناء المعالجة أو التخزين أو النقل.

الإطار النظري

أمن نظم المعلومات:

يمثل أمن نظم المعلومات العمليات والتدابير والتوجيهات التي تصدرها إدارة الشركة بهدف حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغرض تحقيق سلامتها وتوافرها وسريتها وفقًا للصلاحيات والترتيبات المتعارف عليها (الدنف، 44:2013).

عرف أمن نظم المعلومة (Joint Task Force Transformation)بأنه: حماية المعلومات وأنظمة المعلومات من الوصول غير المصرح به أو الاستخدام أو الإفشاء أو التعطيل أو التعديل أو التدمير من أجل توفير السرية والنزاهة والتوافر (Joint Task Force Transformation Initiative,2012:6). بينما عرفة (جبوري، 76:2011) بأنه: القدرة على التفاعل وحماية المعلومات وقواعد البيانات من العبث والتدمير والكشف عن أي مخاطر تتعرض لها ومحاولة معالجتها، ويعد من السياسات الأمنية التي لابد للمنظمة من أن تتبناها من خلال اتباع أفضل الممارسات الأمنية وأحدث التقنيات للحفاظ عليها من الاختراق غير المباشر من قبل غير المخولين ومهاجمة البيانات والمعلومات المخزنة في الحاسوب للضرر بالشركة.

أمن نظم المعلومات المحاسبية:

هو التحكم في عملية الوصول للنظام وبياناته (ستينبارت، ورومني، 342:2009)، وعرفه الشمالي (190:2017) بأنه: مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات. ويقصد بأمن نظم المعلومات

المحاسبية: حماية أنظمة المعلومات المحاسبية من مجموعة واسعة من المخاطر لضمان سرية المعلومات، وسلامتها، وتوافرها في أثناء المعالجة أو التخزين أو النقل (الحميري، 23:2021).

ويفرق بعض الباحثين بين أمن المعلومات وأمن نظم المعلومات في أن الأول هو حماية للمعلومات دون ذكر لنظام المعلومات بما يشمله من تقنيات واستراتيجيات، والآخر هو حماية للموارد التقنية وما تحتويه من معلومات. ولكن لا يمكن حماية هذه المعلومات دون توفير حماية للأنظمة؛ فالمعلومات هي موجودة داخل الأنظمة (الدنف، 2013 :45). وأن من يتمعن في تعريفات أمن المعلومات وتعريفات أمن نظم المعلومات يجد أن لهما تعريفًا واحدًا بالضبط؛ فحماية المعلومات لا يمكن أن تتحقق دون توفير حماية لنظم المعلومات؛ وعليه يمكن النظر إلى أمن المعلومات وأمن نظم المعلومات بوصفهما مصطلحين لمفهوم واحد (فيلالي، 2019 :61).

تكنولوجيا المعلومات:

عرفها المعهد الأمريكي لتكنولوجيا المعلومات بأنها: "دراسة، وتصميم، وتطوير، وتطبيق، ودعم أو إدارة نظم المعلومات المعتمدة على الحاسوب، خصوصًا التطبيقات البرمجية والأجهزة التي تتعامل من خلالها تكنولوجيا المعلومات مع تقنيات الحاسوب والبرامج الحاسوبية لتحويل وتخزين ومعالجة ونقل واسترجاع المعلومات بشكل آمن" (نصور، 2014: 16)

تتضمن التكنولوجيا الأجهزة والأنظمة؛ مثل أنظمة التشغيل والأجهزة الصلبة والشبكات والوسائط المختلفة وقواعد البيانات (نصور، 2015: 78)؛ إذ يُعد الحاسوب والأجهزة الملحقة به الأساس المادي لبنية تكنولوجيا المعلومات، ويمكن تفصيل هذه المكونات على النحو الآتي (عي؛ بولفراخ،2020 :21):

1- وسائل الإدخال: تتضمن لوحة المفاتيح، الفأرة، الكاميرات...؛

2- وحدة المعالجة المركزية: تعالج البيانات وتسيطر على نظام الحاسوب؛

3- وسائل الخزن: الأقراص، الأشرطة الممغنطة...؛

4- وسائل الإخراج: الطابعات، الشاشات، وسائل الإخراج الصوتي...؛

5- وسائل الاتصال: تستخدم لربط الحواسيب ببعضها.

قياس أمن نظم المعلومات المحاسبية:

يتم قياس أمن نظم المعلومات من خلال الأبعاد الثلاثة: السرية، والسلامة، والتوافر التي تضمنها التعريف، وتوضيحها في الآتي (الربيدي، والحميري، 129:2021):

سرية المعلومات: هي حماية المعلومات الحساسة من الكشف، وتقييد عمليات الوصول المصرح به، ومنع الوصول غير المصرح به (الحميري، 2021: 32)؛ وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها أشخاص غير مخولين بذلك (صالح، وعبدالله، 2016:

214)؛ بمعنى حماية المعلومات الحسّاسة من الإفصاح غير المرخّص. (نصور، 17:2015)،

سلامة المعلومات: يقصد بها: اتخاذ التدابير اللازمة لحماية المعلومات من التغيير والتعديل المقصود وغير المقصود (عقيل، 2011 :25)، ويهتم هذا العنصر بدقة المعلومات والأنظمة وسلامتها من التلاعب أو التعديل غير المصرح به، كما يهتم بكشف تعديل المعلومات (القحطاني، 94:2015)؛ وهذا أمر لازم لضمان أن تبقى المعلومات صحيحة ودقيقة (الاتحاد الدولي للاتصالات، 22:2007).

توافر المعلومات: يقصد بها أن تكون قابلة للوصول إليها واستخدامها حين الطلب من قبل أي شخص أو أي جهة معروفة ومحددة وفي أي وقت (مصرح به) (القحطاني، 2015 :96)، (طارش، 51:2015).

الإجراءات الرقابية لتكنولوجيا المعلومات:

عرَّفها المعهد الوطني للمعايير والتكنولوجيا (JTFTI, 2013:1) بأنها الضمانات/ الإجراءات المضادة المنصوص عليها لأنظمة المعلومات أو المنظمات المصممة من أجل: (1) حماية سرية وسلامة وتوافر المعلومات التي تتم معالجتها وتخزينها ونقلها عبر تلك الأنظمة؛ (2) تلبية مجموعة من متطلبات الأمن المحددة.

وعرفها الحميري (79:2021) بأنها "تلك الإجراءات التقنية والإدارية اللازمة لحماية سرية المعلومات والأنظمة وسلامتها وتوافراها من المخاطر المختلفة أثناء المعالجة أو التخزين أو النقل".

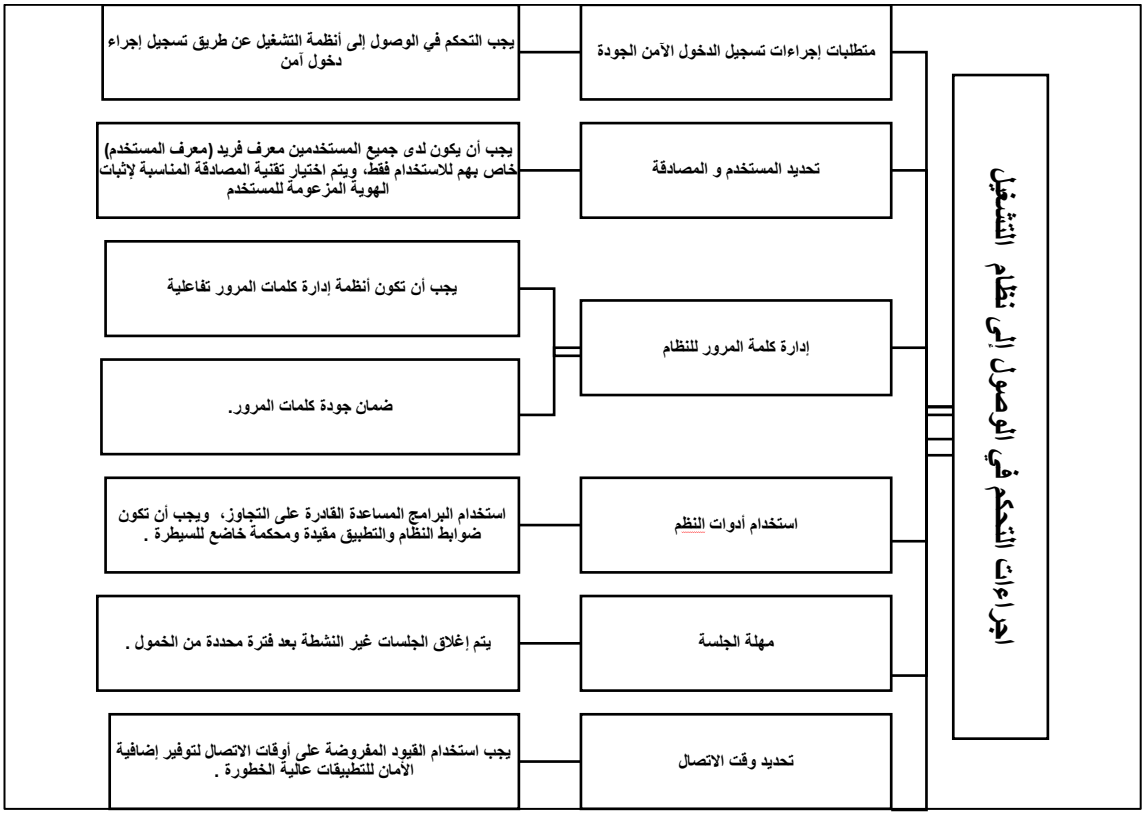
ولأغراض الدراسة الحالية فإنه يمكن تعريف الإجراءات الرقابية بأنها الإجراءات الرقابية على التكنولوجيا اللازمة لحماية الأنظمة وسرية المعلومات وسلامتها وتوافراها من المخاطر المختلفة التي تهدد أمن نظم المعلومات في أثناء المعالجة أو التخزين أو النقل.

الإجراءات الرقابية المتعلقة بالتكنولوجيا:

تتضمن التكنولوجيا الأجهزة والأنظمة مثل أنظمة التشغيل، والأجهزة الصلبة، والشبكات والوسائط المختلفة، وقواعد البيانات (نصور، 78:2015)، وتتضح الإجراءات الرقابة الخاصة بالتكنولوجيا على النحو الآتي:

1) التحكم في الوصول إلى نظام التشغيل:

الهدف من التحكم في الوصول إلى نظام التشغيل هو منع الوصول غير المصرح به إلى أنظمة التشغيل (ISO/IEC27001,2005:23)، ويوضح الشكل (2) إجراءات الرقابة في التحكم في الوصول إلى نظام التشغيل.



الشكل (2): إجراءات التحكم في الوصول إلى نظام التشغيل

المصدر: (إعداد الباحثين،2023) بتصرف من (ISO/IEC 27001,2005:23)

إدارة أمن تكنولوجيا المعلومات:

ينبغي توجيه وإدارة أمن المعلومات من أعلى سلطة في الشركة؛ للتأكد من تحقيقها لمتطلبات أعمال الشركة الأمنية (عقيل، 109:2011). ويجب أن يدار أمن تكنولوجيا المعلومات؛ بحيث تتماشى التدابير الأمنية مع متطلبات العمل، ويتضمن هذا الآتي: (IT Governance,2000:101)

1) ترجمة معلومات تقييم المخاطر إلى خطط أمن تكنولوجيا المعلومات.

أ- تنفيذ خطة أمن تكنولوجيا المعلومات.

ب- تحديث خطة أمن تكنولوجيا المعلومات لتنعكس التغييرات في تكوين تكنولوجيا المعلومات.

ج- تقييم تأثير طلبات التغيير على تكنولوجيا المعلومات الأمان.

د- مراقبة تنفيذ خطة أمنية تكنولوجيا المعلومات.

هـ- مواءمة إجراءات أمن تكنولوجيا المعلومات مع السياسات والإجراءات الأخرى.

2) المراقبة الأمنية:

يجب أن تضمن إدارة أمن تكنولوجيا المعلومات تسجيل النشاط الأمني، وأن يتم الإبلاغ عن أي مؤشر على انتهاك أمني وشيك على الفور إلى جميع الأشخاص المعنيين (داخليًا وخارجيًا)، والتصرف بناءً على ذلك في الوقت المناسب. (IT Governance,2000:101).

3) التعامل مع الحوادث:

يجب أن يكون للإدارة قدرة على التعامل مع حوادث أمن الكمبيوتر لمعالجة الحوادث الأمنية من خلال توفير منصة مركزية مزودة بالخبرة الكافية ومجهزة بمرافق اتصال سريعة وآمنة، وينبغي وضع مسؤوليات وإجراءات إدارة الحوادث لضمان استجابة مناسبة وفعالة وفي الوقت المناسب للحوادث الأمنية (معهد حوكمة تكنولوجيا المعلومات، جمعية تدقيق ومراقبة نظم المعلومات، 2004)، وتتمثل إجراءات الرقابة في الآتي: (IT Governance Institute,2004:100)

أ- تتم مراجعة الحوادث الأمنية المبلغ عنها (الخروقات) على الفور من قبل فريق مركزي يتمتع بالخبرة الكافية لتقليل الضرر وإيجاد/إزالة السبب الجذري لخرق الأمان.

ب- إبلاغ الإدارة بجميع الانتهاكات الأمنية الجسيمة.

ج- الإبلاغ عن عملية تأديبية رسمية بشكل مناسب للموظفين الذين تبين أنهم انتهكوا سياسات وإجراءات الأمن المؤسسي؛ ويتم إبلاغ الموظفين والمقاولين بهذه العملية.

4) ثقة الطرف المقابل:

يجب أن تضمن السياسة التنظيمية تنفيذ ممارسات الرقابة للتحقق من صحة الطرف المقابل الذي يقدم التعليمات أو المعاملات الإلكترونية، ويمكن تنفيذ ذلك من خلال التبادل الموثوق به لكلمات المرور، أو الرموز المميزة أو مفاتيح التشفير (IT Governance ,2000,p102).

5) ترخيص العمليات:

يجب أن تضمن السياسة التنظيمية، عند الاقتضاء، تنفيذ الإجراءات لتوفير أصالة المعاملات وإثبات صحة هوية المستخدم المطالب بها للنظام، ويتطلب ذلك استخدام تقنيات التشفير لتوقيع المعاملات والتحقق منها (IT Governance,2000:102).

6) عدم رفض العمليات:

يجب أن تضمن السياسة التنظيمية، عند الاقتضاء، أنه لا يمكن رفض المعاملات من قبل أي من الطرفين، ويتم تنفيذ الإجراءات لتوفير عدم إنكار المنشى أو الاستلام، وإثبات التقديم واستلام المعاملات، ويمكن تنفيذ ذلك من خلال التوقيعات الرقمية، والختم الزمني والأطراف الثلاثة الموثوقة، مع السياسات المناسبة التي تأخذ في الاعتبار المتطلبات التنظيمية ذات الصلة (IT Governance,2000:103)

7) تبادل البيانات الحساسة:

تبادل بيانات المعاملات الحساسة فقط عبر مسار أو وسيط موثوق به مع عناصر تحكم لتوفير أصالة المحتوى وإثبات التقديم وإثبات الاستلام وعدم التنصل من الأصل. (COBIT4,2007:118). وتتضمن المعلومات الحساسة: معلومات إدارة الأمان وبيانات المعاملات الحساسة وكلمات المرور ومفاتيح التشفير. ولتحقيق ذلك قد يلزم إنشاء القنوات الموثوقة باستخدام التشفير بين المستخدمين وبين الأنظمة (IT Governance,2000:103).

وتتمثل إجراءات الرقابة في هذا الجانب (IT Governance Institute,2007:121) في الآتي:

أ- تحديد كيفية حماية البيانات عند تبادلها باستخدام نظام تصنيف المعلومات المعمول به.

ب- تطبيق ضوابط التطبيق المناسبة لحماية تبادل البيانات.

ج- تطبيق ضوابط البنية التحتية المناسبة، على أساس تصنيف المعلومات والتكنولوجيا المستخدمة، لحماية تبادل البيانات.

8) إدارة مفتاح التشفير:

تعنى السياسات والإجراءات المعمول بها لتنظيم عملية الإنشاء والتغيير والإلغاء والإتلاف وتوزيع الشهادات وإصدارها والتخزين والإدخال واستخدام وأرشفة مفاتيح التشفير لضمان حماية المفاتيح من التعديل والكشف غير المصرح به. (COBIT4,2007:118). وينبغي التعامل مع مفاتيح التشفير بسرية تامة، ومراقبة عمليات تغيرها وتبادلها وفقا لإجراءات محددة (عقيل، 109:2011)، وفي حالة اختراق أحد المفاتيح، يجب أن تضمن الإدارة نشر هذه المعلومات إلى أي طرف مهتم من خلال استخدام قوائم إبطال الشهادات أو الآليات المماثلة (IT Governance,2000:103).

الدراسة الميدانية

منهج الدراسة:

استخدمت الدراسة المنهج الوصفي التحليلي وهو الذي يصف الحالة ويكشف ويحدد الخصائص وطبيعة العلاقة بين متغيرات الدراسة، والاعتماد على هذا المنهج وفقًا للآتي:

i. المنهج الوصفي: يتمثل في الأدبيات الخاصة بمتغيرات الدراسة، والقراءة المتعمقة في المكتبة العلمية المعاصرة وتقديم الإطار النظري والفكري، مستندًا إلى كتابات ومراجع علمية موثقة، والتعليق عليها، ومحاولة الإضافة في الإطار المفاهيمي لمتغيرات الدراسة.

ب- المنهج التحليلي: هو المتمثل في تحليل البيانات تحليلًا متعمقًا ومحاولة استكشاف أثر الإجراءات الرقابية المتعلقة بالتكنولوجيا في أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية.

وحدة التحليل:

بما أن متغيرات الدراسة لا يمكن قياسها إلا على مستوى المنظمات؛ لذا فإن وحدة الدراسة هي الشركة، وفي هذه الدراسة فإن وحدة التحليل هي البنك.

مجتمع وعينة الدراسة:

وتمثل مجتمع الدراسة في البنوك العاملة في اليمن؛ إذ تم إجراء الدراسة الميدانية في البنوك العاملة في اليمن والبالغ عددها (10) من خلال توزيع الاستبانة على عينة قصدية مثل أفرادها موظفي الإدارة المالية والمراجعة الداخلية، والحاسب وتقنية المعلومات بوصفهم القادرين على إعطاء بيانات ومعلومات تسهم في تحقيق أهداف الدراسة.

وقد تم توزيع (127) استمارة استبيان، وتم استعادة (88) استبانة، وبنسبة (69%) من العدد

الكلـي للاسـتبانات الموزعـة. والجـدول (1) يوضـح ذلك:

جدول (1): عدد الاستبانات الموزعة ونسبة العائد منها

البيان	الاستبانات		نسبة الاستجابة
	الموزعة	المستلمة	
عدد الاستبانات	127	88	69%

خصائص عينه الدراسة:

لقد تم استخراج التكرارات والنسب المئوية لوصف خصائص عينتي الدراسة جدول رقم (2) توزيع العينة حسب البيانات الشخصية.

جدول (2): توزيع أفراد العينة حسب الخصائص الديموغرافيـة

م	البيان	الفقرات	التكرار	النسبة المئوية (%)
1	فئات العمر بالسنوات	من 25 إلى 35 سنة	49	55.7%
		من 36 سنة فأكثر	39	44.3%
		الإجمالي	88	100.0%
2	المؤهل العلمي	بكالوريوس	69	78.4%
		ماجستير	15	17.0%
		أخرى	4	4.5%
		الإجمالي	88	99.9%
3	التخصص	محاسبة	57	64.8%
		حاسوب / تقنية معلومات	25	28.4%
		أخرى	6	6.8%
		الإجمالي	88	100.0%
4	الوظيفة الحالية	محاسب	37	42.0%
		مهندس حاسوب / تقنية معلومات	24	27.3%
		أخرى	27	30.7%
		الإجمالي	88	100.0%
5	سنوات الخبرة	من 5 سنوات فأقل	27	30.7%
		من 6 سنوات فأكثر	61	69.3%
		الإجمالي	88	100.0%

يتضح من خلال الجـــدول رقم (2): أن غالبيـة المبحوثـــين تتـراوح أعمارهـــم بـين 25 إلى35سنة وبنسبة55,7%من إجمالي أفراد العينة؛ وهذا يدل على النضج الكافي نسبيًا لدى أفراد العينة

للحكم والإجابة بموضوعية عن أسئلة الاستبانة حول موضوع الأثر الرقابي على أمن النظم المحاسبية الإلكترونية من منظور حوكمة تكنولوجيا المعلومات.

كما أن أغلب أفراد العينة لديهم مستوى تعليمي مناسب؛ إذ إن (78,4%) من أفراد العينة ذوى المؤهل بكالوريوس، و17%منهم مؤهل ماجستير، و 4,5% منهم مؤهلات أخرى، وعليه فإن معظم أفراد العينة ذوو مستوى تعليمي عالٍ يتناسب مع وظيفة أمن نظم المعلومات.

وأن التخصص الشائع بين غالبية أفراد العينة هو تخصص (محاسبة) وبنسبة 64,8%؛ وهذا ما يعطي نتائج أكثر واقعية؛ لأن حاملي هذا التخصص أكثر دراية بموضوع الدراسة من غيرهم، و28,4% تخصصهم (حاسوب/تقنية معلومات)؛ يليها6,8% تخصصات أخرى؛ حيث إن 42% يعمل في وظيفة محاسب، و27,3% يعمل في وظيفة قسم تقنية معلومات/حاسوب، وأن30,7% يعمل في مجالات أخرى؛ ونلاحظ أن من يعمل في قسم المحاسبة يعمل بمسؤولية وخبرة عالية ذات أثر رقابي على أمن النظم المحاسبية الإلكترونية من منظور حوكمة تكنولوجيا المعلومات.

كما يتضح من الجدول (2): أن غالبية المبحوثين تتراوح سنوات خبرتهم بين6 سنوات فأكثر وبنسبة (69,3%) ، يليهم الذين لهم خبرة عمل5 سنوات فأقل وبنسبة (30,7%)، وعليه يمكن القول: إن غالبية أفراد الدراسة تتمتع بخبرة عمل (أكثر من5 سنوات)؛ إذ تصل إلى ما نسبته (69,3%) من أفراد العينة، وتدل النتيجة السابقة على توافر عامل الخبرة لدى المبحوثين؛ وذلك يجعلهم قادرين على تكوين إجابات إيجابية أو سلبية أكثر دقة عن موضوع الأثر الرقابي على أمن النظم المحاسبية الإلكترونية؛ لأن الخبرات المتراكمة عبر الممارسات والتجارب تسهم إلى حد كبير في تكوين إجابات إيجابية أو سلبية نحو موضوع معين.

وسائل جمع البيانات والمعلومات:

اعتمدت الدراسة على وسيلتين رئيستين في جمع المعلومات، وهما: الاستبانة وفقًا لمقياس (Likert) الخماسي بالاستفادة من الدراسات السابقة التي درست متغيرات الدراسة، وتم تحكيم الاستبانة ومراجعتها وتوزيع الاستبانة لأفراد العينة المستهدفة، بالاعتماد على النموذج الورقي والنموذج الإلكتروني، كما تم حجز مجال خاص بالاستبانة الإلكترونية، مصمم بشكل تفاعلي على العنوان (https://forms.gle/rqHrpvPcCx8fRYoy6) ، وتمت الاستعانة بإدارات الموارد البشرية في البنوك لتوزيعها على العينة المستهدفة.

أساليب التحليل الإحصائي:

لتحقيق أهداف الدراسة وتحليل البيانات التي تم جمعها من أفراد العينة؛ تم استخدام عدد من الأساليب الإحصائية المناسبة باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (Statistical Package for Social Sciences) التي يرمز لها اختصارًا بالرمز (SPSS)، وهذه الأساليب الإحصائية على النحو الآتي:

- النسب المئوية والتكرارات: تم استخدام الجداول التكرارية لمعرفة توزيع الاجابات (عدد تكرار الاجابات والنسب المئوية)، حسب مقياس ليكرت الخماسي المستعمل في الاستمارة.
- معامل ألفا كرونباخ (Cronbch's Alpha) لقياس الثبات: تم استخدام هذا المعامل لاختبار وقياس ثبات أداة الدراسة، وقياس مدى الاتساق الداخلي بين عبارات ومحاور الدراسة، وتتراوح قيمته بين (0 و1)، وانخفاض قيمته عن 0.6 دليل على انخفاض الثبات الداخلي، أما إذا تجاوزت 0.6 فهذا دليل على ثبات الأداة وإمكانية اعتمادها في الدراسة (فيلالي، 2019 :199).
- معامل ارتباط وانحدار بيرسون (Pearson Correlation & Regression): تم استخدام معامل ارتباط بيرسون لقياس صدق مضمون (فقرات) الاستبانة؛ إذ يتم حساب معامل الارتباط بين درجة كل عبارة والمحور الذي تنتمي إلية، كما تم استخدامه مع معامل انحدار بيرسون لاختبار الفرضيات؛ إذ تتراوح قيمته بين (1 و -1).
- اختبار تي للعينة الواحدة (One Sample t- test).

تم استخدامه لاختبار الفرضيات وتحليل فقرات الاستبانة، بحيث تكون الفقرة إيجابية (أي إن أفراد العينة يوافقون على محتواها) إذا كانت قيمة (t) المحسوبة أكبر من قيمة (t) الجدولية؛ والتي تساوي (1,989) (أو مستوى المعنوية أقل من 0,05 والوزن النسبي أكبر من 60%)، وتكون الفقرة سلبية (أي إن أفراد العينة لا يوافقون على محتواها) إذا كانت قيمة t المحسوبة أصغر من قيمة (t) الجدولية؛ وتساوي (1,989)- (أو مستوى المعنوية أقل من 0.05 والوزن النسبي أقل من 60%)؛ وتكون آراء العينة في الفقرة محايدة إذا كان مستوى الدلالة لها أكبر من(0,05).

صدق وثبات الاستبيان:

قام الباحثان بالتأكد من صدق فقرات الاستبانة بطريقة صدق الاستبانة بالتحكيم، فضلًا ن التأكد من ثبات الاستبانة بطريقة معامل ألفا كرونباخ، وفيما يأتي عرض نتائج صدق الاستبانة وثباتها:

صدق الاستبانة بالتحكيم:

تم عرض الاستبانة على مجموعة من المحكمين تألفت من (7) من الأساتذة من أعضاء الهيئة التدريسية في مجال المحاسبة في جامعة صنعاء وجامعة تعز وجامعة إب وجامعة العلوم والتكنولوجيا، وقد استجاب الباحثان لآراء الأساتذة المحكمين وقام بإجراء ما يلزم من حذف وتعديل في ضوء مقترحاتهم بعد تسجيلها في نموذج تم إعداده، وبذلك خرجت الاستبانة في صورتها النهائية؛ ليتم تطبيقها على عينة الدراسة.

ثبات الاستبانة:

تم إجراء خطوات اختبار الثبات على العينة المبحوثه نفسها بطريقة معامل ألفا كرونباخ، ويمكن استعراض نتائج الاختبارين كما يأتي:

ثبات الاستبانة بطريقة ألفا كرونباخ:

استخدم الباحثين طريقة ألفا كرونباخ بوصفها طريقة ثانية لقياس ثبات الاستبانة، وقد جاءت النتائج كما يبينها الجدول (3):

جدول (3): معاملات الثبات (طريقة ألفا كرونباخ)

مجالات الاستبانة	عدد الفقرات	معامل ألفا كرونباخ للثبات
المجال الأول: الإجراءات الرقابية المتعلقة بالتكنولوجيا.	11	**0.903**
المجال الثاني: السرية.	5	**0.880**
المجال الثالث: السلامة.	5	**0.892**
المجال الرابع: التوافر.	6	**0.905**
جميع الفقرات	**27**	**0.970**

المصدر (إعداد الباحثين، 2023) بالاعتماد على مخرجات برنامج SPSS

يتضح من الجدول رقم (3): أن معاملات الثبات تتراوح بين0.880 و0.905؛ وهو ما يؤكد أن هناك معاملات الثبات مرتفعة لمحاور الدراسة.

نتائج التحليل الوصفي لإجابات المبحوثين على متغيرات الدراسة:

في سبيل القيام باختبار الفرضيات؛ تم القيام بالتحليل الوصفي لإجابات المبحوثين على متغيرات الدراسة باستخدام اختبار(T) للعينة الواحدة الذي بموجبه تكون الفقرة إيجابية (بمعنى أن أفراد العينة يوافقون على محتواها) إذا كانت قيمة (t) المحسوبة أكبر من قيمة (t) الجدولية التي تساوي (1.989) (أو مستوى المعنوية أقل من (0.05) والوزن النسبي أكبر من(60%)، وتكون الفقرة سلبية (أي إن أفراد العينة لا يوافقون على محتواها)، إذا كانت قيمة(t) المحسوبة أصغر من قيمة (t) الجدولية التي تساوي (1.989) – (أو مستوى المعنوية أقل من (0.05) والوزن النسبي أقل من 60%) ، وتكون آراء العينة في الفقرة محايدة إذا كان مستوى الدلالة لها أكبر من(0.05) .

تحليل فقرات الإجراءات الرقابية المتعلقة بالتكنولوجيا:

تم استخدام اختبار(T) للعينة الواحدة في تحليل فقرات (الإجراءات الرقابية المتعلقة بالتكنولوجيا) والنتائج مبينة في الجدول (4):

جدول (4): تحليل فقرات الإجراءات الرقابية المتعلقة بالتكنولوجيا

م	الفقرة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	قيمة t المحسوبة	مستوى الدلالة	اتجاة العينة	ترتيب السؤال
1	تدعم التكنولوجيا التحكم في إدارة وصول المستخدم للأنظمة التشغيل وفقًا لمستويات متعددة.	1	1	5	38	43	4.38	0.748	87.5	17.253	0	موافق بشده	1
2	يشرف البنك على تنفيذ خطة أمنية محدثة الضوابط بما يتوافق مع التغيرات التكنولوجية.	0	4	6	45	33	4.22	0.765	84.3	14.913	0	موافق	5
3	يمتلك البنك نظامًا للإبلاغ عن الانتهاكات الأمنية وفقًا للسلطات والصلاحيات المعنية.	0	5	13	41	29	4.07	0.841	81.4	11.909	0	موافق	11
4	تُراجع الاختراقات الأمنية المبلغ عنها من قبل فريق متخصص لتقليل الاختراقات.	0	2	12	49	25	4.10	0.712	82.0	14.527	0	موافق	9
5	توجد معايير تأديبية لمخالفي السياسات الأمنية تدرج في أطر التقييم الوظيفي للمستخدم.	0	1	7	42	38	4.33	0.673	86.6	18.523	0	موافق بشدة	3
6	تدعم البنية التكنولوجية الإجراءات الرقابية لإثبات هوية المستخدم.	0	1	2	48	37	4.38	0.593	87.5	21.740	0	موافق بشدة	2
7	يتم تطبيق التوقيعات الرقمية في البنك لضمان نقل البيانات من خلال مصدر	0	4	10	40	34	4.18	0.810	83.6	13.686	0	موافق	6

م	الفقرة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	قيمة t المحسوبة	مستوى الدلالة	اتجاة العينة	ترتيب السؤال
	موثوق.												
8	تُحدد تقنيات حماية وتبادل المعلومات على أساس نظام التصنيف المعلومات في البنك.	0	2	7	52	27	4.18	0.670	83.6	16.539	0	موافق	7
9	توجد منظومة ضوابط لإدارة مفاتيح التشفير للحماية من التعديل والكشف غير المصرح.	0	3	8	49	28	4.16	0.725	83.2	14.990	0	موافق	8
10	تدعم تقنيات التشفير سلامة المعالجة وتبادل وخزن البيانات والمعلومات في البنك.	0	1	8	48	31	4.24	0.661	84.8	17.584	0	موافق	4
11	توجد شهادة تصديق بموثوقية تكنولوجيا المعلومات في البنك.	0	3	15	43	27	4.07	0.785	81.4	12.767	0	موافق	10
	الإجراءات الرقابية المتعلقة بالتكنولوجيا.	0.09	2.45	8.45	45.00	32.00	4.209	0.737	84	15.384	0		

قيمة (t) الجدولية عند مستوى دلالة (0.05) ودرجة حرية (87) تساوي (1.989)

المصدر: التحليل الإحصائي لبيانات الدراسة الميدانية

يتضح من الجدول رقم (4): أن آراء المستجيبين في جميع فقرات المجال الثالث إيجابية؛ إذ وجد في كل فقرة أن قيمة (t) المحسوبة أكبر من قيمة (t) الجدولية التي تساوي (1.989)، ومستوى الدلالة لكل فقرة أقل من(0.05) ، والوزن النسبي لكل فقرة أكبر من الوزن النسبي المحايد (60%)؛ بمعنى أن (87.6%) من أفراد مجتمع الدراسة يتفقون على أنه: "تدعم البنية التكنولوجية الإجراءات الرقابية لإثبات هوية المستخدم"، كما أن (87.6%) من أفراد مجتمع الدراسة يتفقون على أنه: "تدعم التكنولوجيا التحكم في إدارة وصول المستخدم للأنظمة التشغيل وفقًا لمستويات متعددة"، وأن (86.6%) من أفراد مجتمع الدراسة يتفقون على أنه: "توجد معايير تأديبية لمخالفي السياسات الأمنية تدرج في أطر التقييم الوظيفي للمستخدم"، وأن(84.8%) من أفراد مجتمع الدراسة يتفقون على أنه: "تدعم تقنيات التشفير سلامة المعالجة وتبادل وخزن البيانات والمعلومات في البنك"، كما أن(84.4%) من أفراد مجتمع الدراسة يتفقون على أن: "يشرف البنك على تنفيذ خطة أمنية محدثة الإجراءات بما يتوافق مع التغيرات التكنولوجية"، وأن(83.6%) من أفراد مجتمع الدراسة يتفقون على أنه: "تُحدد تقنيات حماية وتبادل المعلومات على أساس نظام التصنيف المعلومات في البنك"، وأن(83.6%) من أفراد مجتمع الدراسة يتفقون على أنه: "يتم تطبيق التوقيعات الرقمية في البنك لضمان نقل البيانات من خلال مصدر موثوق"، وأن(83.2%) من أفراد مجتمع الدراسة يتفقون على أنه: "توجد منظومة ضوابط لإدارة مفاتيح التشفير للحماية من التعديل والكشف غير المصرح"، وأن(82%) من أفراد مجتمع الدراسة يتفقون على أنه: "تُراجع الاختراقات الأمنية المبلغ عنها من قبل فريق متخصص لتقليل الاختراقات"، كما أن(81.4%) من أفراد مجتمع الدراسة يتفقون على أنه: "توجد شهادة تصديق بموثوقية تكنولوجيا المعلومات في البنك"، وأن(81.4%) من أفراد مجتمع الدراسة يتفقون على أنه: "يمتلك البنك نظامًا للإبلاغ عن الانتهاكات الأمنية وفقًا للسلطات والصلاحيات المعنية".

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات تحليل فقرات الإجراءات الرقابية المتعلقة بالتكنولوجيا (4,222) والوزن النسبي يساوي (84,44%)، وهي أكبر من الوزن النسبي المحايد (60%)، وقيمة (t) المحسوبة تساوي (17,958)، وهي أكبر من قيمة(t) الجدولية التي تساوي (1,989)، ومستوى الدلالة تساوي (0,000)، وهي أقل من (0.05)؛ وهو ما يدل على أن ما نسبته (84,44%) من المبحوثين يتفقون على توافر الإجراءات الرقابية المتعلقة بالتكنولوجيا في البنوك العاملة في الجمهورية اليمنية الخاضعة للدراسة.

اختبار الفرضية

في سياق اختبار الفرضية؛ تم الاعتماد على اختبار معامل ارتباط وانحدار بيرسون واختبار

(T-test) للعينة الواحدة فيما بين المتغيرات المستقلة المعبر عنها في الإجراءات الرقابية المتعلقة بالتكنولوجيا، وبين المتغير التابع المعبر عنه بواقع أمن نظم المعلومات المحاسبية في البنوك اليمنية فيما يتعلق بالسرية والسلامة والتوافر.

ووفقًا لتحليل الانحدار والارتباط واختبار (T-test) للعينة الواحدة فإن وجود علاقة الارتباط الإيجابية ذات الدلالة الإحصائية المعنوية عند مستوى دلالة ($\alpha \geq 0.05$) فيما بين المتغيرات المستقلة والمتغير التابع تتوافر فقط؛ حيثما تكون قيمة (T) المحسوبة أكبر من قيمة (T) الجدولية (1.989)، وكذا عندما تؤكدها قيمة مستوى الدلالة المعنوية المحسوبة بأن تكون أصغر من مستوى الدلالة المعتمدة في هذه الدراسة (0.05)، و على أن يشير معامل الارتباط (R-Pearson) المحسوب الموجب إلى وجود الارتباط الإيجابي بدرجة أكبر من أو تساوي قيمة(R) الجدولية (0.239). أما قوة هذا الارتباط فتدل عليه قيمة معامل الانحدار B-Pearson المحسوبة التي تزداد كلما اقتربت من الواحد الصحيح والعكس، وتؤكد معنوية هذه العلاقة قيمة (F) المحسوبة إذا كانت أكبر أو تساوي قيمة الوسط الفرضي للمقياس المستخدم في الدراسة، وهو (3). وبعد إجراء الاختبارات المبينة أعلاه؛ تم الحصول على النتائج على النحو الآتي:

الفرضية:

" لا يوجد أثر للإجراءات الرقابية المتعلقة بالتكنولوجيا على أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية ".

لاختبار الأثر الرقابي للإجراءات الرقابية المتعلقة بالتكنولوجيا على أمن نظم المعلومات المحاسبية في البنوك العاملة في اليمن؛ تم استخدام اختبار الارتباط والانحدار واختبار (T-test) للعينة الواحدة والنتائج مبينة في الجدول (5):

جدول (5): نتائج اختبار الارتباط والانحدار واختبار (T-test) للفرضية

	المتغير المستقل الثالث: الإجراءات الرقابية المتعلقة بالتكنولوجيا	معامل الارتباط (R-Pearson)	معامل الانحدار (B-Pearson)	معامل التحديد (R^2)	قيمة (T) المحسوبة	قيمة (T) الجدولية	قيمة (F) المحسوبة	مستوى الدلالة المعنوية (Sig.)	معنوي/ غير معنوي
1	تدعم التكنولوجيا التحكم في إدارة وصول المستخدم للأنظمة التشغيل وفقًا لمستويات متعددة.	0.574	0.406	0.329	6.497	1.989	42.216	0.000	معنوي
2	يشرف البنك على تنفيذ خطة أمنية محدثة الضوابط بما يتوافق مع التغيرات التكنولوجية.	0.374	0.259	0.140	3.736	1.989	13.958	0.000	معنوي

	المتغير المستقل الثالث: الإجراءات الرقابية المتعلقة بالتكنولوجيا	معامل الارتباط (R-Pearson)	معامل الانحدار (B-Pearson)	معامل التحديد (R^2)	قيمة (T) المحسوبة	قيمة (T) الجدولية	قيمة (F) المحسوبة	مستوى الدلالة المعنوية (Sig.)	معنوي/ غير معنوي
3	يمتلك البنك نظامًا للإبلاغ عن الانتهاكات الأمنية وفقًا للسلطات والصلاحيات المعنية.	0.405	0.255	0.164	4.106	1.989	16.856	0.000	معنوي
4	تُراجع الاختراقات الأمنية المبلغ عنها من قبل فريق متخصص لتقليل الاختراقات.	0.230	0.171	0.053	2.187	1.989	4.748	0.031	معنوي
5	توجد معايير تأديبية لمخالفي السياسات الأمنية تدرج في أطر التقييم الوظيفي للمستخدم.	0.429	0.337	0.184	4.403	1.989	19.385	0.000	معنوي
6	تدعم البنية التكنولوجية الإجراءات الرقابية لإثبات هوية المستخدم.	0.339	0.302	0.115	3.338	1.989	11.139	0.001	معنوي
7	يتم تطبيق التوقيعات الرقمية في البنك لضمان نقل البيانات من خلال مصدر موثوق.	0.464	0.303	0.216	4.862	1.989	23.641	0.000	معنوي
8	تُحدد تقنيات حماية وتبادل المعلومات على أساس نظام التصنيف المعلومات في البنك.	0.302	0.238	0.091	2.937	1.989	8.627	0.004	معنوي
9	توجد منظومة ضوابط لإدارة مفاتيح التشفير للحماية من التعديل والكشف غير المصرح.	0.587	0.428	0.344	6.718	1.989	45.130	0.000	معنوي
10	تدعم تقنيات التشفير سلامة المعالجة وتبادل وخزن البيانات والمعلومات في البنك.	0.555	0.445	0.308	6.188	1.989	38.293	0.000	معنوي
11	توجد شهادة تصديق بموثوقية تكنولوجيا المعلومات في البنك.	0.489	0.330	0.239	5.204	1.989	27.077	0.000	معنوي
	المتغير التابع: أمن نظم المعلومات المحاسبية من منظور حوكمة المعلومات	0.637	0.528	0.406	7.664	1.989	58.734	0.000	معنوي

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية 87 تساوي 0.239

في ضوء النتائج المبينة في الجدول (5) أظهرت نتائج تحليل الانحدار والارتباط واختبار (T-test) للعينة الواحدة؛ وجود علاقة ارتباط إيجابية ذات دلالة إحصائية معنوية عند مستوى دلالة (0.05) بين الإجراءات الرقابية المتعلقة بالتكنولوجيا (المتغير المستقل) المشار إليها بالفقرات رقم (9،1،10،11،7،5،3،2،6،8،4) على التوالي، وبين واقع أمن نظم المعلومات المحاسبية في البنوك العاملة في اليمن من منظور حوكمة المعلومات (المتغير التابع)؛ إذ تشير قيمة معامل الانحدار إلى أن الزيادة بدرجة واحدة في الالتزام بالإجراءات الرقابية المتعلقة بالتكنولوجيا يؤدي إلى الزيادة في واقع أمن نظم المعلومات المحاسبية في البنوك العاملة في اليمن من منظور حوكمة المعلومات لتلك الفقرات، بمقدار (0.587، 0.574، 0.555، 0.489، 0.464، 0.429، 0.405، 0.374، 0.339، 0.302، 0.230) على التوالي من الدرجة والعكس. كما تشير قيمة معامل التحديد إلى أن التغير في الالتزام بالإجراءات الرقابية المتعلقة بالتكنولوجيا مسؤولة عن (34%، 33%، 31%، 24%، 22%، 18%، 16%، 14%، 12%، 10%، 5%) على التوالي من التغير في واقع أمن نظم المعلومات المحاسبية في البنوك العاملة في اليمن من منظور حوكمة المعلومات. وهذا التأثير المعنوي تؤكده قيمة (F) المحسوبة التي بلغت (45.130، 42.216، 38.293، 27.077، 23.641، 19.385، 16.856، 13.958، 11.139، 8.627، 4.748) على التوالي، وهي جميعها دالة معنوية؛ لأن مستوى الدلالة المحسوبة كانت أقل من مستوى الدلالة المعتمدة في الدراسة (0.05). ومن خلال المقارنة بين قيمة اختبار (t) المحسوبة (6.718، 6.497، 6.188، 5.204، 4.862، 4.403، 4.106، 3.736، 3.338، 2.937، 2.187) على التوالي، وهي تزيد بدرجة معنوية عن القيمة الجدولية (1.989)، ويعني ذلك وجود أثر إيجابي بدرجة ذات دلالة إحصائية معنوية عند مستوى دلالة (0.05) للالتزام بالإجراءات الرقابية المتعلقة بالتكنولوجيا على واقع أمن نظم المعلومات المحاسبية في البنوك العاملة في اليمن من منظور حوكمة المعلومات.

في ضوء ما سبق، وبشكل عام، يتبين أن قيمة معامل الارتباط العام للإجراءات الرقابية المتعلقة بالتكنولوجيا بلغت (0.637) بمدى تراوح بين (0.587-0.230)، كما أن قيمة معامل الانحدار العام بلغت (0.528) بمدى تراوح بين (0.428-0.171)، وبلغت قيمة معامل التحديد العام (0.406) بمدى تراوح بين (0.344-0.053)، وبما أن قيمة اختبار (t) المحسوبة للإجراءات الرقابية المتعلقة بالتكنولوجيا بلغت (7.664) بمدى تراوح بين (6.718-2.187)، وقيمة معامل (F) المحسوبة بلغت (58.734) بمدى تراوح بين (45.130-4.748)، وقيمة مستوى الدلالة المحسوبة للمحور كانت (0.000) بمدى تراوح بين (0.000-0.031)، وهي أقل

من مستوى الدلالة المعتمدة في الدراسة (0.05). فإن ذلك يعني وجود أثر إيجابي بدرجة ذات دلالة إحصائية معنوية للإجراءات الرقابية المتعلقة بالتكنولوجيا على واقع أمن نظم المعلومات المحاسبية في البنوك العاملة في اليمن من منظور حوكمة المعلومات.

وبناء على ما سبق يمكننا رفض الفرضية التي تنص على أنه: " لا يوجد أثر ذو دلالة إحصائية للإجراءات الرقابية المتعلقة بالتكنولوجيا على أمن نظم المعلومات المحاسبية الإلكترونية في البنوك العاملة في الجمهورية اليمنية".

ويستعاض عنها بالفرضية البديلة التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية للإجراءات الرقابية المتعلقة بالتكنولوجيا على أمن نظم المعلومات المحاسبية الإلكترونية في البنوك العاملة في الجمهورية اليمنية".

الاستنتاجات والتوصيات:

الاستنتاجات:

توصلت الدراسة إلى وجود تأثير للإجراءات الرقابية المتعلقة بالتكنولوجيا في أمن نظم المعلومات المحاسبية في البنوك العاملة في الجمهورية اليمنية بنسبة 84.44% حول توافر الإجراءات الرقابية المتعلقة بالتكنولوجيا، كما تشير أيضًا إلى توافق عالٍ بنسبة 89.10% حول توافر أمن نظم المعلومات المحاسبية في مجالات السرية، السلامة، والتوافر، وأن الزيادة بدرجة واحدة في الإجراءات الرقابية المتعلقة بالتكنولوجيا يؤدي إلى الزيادة في أمن نظم المعلومات المحاسبية في البنوك اليمنية، بمقدار (0,528).

التوصيات:

في ضوء ما سبق التوصل إلية من الدراسة من استنتاجات؛ توصي الدراسة بأنهُ يجب على البنوك العاملة في الجمهورية اليمنية أن تبذل مزيدًا من الاهتمام في تعزيز إجراءات التحقق من الهوية وضبط التحكم بالوصول المادي والمنطقي واستخدام تقنية التشفير ومنع التسلل والجدران النارية.

المراجع:

الكتب:

1. الاتحاد الدولي للاتصالات. (2007). دليل الأمن السيبراني للبلدان النامية.
2. حجر، عبد الملك. (2014). نظم المعلومات المحاسبية. ط4. الأمين للنشر والتوزيع. صنعاء. اليمن.
3. ستينبارت، بول، و رومني، مارشال. (2009). نظم المعلومات المحاسبية. ترجمة (قاسم إبراهيم الحسيني). دار المريخ: الرياض. المملكة العربية السعودية.
4. عقيل، محمد. (2011). مقدمة في حوكمة تقنية المعلومات باستخدام نموذج كوبت الإصدار الرابع 2007، ط الأولى.
5. القحطاني، ذيب. (2015). أمن المعلومات. مدينة الملك عبد العزيز للعلوم والتقنية.
6. معهد حوكمة تكنولوجيا المعلومات، جمعية تدقيق ومراقبة نظم المعلومات. (2004).

رسالة ماجستير، جامعة محمد البشير الإبراهيمي، الجزائر.

ثانيًا: الأطاريح والرسائل الجامعية:

1. الحميري، نبيل. (2021). أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الإجراءات الأمنية. دراسة ميدانية في شركات الاتصالات العاملة في اليمن. رسالة دكتوراه الفلسفة في المحاسبة. أطروحة غير منشورة. جامعة العلوم والتكنولوجيا. اليمن.
2. الدنف، أيمن. (2013). واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، رسالة ماجستير منشورة. الجامعة الإسلامية غزة.
3. الشرعبي، نبيل. (2014). التطوير المقترح للرقابة الداخلية في البنوك اليمنية من خلال الإصدارات والتشريعات ذات العلاقة، رسالة دكتوراة غير منشورة. جامعة بورسعيد.
4. طارش، أحمد. (2015). رؤية إستراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقق والادعاء العام في المملكة العربية السعودية. رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية. كلية العلوم الاستراتيجية.
5. عي، راضية؛ وبولفراخ، ونسرين.(2020). أثر استخدام تكنولوجيا المعلومات والاتصال على تسيير الموارد البشرية– دراسة حالة البنك الخارجي الجزائري BEA – برج بوعريريج،
6. فيلالي، أسماء. (2019). مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثرها بطبيعة التهديدات وطبيعة الحماية المطبقة، أطروحة دكتوراه منشورة. جامعة أبي بكر بلقايد.
7. نصور، ريم. (2015). أثر حوكمة تكنولوجيا المعلومات على جودة التقارير المالية، دراسة ميدانية. أطروحة دكتوراه. جامعة تشرين. سوريا.
8. نصور، ريم؛ علي، حسين؛ زيود، لطيف. (2004). تحديد مستوى حوكمة تكن ولوجيا المعلومات المطبق في المصرف التجاري السوري باللاذقية وفق إطار عمل (COBIT).

ثالثًا: المجلات العلمية المحكمة:

1. الحكيم، سليم. (2010). إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمتة للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية. المجلد 26 العدد الأول. ص563–592.
2. جبوري، ندى. (2011). حماية أمن أنظمة المعلومات. دراسة حالة في مصرف الرافدين. مجلة تكريت للعلوم الإدارية والاقتصادية . المجلد7 العدد 21. ص72–94.

3. الربيدي، محمد؛ والحميري، نبيل. (2023). أثر الضوابط الأمنية في أمن نظم المعلومات المحاسبية في قطاع الاتصالات باليمن، مجلة جامعة العلوم والتكنولوجيا للعلوم الإدارية والإنسانية. المجلد (1) العدد (2). ص1-39.
4. الربيدي؛ والحميري. (2021). أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات – دراسة ميدانية في شركات الاتصالات العاملة في اليمن، مجلة الدراسات الاجتماعية. المجلد السابع والعشرون العدد (1) مارس 2021م. ص125-157.
5. الربيدي، محمد. (2012). تقييم نظام الرقابة الداخلية للمنشآت المستخدمة لتكنولوجيا المعلومات: دراسة ميدانية في مكاتب المراجعة اليمنية. المجلة العربية للمحاسبة. أكتوبر 2012. ص89-122.
6. شحادة، فراس؛ وبدر، محمد. (2020). واقع أمن وسرية المعلومات الإلكترونية في بنك فلسطين، المؤتمر الدولي الأول في تكنولوجيا المعلومات والأعمال (ICITB2020).
7. الشمالي، حسين. (2017). أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، فلسطين. المجلد الثاني العدد7. ص187-200.
8. صالح، سادات؛ وعبدالله، معاوية. (2016). أثر نظام الرقابة الداخلية في تحقيق أمن المعلومات المحاسبية. مجلة جامعة القرآن الكريم والعلوم الإسلامية – السودان .المجلد 19. ص191-234.
9. عبدالله، علي؛ والناصر، خالص. (2019). حوكمة أمن المعلومات ودورها في تخفيض مخاطر نظم المعلومات المحاسبية الإلكترونية، ورقة عمل مقدمة إلى الندوة العلمية لقسم إدارة الأعمال كلية الإدارة والاقتصاد جامعة الموصل بالتعاون مع قيادة عمليات نينوى الموسومة "الإدارة الأمنية في محافظة نينوى وسبل تطويرها، ص1-9.
10. نصور، ريم. (2014). أثر تطبيق حوكمة تكنولوجيا المعلومات وفق إطار عمل COBIT على جودة التقارير المالية، دراسة ميدانية في المصارف السورية، مجلة جامعة البعث. المجلد (36) العدد (2). ص207-236.

المراجع الأجنبية:

1. Cobit®4.1, 2007 COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance,2007, IT Govern-ance Institute, 2nd Edition Print-

ed in the United States of America.

2. International Standard ISO/IEC 27001,2005.
3. International Telecommunication Union (ITU) (2020). Global cybersecurity Index.
4. International Telecommunication Union (ITU) (2015). Global cybersecurity.
5. International Telecommunication Union (ITU) (2017). Global cybersecurity index
6. International Telecommunication Union (ITU). (2018). Global cybersecurity
7. IT Governance ,2000, COBIT®3rd Edition Control Objectives.
8. Joint Task Force Transformation Initiative (JTFTI). (2013). Security and privacy controls for federal information systems and organizations. Special publication No. 800-53 revision 4. Gaithersburg, Maryland: National Institute of Standards and Technology (NIST)
9. Joint Task Force Transformation Initiative. (2012). Guide for conducting risk.
10. Shamsi S. Bawaneh (2018) ,Securing Information Technology for Banks and Accounting Information Systems , International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 3291-3300.
11. Sheikhpour, Razieh, and Modiri, Nasser,2012 ,An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012,13-27, P17.
12. The IT Governance Institute, Information Systems Audit and Control Association,2004, Cobit® Student book.